一様乱数の数理

中澤　宏

平成 16 年 1 月 12 日

緒　　言

「一様乱数の数理」を刊行してから 2 年が過ぎ, その間に文中の多くの誤りについて御指摘を頂きました. 詫間電波高専での 5 年制御工学科の学生諸君への応用数学の 1 テーマとして授業を行う中でも多くの誤植が発見され, さらに連結 M 系列乱数に関する Tausworthe, 或いは Lewis-Payne の方法と伏見-手塚の定理の重みに関する記述の重要な誤りの認識に達しました. この結果は環瀬戸内応用数理研究集会 (2001 年 6 月) で報告されたところですが, 短く言うと連結 M 系列乱数を考えるには専ら伏見-手塚の定理に基づくべきなのです.

視野を高専 5 年生への授業のテーマに絞って振り返るならば, まず量として週 2 時間 2/3 年ですべてを終える事は難しく, 特に加算生成法についての Brent の判定条件の導出は, 結果の端的な判定条件の使用には特に困難はないのに比べて証明の面倒と実用上の興味の少なさもあって, 大きく端折らざるを得ないのが現実でしょう. しかしその様な限定を外し, 一般に 18 才程度以上の学年でゆっくり沈潜して頂くべきものとして考えると, 乱数問題が「群」や「体」という代数系への導入の, 僥倖とも言うべき適度の難易度, 大きさ, ··· を兼ね備えた好個のテーマである事, さらに言えば加算生成法の議論や一般の線形漸化式の考察が「環」の概念導入の必要への明澄な透視を与える事は殆ど不思議とも思われる程です. この問題の重要さの確信は強まるばかり, さまざまな情報技術に関連した基礎数理の 1 つとしてこれらの代数構造の理解の伝達が, 数学的のみではなく工学応用への視野と興味とを保った, いわゆる「応用数学」のテーマとして重要である事の痛感は深まるばかりです. この事に 1 人でも多くの方々の共感を頂く事が願われてなりません.

この認識を自己の励みとして, 再度多方面の御批判を仰ぐ様に努力を続けました. もちろん前版から続けても未だ, この様な小冊子でさえ構成と文面の細部にまで目を届かせる事の難しい自分の力に頭を垂れざるを得ません. ただ読者の御寛容と, 御慧眼からの新たな御叱正とを願って, はじめの言葉とします.　　**(2001.8.18. 著者)**

目　　次

まえおき

この本はコンピュータ上での一様乱数生成に関係する数学構造の概観を演習型式で展開する. 目指すのは最も容易な理解の伝達である; 優れた端的な証明ではなかろうし, ましてや新しい論考でもない. 目的を「完全で理想的な, すべての使用目的に役立つ乱数生成機構の知識を記そうとしている」と考えて貰っても困る. 含まれた具体的な話題は遥に慎ましい. 目指す結論は, 1,2 の明るい展望を除いて, 高々どのような乱数機構を考えればそれがうまくない, 問題を含むか, についての見通しであり, また理想的な all purpose な乱数ルーチンは存在しそうにもないというある意味で残念な悟りである. しかし全体を振り返って見直す位置に立つ時, これらの工学的知識が小さくも無意味でもないと思われると信じる. そしてまた, 途上で触れられた数学構造から, 我々の用いている「数」というものについて新しい視野と興味とを発見されていれば, と深く願う.

この本では理工系の基礎数学知識, 我が国の現在までの常識で言うと極限や微分, 積分, 特殊な関数, あるいは確率統計さえも特には求めない. 読み進むには 2 次方程式や複素数, そして行列の積や和, 連立 1 次方程式とその行列式演算による解法の簡単な知識で十分である. しかしここに記された事柄が初等的だ, つまらない, と受け取って頂いては困ると大急ぎで付言する. 述べる事ができた内容からは気恥かしいが, 私たちは現代的な数学を僅かでも垣間見るし, この様な理工系数学の世界の存在は現在強調しなければならないからでもある; 実際ここで次々に現れる演算の中には難しくはないが余り見慣れない, 風変わり, 面白いのに学校では全然教わらなかった, と感じられるものも多いだろう. 記述された内容を十分に理解し, 演算に慣れながら進む事は, 理工参考書の常として, また特にこの事情からも, 読者の側の努力に委ねられなければならない. 何もしないで理解できる理工数学書というものがあるなら, それはつまらない内容しか持てない. 問題の構造についての新しい視野と理解とを得る道程は, 幾何学の証明などで既知の通り, 何にもまさる数学の喜び, 楽しみである. 紙と鉛筆で試みて体得する努力は大いに払って頂きたい.

コンピュータ上の乱数ルーチン開発の歴史は, 歴史或いはドラマと言える程のものが実際既にできていると思われるのだが, 我々が数理, 特に整数の数理に翻弄され続けた姿である. その中で専門家も含む多くの人々の辛苦や悔し涙と共に得られた知識, 陥りやすい幾つかの過ち (乱数問題では特に, 過ち自体は恥ずべき何ものでもなく, 認め正す勇気こそが大切である) を避ける智恵, はこれからの強い力となるだろう. 少なくとも確信と共にコンピューターシミュレーションを行う助けとなり, もっと具体的には例えばシミュレーションに基づいて仕事や研究を進める上で乱数の性質が問題なのではないか, という厄介な疑問を生じた時にも自信を持って進み, さらに多くの問題で過信からの実際的危険を避ける事を可能にするだろう. しかしこれらでもまだ小さな事ではある. 読者は何よりも, 乱数に関わる数理がどれも大変美しく面白い, という認識を共にして頂けると信じる.

幾分数量的, 数学的に話そう. 値 x が区間 $0 \leqq x \leqq 1$ で均等な確率を持つ[1]確率変数 x は一

[1]確率分布 (密度関数)$f(x)$ の言葉を使えば「$f(x) = 1$ である」事, 即ち「範囲 $0 \leqq u \leqq x \leqq u + \Delta u \leqq 1$ の値が出現する確率が $f(u)\Delta u = \Delta u$ である」事が一様乱数 x の定義となる.

様乱数 uniform random number と呼ばれる. 一様乱数 x の独立な系列 $x_1, x_2, \cdots$, つまり乱数 x_j と x_k の取る $[0,1]$ での値が異なる j, k では全く関係がない, もっと正確には任意の個数 l と番号の組 $i_1, i_2, \cdots, i_l$ とに対してすべての変数を区間 $[0,1]$ 上で考えた確率密度関数が $f_l(x_{i_1}, x_{i_2}, \cdots, x_{i_l}) = 1$ であるものを一様独立乱数列と言う. 一様独立 (に近い, 或いはその様に「見える」) 乱数列を発生する乱数機構は, 現在のどんな小さなコンピューター上にも, シミュレーションやゲームには欠かせないルーチン, 関数として装着されている. 乱数については容易に利用できるいくつかの教科書がある.[1),2),3),4)] これらは乱数生成の色々な方法, それらの使い方や注意, 結果の乱数列の確率統計的性質の検定の問題, (現在はパソコン上でさえ問題の緊迫度は幾分薄れたが) 計算機上の生成速度等や必要とする記憶量等をそれぞれ色々な重みで議論して, 実用上大切な多くの情報, 示唆を与えてくれる.

しかし計算機上に, あるいはこれら文献の記述の中に使用目的に適したルーチンがない事は多々ある. 例えば計算機組込み乱数より長い周期が必要な場合はごく普通に起きる. そうでなくても, 組込み乱数の使用から問題が生じる事さえある. 昔の汎用計算機, IBM システム 370 上に置かれた RANDU という一様乱数ルーチン

$$x_k = 65539 x_{k-1}, \ (\mathrm{mod}\ 2^{31})$$

即ち $65539 \times x_{k-1}$ を計算し, それを 2^{31} で割った余りを x_k とする方式[2]は, 専門家の誤りから, 大変性質の悪いものである事が多くの users のクレームの後判明したという.[3] そうとは知らず, おかしな計算結果に悩まされた人々はクレームを申立てた人々の何十倍にもなる事だろう. 最近でも, 多くの検定を pass した「良い発生方法」からの相続く乱数にひそんでいた相関がシミュレーションに大きな誤差を発生させてしまった例[5)] もある. これらの事を聞くと我々はなにを信じて頻繁に生じるシミュレーションの必要に対応すればよいのか分らなくなる. 最良の道は自分の知識でいろんな乱数ルーチンを検討し直し, 別の方法を選択し, 使用法を変更し (例えば shuffle する; 但しこれが「高度な性質」をかえって悪化させる事もあるからややこしい; 終章参照), さらには新しく設計, 作成する事だろうが, 各人の各仕事に忙しい時にゆったりと乱数の原理まで勉強しなおす余裕はなかろう, とは確信を持って言える. 前もって教養, 予備知識として, 乱数発生の数理, 原理の理解, 或いは概観を身につけて置く事の必要性を仕事の上で既に痛く思い知らされている読者も多いだろう.

しかし残念な事に, Knuth[2)] を除いて我々の周りの文献にはこの数理メカニズムの解説は殆どない. そして文献 [2)] を読み通して理解することは, 少なくとも現在この本を手にしておられる大部分の読者にとって, 大変難しい. 記述が我々の知識に最適と思われる参考文献 [6)] はあるが, 入手が大変困難である.[4] 実はこの数理の基本的な部分は, 信号の符号化, 誤り検出や訂正等の通信情報的な問題の基礎分野と深い関係を持っていて, 乱数発生の原理の理解はこれらの重要な事柄の理解獲得の機会も与えているのである. しかし残念な事の第 2 にこの「数理」は, 現在の所, 普通我々が学ぶ事の少ない「代数学」や, 難解な「(整) 数論」の深い山の中にある様に見えて (本当は違うのだが), 数学のそれらの分野の専門家は別として「乱数の使用者」が一人で取り付くには敷居が大変高い. 文献 [1),3),4)] での記述の少なさや欠如はこの事の現れであり, また実際に文献 [2)] の各所を開いて見ればその「難しさ」はた

[2]一様乱数としては $u_k := x_k/2^{31}$ を取る事になる.

[3]この RANDU の生成する系列 $\{x_k\}$ については $9x_k - 6x_{k+1} + x_{k+2} = 0 \ (\mathrm{mod}\ 2^{31})$ の漸化式の存在が知られている. これはすぐ後に問題として見られる.

[4]この古典文献 [6)] は, 読者にもし機会があれば是非一読を勧める.

ちまちに実感されよう. もう少し理解しやすく, 乱数生成のいろいろなアイデアの歴史や基礎数理に詳しい文献 [6] でさえも, 著者にとっての自明な知識であるためだろうが, 我々が必要とする基礎的な事柄についての記述は親切とは言えない.

この本の目的はこれら基礎原理について, 欠けているやさしい解説を補い構造を見通せる視野を準備する事にある. 幸い目指す数学知識は情報系の数学としての応用をますます広げつつあって, それらを学ぶ事の大切さ, 将来的な価値は疑いもない. さらに喜ばしい事に, 専門として情報数学を必要とはしてなくても試みに立ち入って見れば, 理論全体の簡明な体系, 構造が少しの手の (即ち紙と鉛筆の) 使用で意外な美しさと多くの驚き, 楽しさと共に見出されるだろう. 以下, できればあまり苦労をせずに「思考の散歩」としてこれらに共に分け入ってみたい.

歴史的な事項については文献 [2),6)] に詳しい. 論文なら以下の事はこれらの文献を引用するだけでも十分だが, 入門書としては幾分の記述が理解のため適当である. 乱数実現の実際手段としては真空管や放射線から生成される noise などが「物理乱数」の名で用いられた事もあるらしい. しかし現在我々が乱数を用いるとしたら, 得る事の容易さ, (計算) 費用, 速度のどの点から見ても, 計算機上のなんらかの整数算法の利用が例外のない実現手段になる. これらは上の物理乱数とは違って擬似乱数 pseudorandom number と呼ばれる; その乱数系列 $\{x_0, x_1, x_2, \cdots\}$ では, 良く知られている事だが, 本当は x_{k-1} から x_k への簡単な変換規則があって, その予備知識なしにその規則を見つけるのは簡単ではないが規則を知っている人にとってはでたらめとは言えないからである. これは乱数の出現系列の独立性を少しまやかす事ではある.

しかしこのような簡単な規則の存在はむしろ望ましい. それは特に乱数系列の再現性という代えがたい利点を与える. シミュレーションの計算プログラムの debug[5]をしよう, 計算結果を比較しよう, と思うなら同じ乱数系列の再現が要求される. 勿論この再現はコンピュータの機種によらず (portable) に成り立たなければならない. この必要性は大変重要なもので, 実際, たとえ少々乱数としての性質が良くても再現性のない物理乱数を使う (従って debug の殆ど不可能な) シミュレーションに計算費をかけて乗り出す事は「蛮勇」としか言えない. 当然我々はこのような擬似乱数 pseudorandom number だけを考える.

擬似乱数の発生にも歴史的には沢山のアイデア [1),2),3),4),6)] が記され, 現在も新たに提案されている. これからも次々に新しい方法が発見されるだろう. ただ確実な事として, 一般に独立乱数系列発生法は, 始めにも触れたように, まず $0 \leqq u \leqq 1$ の区間に一様に分布した一様乱数の列 $\{u_k;\ k = 0, 1, 2, \cdots\}$ の生成から出発するという事は言える. 他の色々な確率分布の乱数はこの一様乱数からそれぞれ解析的な変換で得られるからである. 変換はある意味で微積分学の応用で, それらにも目覚ましいアイデアは沢山あって多くの話題に事欠かないが, 計算機上での変換計算が含む問題は少なく, 必要な時に個々に理解するのにさほど困難もない. 我々はそれは置いて, より大掛かりで体系的な努力が理解に求められる一様独立的な乱数列, 中でも「高精度乱数列」の高速生成方法に集中する.[6]

独立性を少し忘れて一様分布だけを考えると, 一様乱数を得るための現在の共通の戦術は, 大雑把に言って 0(或いは 1) から十分大きい整数 m(又は $m-1$) までの間のすべて (或い

[5]「虫」取り, 計算プログラムの誤りの除去.

[6]乱数列の高精度は必ずしもその生成機構の推定の困難とはならない. 通信の大切な実際応用に関連して暗号理論 [7),8),9)] からは乱数に高精度や高速生成とは異なる面から大きな問題提起がある. 以下これには殆ど立ち入らないが, 得られる理解は解読容易な乱数を避ける知識には深く関わる.

は一定の間隔) の整数値を同じ回数, 例えばそれぞれ必ず 1 度しかもすべて 1 度だけ, 取る様な系列 $\{x_0, x_1, x_2, \cdots\}$ を作る事である. それがでたらめな順番 (正確には $j \neq k$ に対する x_j と x_k が統計的に無関係, 独立) に「見える」ように作れれば, それを m で割った $u_k := x_k/m$ として一様且つ独立な乱数列の類似物 $\{u_0, u_1, u_2, \cdots\}$ が得られる事になる. これは現在主として次の 4 種類の方式に基づいて実現されている:

(a) **線形合同法** linear congruential method:

$$x_k = ax_{k-1} + c, \ \ c \neq 0 \pmod{m}.$$

既に登場し, これから頻繁に用いる重要な記号 $\bmod m$ は「m で割った剰余を取る」, 「m を法 *modulus* として考える」, 「*modulo m*」という意味である.

(b) **乗算合同法** multiplicative congruential method:

$$x_k = ax_{k-1} \pmod{m}.$$

形からはこれは線型合同法の $c = 0$ の特別の場合だが, 構造原理の違いが法 m 等によって大きいので, 以下では実際によく用いられる名前を与えて独立に扱う.

(c) **M 系列法** [10),11),12)]:

$$x_k = x_{k-i} \oplus x_{k-j}, \ \ 0 < i < j.$$

ここで $\oplus$ は 2 進表示桁毎の mod 2 での和, 即ち FORTRAN 等での exclusive or, 排他的論理和 XOR であり, この方法は実現の仕方によって feedback-shift-register 法等とも呼ばれる.

(d) **加算生成法** additive generator (lagged Fibonacci 法):

$$x_k = x_{k-i} + x_{k-j} \pmod{m}, \ \ 0 < i < j.$$

(a) で法 m は十分大きい整数, 他の場合共大体において 4 バイト整数の最大値 2^{32} 程度の大きさに取られる. a と c は勿論 m 未満の「適当に (あるいはうまく, さらには正しく)」選ばれた整数で, 特に a は「乗数 multiplier」と呼ばれる. 「うまく」取らなければならない事は, 例えば $a = 1, c = 1$ としても $x_0 = 0, x_1 = 1, x_2 = 2, \cdots$ と 0 から $m - 1$ まで均等に取るが, これではとても独立乱数列とは言えない事からも明らかである.

(b) では m は大きい「素数 prime number」が好ましい. その場合の最長周期乗数 a の選択には上の線形合同法の例えば $a = 1, \ c = 1$ とは見掛けの大いに異なる構造[7]の理解が求められる, 勿論方式 (b) も一枚岩ではなく, m を計算機の仕組に適した $m = 2^r$ の形[8]に取る事もできるが, この場合最長周期条件はまた異なる機構に基づき, さらに出発値の選択に少し注意がいる. 方法 (b) で法 m を大きい素数 (従って奇数) に選ぶ事の 1 つの利点は出発値 $x_0 \neq 0$ の選び方が完全に自由になる所にある. 勿論利点ばかりではなく欠点もある事は後に見られる. いずれにせよ高性能乱数生成方式を得るには「良い乗数 a」を必ず検定 (第 4 章) を経て選ばなければならない.

(c) では方式, 即ち番号の lags(遅れ)i, j の選択と共に, 線形漸化式の出発値 (初期条件) の取り方がこの上なく重要な鍵となる事を我々は見る. 記号 $\oplus$ は説明の通り整数の 2 進表示

[7] しかし数学の広い見方からは, この 2 つの構造はある対応で「同じ形 (同形)」と看做すことも行われる. 勿論その同形を実現する対応 (離散対数) が複雑だからこの変換は trivial なものではない.

[8] 整数 n を $m = 2^r$ で割った余りは n の 2 進数表示の下 r 桁で, それは例えば FORTRAN 等の諸言語では組み込み関数を用いて簡単に得られる. 特に $m = 2^{32}$ の場合, 計算機種によっては 2^{32} を越えた整数は自動的に桁溢れとしてこの余りだけを取るので, さらに経済的に計算できる.

での桁毎に

$$1 \oplus 1 = 0 \oplus 0 = 0, \qquad 1 \oplus 0 = 0 \oplus 1 = 1$$

と計算する「排他的論理和 XOR, exclusive or」である. FORTRAN 等の言語ではこれはわざわざ整数を 2 進表示しなくても 2 つの数の直接 2 項演算として書けるので計算プログラムの実現はたやすい. 取るべき遅れ i, j は「原始多項式」という概念で特徴付けられ, それに基づく乱数が Tausworthe[10], Lewis-Payne[11], 等の研究を経て Fushimi-Tezuka[12] によって完成され, 乱数生成方式の 1 つの核心である. 我々は原始多項式とは何であるか, どうしてそれが存在するかを知り, 各方法の利点と難点を明確にする. 算法 $x_{k-i} \oplus x_{k-j}$ では 2 進表現の下位の桁からの「繰り上がり」はない. この方法も複雑な発展を辿った. ある段階では「性能が最悪, some of the worst of all generators」とまでも酷評された事もある [14] が, これはもはや正鵠ではない. M 系列法は原理的にも実際的にも大変優れた方法の 1 つである事が現在では伏見-手塚の優れた研究によって確立している.

(c) の $\oplus$ の代りに例えば繰り上がり carry のある通常の和 $+$ に取って加算乱数生成方式 (d) ができる. 一般に lagged Fibonacci 法と呼ばれているこの方法は, 特に経験的に計算量 cost の点で優れたものである. ただ生成される乱数系列の性格については, 得られた理論的理解が (Knuth[2] 以来何年も経た現在でも) まだ少ない. 方法が実際的な幾つかの美点を持つと今の所思われる, と言っても, 例えば系列を起動するのに必要になる漸化式の出発 (初期) 値 $\{x_0, x_1, x_2, \cdots, x_{j-1}\}$ や遅れ i, j の取り方について, そしてそれから結果として得られる (例えばモンテカルロ計算の) 精度について, シミュレーションに先立つ (先験的な) 性能の保証が困難で, 他人からの推奨や know-how に頼らなければ確信をもって利用を進めにくい事を意味する. 問題点を回避し, 或いは改良し, 目的精度に合った設計を得るためには構造の見通しは欠かせない. それを自分或いは他人の経験に頼る事の危険は Knuth[2] に様々に述べられている通りで, これはこの方法に残る大きな困難である. しかし一方利用を退ける強い理由とも言い切れない. もどかしい事だが, 幸いこの状況は最近 Lüscher[13] による大きな改善を見た.

議論は以下専ら上の (b)-(d) の 3 方式について進められる; (a) は応用の主流から外れ, (b)-(d) が実際的に現在の, そして展望される将来の乱数発生方法の殆どすべての原理を包含するからである. 我々は抽象的な言葉よりはむしろ多くの例や問題解析を通してこれらの認識に近付こうと思う. しかし方法全体の理論構造の先立つ見通しはやはり重要だから, この場所で触れておこう.

方法の数学的構造として, 一見 (b) は (a) と近く, (c), (d) は (a) や (b) とは掛け離れて見える. 所が, ここが誠に面白いのだが, 実は (b), 特に素数の法の場合, と (c) は大変密接な親近関係があって, それに比べて (a) はかなり遠い. 具体的に言うとその場合の (b) は数学的には「素数の $m = p$ を法とする整数の作る体 $\boldsymbol{Z}_p$ に伴われる乗法群の巡回性」と言うものを基礎とし, (c) は「体 $\boldsymbol{Z}_2 =: \mathrm{GF}(2)$ の j 次拡大体 $\mathrm{GF}(2^j)$ の乗法群の巡回性」という近い構造の上に立つ. 我々はこれら「群」や「体」などの代数系の山々のふもとをゆったりと散策したい. いや, 山のように頂きに近付けば高く狭くなるというよりは大洋のように進むほどに水平線がさらに彼方へ霞む世界だろうから, 乱数生成という具体的な問題を櫂や帆への風にしてこれらの事柄へ舟出したい, 内海の概観を得て, そこから多様な外海航路の見通しが得られればと思う. 数学としては群 group, 体 field, そして一部 (d) に関連して環 ring, というものが登場する.

まえおきの最後に, コンピュータ上の乱数生成という限定に伴われる方式の重大な要件に触れよう. コンピュータ上では, 整数は勿論実数であろうと, すべて有限の状態しか表す事はできない. たとえば単精度実数は, 言語や方式によらず, 高々4 バイト=32 ビットに相当する 2^{32} 個の状態, 従って同じ個数の数値 (通常 10 進有効桁数で高々7 程度の有限小数) しか取れない. 乱数生成方式はすべて 1 つ前の, 或いは現在からの一定の遅れ (lag)j 前までの系列の状態で次の乱数が決定される. この j 以前までの系列の状態の総数も高々有限の $(2^{32})^j = 2^{32j}$ 個しかないから, 結局コンピュータが生成する乱数系列は, たとえ実数に基づくどんな方式を用いようと, 必ず有限回の発生後再び同一の初期状態を再現し, それ以後は系列は以前と同じ道を辿る. コンピュータ上では乱数系列は必ず有限の周期を持つのである. シミュレーションを行うには, だから, 使用する乱数の周期を知りシミュレーションがその周期を使い切る恐れがない事を先立って確かめなければならない. この点で実数に基づく乱数発生方法は大変厄介である. 例えば logistic map として知られる変換[9]

$$x_k = f(x_{k-1}),\ \ f(x) := 4x(1-x)$$

は $0 \leqq x_0 \leqq 1$ の殆どすべての (正確には不変測度に関して測度 1 の) 出発値 x_0 に対してこの区間を稠密に覆って動くエルゴード的な非周期的な系列を生成する. しかし, それは無限の桁数を持つ実数で考えての話である. 計算機上でこの方式をどの様に実現しようと, 上に記した通り有限個の状態しか取れず, 有限のステップの後には同じ初期値, 例えば x_0 が再現し, 必ず有限の周期が生じる.[15] 周期 T の存在は T が十分大きければ構わない. しかし具合の悪い事に T は乱数系列の初期値 x_0 と計算機諸言語では明確には規定されない実数計算での丸め方や打ち切り方, 或いは桁あふれや桁落ちの捌き方にも依存する. 計算機を変えれば同じ出発値でも異なった周期となる事は避けられない; これは portability の欠如である. だからシミュレーションを行うためには, 乱数の出発値と計算機の機種毎に予めその周期がいくらになるか, まず確かめて掛からなければならない. そんな暇は普通シミュレーションに際してはほぼ確実に存在しない. これは実用を不可能にする障害である. 計算機上の乱数生成機構が整数演算に限定される理由を理解しよう; この限定によって, 計算機種や言語にもよらない再現性と, 計算に先立つ周期の見通しが保証されるのである.

整数の中だけでの演算は実数や複素数に比べて大変制限が強い. それにも関わらずなのか当然と言うべきか, 実数や複素数の自由だが特徴のない演算とは異なって, 整数の算術ではそれぞれの数が大変個性的な, それでいて一般性のある美しい性質を示す. この体験を我々は貴重なものとして得る事になろう.

[9]既にも用いたが, 下で $f(x) := 4x(1-x)$ はコロンの付いた側の $f(x)$ を反対側の式で定義する, という意味である. これからできるだけこの約束 (定義) に従う. なおこの変換で不変な $0 \leqq x \leqq 1$ 上の分布密度関数, 不変測度, いわゆる定常分布, は一様分布ではなく一様乱数にするには滑らかな変数変換を経なければならないが, これは実数変換に基づく乱数生成方式一般での周期問題 [15] の本質を変えるものではない.

1. 整数の合同算法

1.1. 法 m の算法, 合同算法

算術の腕慣らしと問題の所在の見当付けのために暫く (b) の乗算合同法を軸に取る. 法 m, $\bmod m$ の算法は「合同算法」と呼ばれる. この再定義から始めよう:

定義 1.1. 整数 x, y について $x-y$ が m で割り切れる事, 即ち $x-y$ が m の倍数である事を「x と y は m を法 (*modulus*) として合同」と言い, $x = y \pmod m$, $x \equiv y \pmod m$ (Gauss の記号), 或いは単に $x \equiv y$ と記す. **(定義 1.1. 終り)**

以下普通の四則演算の等式を=で, 合同は $\equiv \pmod m$ で, それぞれ示すが, 工学文献では $=$ だけとする傾向があり, 混乱しなければ記法としては簡単なので最終的にはそちらに移行する. 定義 1.1. と今まで用いた「m での剰余」による定義との同値を確認しよう:

Corollary 1.2. 整数 x, x' について上の $x \equiv x' \pmod m$ と「x と x' とが m で割って等しい余りを持つ」事とは同値である.
(証明) $x = mq + r,\ x' = mq' + r',\ 0 \leqq r, r' \leqq m-1$ とする; $r^{(\prime)} = x^{(\prime)} - mq^{(\prime)}$ とすれば明らかなように q, q' は x, x' を m で割った商 quotients, r, r' は余り remainders,[10] $x - x' = m(q-q') + (r-r')$ である. ここで $-m+1 \leqq r-r' \leqq m-1$ だから, $x-x'$ が m で割り切れる事と $r-r'=0$, 「m で割った余りが等しい事」, とは同値である. ■

確かに, 定義 1.1. の「法 m での合同」は m で割った余りによる整数全体の m 個のクラスへの類別 (「同じクラスの元は同等, 同一」とする) である.[11] 具体的な例, $\bmod 7$ で考えよう. 整数の全体 $0, \pm1, \pm2, \cdots$ はつぎの 7 つのクラスに分かれる:

$$
\begin{array}{lllllll}
\cdots, & -14, & -7, & 0, & 7, & 14, & \cdots, \quad 7k+0 \equiv 0 \pmod 7 \\
\cdots, & -13, & -6, & 1, & 8, & 15, & \cdots, \quad 7k+1 \equiv 1 \pmod 7 \\
\cdots, & -12, & -5, & 2, & 9, & 16, & \cdots, \quad 7k+2 \equiv 2 \pmod 7 \\
\cdots, & -11, & -4, & 3, & 10, & 17, & \cdots, \quad 7k+3 \equiv 3 \pmod 7 \\
\cdots, & -10, & -3, & 4, & 11, & 18, & \cdots, \quad 7k+4 \equiv 4 \pmod 7 \\
\cdots, & -9, & -2, & 5, & 12, & 19, & \cdots, \quad 7k+5 \equiv 5 \pmod 7 \\
\cdots, & -8, & -1, & 6, & 13, & 20, & \cdots, \quad 7k+6 \equiv 6 \pmod 7
\end{array}
$$

整数を 7 で割った余りは集合 $T = \{0,1,2,3,4,5,6\}$ のものだけだから, 上の「同値関係」の代りに整数全体を T のものだけと看做し, $\bmod 7$(もっと一般に $\bmod m$) での加減乗法をそれらの間の新種算法とする見方も用いる事ができる. しかしこの後者の見方への限定はあまり便利ではない. 乱数問題では多くの合同算法を駆使しなければならず, それには整数全体の同値関係での類別というもっと柔軟 flexible な立場の方が具合がよい. 実際そこで必要となる算法規則は簡明である:

[10] 余り r, r' の定義は後にはもっと一般化して $-m+1 \leqq r, r' \leqq m-1$ を満たす任意のもの, と取る事もある.
[11] 数学的には法 m での合同 $\equiv$ が「同値関係」の 1 つであり, (1) $a \equiv a$, (2) $a \equiv b$ なら $b \equiv a$, (3) $a \equiv b$ かつ $b \equiv c$ なら $a \equiv c$, が成り立つ事を付言すべきだが, これらは自明だろう.

Lemma 1.3. 文字はすべて整数を表すとして:
(a) $a \equiv a',\ b \equiv b' \pmod m$ ならば

$$a \pm b \equiv a' \pm b \equiv a \pm b' \equiv a' \pm b' \pmod m,$$

$$ab \equiv a'b \equiv ab' \equiv a'b' \pmod m.$$

(b) まとめれば, **加減乗法での合同算法では任意の計算段階でどの整数をそれと合同なもので置き換えても結果は同じ**である.
(証明) (a) $a \equiv a' \pmod m,\ b \equiv b' \pmod m$ であるから

$$a - a' = mr,\ \ a = a' + mr;\ \ b - b' = ms,\ \ b = b' + ms$$

となる整数 r, s が存在する. 故に, 例えば

$$a \pm b = (a' + mr) \pm b = a \pm (b' + ms) = a' \pm b + (m \text{の倍数}) = a \pm b' + (m \text{の倍数}),$$

即ち $a \pm b \equiv a' \pm b \equiv a \pm b' \pmod m$. 他の合同式も同様に成り立つ. 積についても

$$ab = (a' + mr)b = a'b + mrb = a'b + (m \text{の倍数}) \equiv a'b \pmod m.$$

他の合同式も同様.
(b) 整数を表す文字ばかりでできた整式 P を計算するとしよう. P の中の任意の整数 a(a が P に 2 つ以上含まれるならその任意の 1 つを取って考える) から見れば $P = ba + c$ の形, b, c は整数, としてよい. だから上の通り $a = a' + mr$ とすれば

$$P = ba + c = b(a' + mr) + c = ba' + c + bmr \equiv ba' + c \pmod m.$$

即ち P の中の任意の整数 a をそれと合同な a' で置き換えても法 m では同じである. b, c の中に残る他の a や他の整数についても同様だから命題は成り立つ. ■

要約すれば, 「法 m の加減乗法の計算では, 途中で出てくる数を法 m で合同な任意のものに置き換えて計算を簡単にしてよい」のである. この簡単だが極めて有用な知識の 1 つの重要な果実を, 計算機上の算術で大切な 2 進計算への導入と共に得よう. 普通整数 n は 10 進で表現される. 例えば

$$2713 = 2 \times 10^3 + 7 \times 10^2 + 1 \times 10^1 + 3 \times 10^0$$

である. 2 進では数字としては 0 と 1 しか用いず, 数を $0, 1, 10, 11, 100, \cdots$ と数え上げる. 具体例で言うと 1101001.01 が 2 進数なら, それを明確にする様に $(1101001.01)_2$ と記し次の数を表す:

$$(1101001.01)_2 := 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^3 + 1 \times 2^0 + 1 \times 2^{-2}$$

$$= 64 + 32 + 8 + 1 + \frac{1}{4} = 105.25.$$

2 進小数点の上の第 j 桁は 2^{j-1} の数を, 小数点の下の第 j 桁は 2^{-j} を表す事に注意しよう. 10 進表示では 10 が, そして 2 進表示では 2 が, それぞれ表現の基数 base と呼ばれる. 上で 10 進, 2 進について見たのと同様に, 任意の基数 b を用いる b 進数では一般に次が成り立つ:

b 進数の小数点の上或いは下の第 j 桁はそれぞれ b^{j-1}, b^{-j} を表す.

さて計算機内部では機構的に全ての数は 0,1 の 2 状態に基づいて表される事が多く, そこでは正の整数の 2 進表現が最も自然で, それに伴って負の整数の「補数表示」が導入される. 要点は計算機では整数に対して有限の桁数しか許容できない事の利用にある. 具体的に整数 n を 2 進の 8 桁迄, $0 \leqq n < 2^8$ の範囲, を記憶できるが, $n = 2^8$ になると $n = 0$ としてしまう (桁溢れの処理の 1 つの) 方式の計算機を考えよう. この計算機は整数を法 $m = 2^8$ で扱っている. 対応する演算設計では扱う正の整数 n を $0 \leqq n < 2^7$ の 2 進 7 桁迄のものに制限して 8 桁の一番上のビット the most significant bit が 0 の時は正の整数を表すと約束する. また一般に $1 \leqq n < 2^7$ を満たす正の整数 n に対して[12]

(1) n の各ビット $0, 1$ を反転した「(法 2^8 での)1 の補数 $n' := (11111111)_2 - n$」と,

(2)「(法 2^8 での)2 の補数 $n'' := n' + 1$」とを定義し,

負の数 $-n$ は計算機内では n の 2 の補数 n'' として (レジスターと呼ばれる記憶装置に) 格納する. $-n$ を表す 1 の補数 n' 或いは 2 の補数 n'' は 2 進 8 桁で共に先頭ビットは必ず 1 で, これが負数である事の旗印になる. 正の整数 n の補数で負の数 $-n$ を保持する事の有利さは次の問題から理解される:

問題 1.4. 一般に法 2^r(の計算機内) で, 整数 m から正の整数 $1 \leqq n < 2^{r-1}$ を引く事は m に「(法 2^r での)n の 2 の補数 n'' を加えて」実現され, また任意の整数 m に $-n$ を掛けた結果は法 2^r では m に n の 2 の補数 n'' を掛けて正しく得られる. これらを示せ.

(証明) 法 2^r で表される最大の正の整数 $N = 2^r - 1 = (111\cdots1)_2$ を取る; ここで ( ) 内の 1 は r 個続く. $1 \leqq n < 2^{r-1}$ を満たす整数 n は 2 進 $r-1$ 桁以下で表せるからそうすると, $N + 1 - n = \{(111\cdots1)_2 - n\} + 1$ は「(法 2^r での)n の 2 の補数 n'' そのもの」である. さて, $N + 1 = 2^r$ は法 2^r では加減乗法 (の計算の任意の段階) で無視してよい; 我々の得た表記法では $-n \equiv n'' \pmod{2^r}$ である. 故に

$$m - n \equiv m + n'' \pmod{2^r}, \quad m \times (-n) \equiv mn'' \pmod{2^r}. \qquad \blacksquare$$

1.2. 合同算法と整数係数多項式

数の合同算法自体は前節の結果から簡明だが, 計算の構造や結果を見通す上では我々が早くから学び上でも 1 部分で使った様に「数に代る」文字を使って「代数的に」考える事が重要になる. 基本的には事柄はごく単純に見えて, 前節の結果から次が成立する:

Corollary 1.5. $f(x, y, z, \cdots)$ は文字 $x, y, z, \cdots$ の整数係数多項式, m は正の整数とする. 法 m で $a \equiv a'$, $b \equiv b'$, $c \equiv c'$, $\cdots$ なら次が成り立つ:

$$f(a, b, c, \cdots) \equiv f(a', b', c', \cdots) \pmod{m}.$$

即ち法 m では, 整数係数多項式の整数値変数での値はその計算の任意の段階で任意の変数や係数をそれぞれに合同な他の整数で置き換えても同じ結果になる. $\blacksquare$

しかし意外にも, これらに基づく代数計算では我々の「常識」からかけ離れた事態はごく

[12] ここでは正の整数だけをある法の下で考えているが, 整数 n の補数の定義は正の整数 n に, 或いは特定の法の下に限るものではない.

普通に生じる. 詳しく考えよう.

まず法 m での算術を考える. 法 m で $ab \neq 0$ なら $a \neq 0$ かつ $b \neq 0$ である事, その対偶として a 或いは $b \equiv 0 \pmod m$ なら $ab \equiv 0$ はどんな法 m についても常に成り立つ. これは「m の倍数かどうか」を考えれば容易に見られる. しかしこれらの逆命題は必ずしも正しくはない. 例えば $m = 6$ を法とすると, 2 や 3 は 0 と合同ではない (6 の倍数ではない) が $2 \times 3 = 6 \equiv 0$; 「$xy \equiv 0$ なら x 又は $y \equiv 0$」も対偶の「$x \neq 0$ かつ $y \neq 0$ なら $xy \neq 0$」も一般には成り立たない. だから法 m が「素数」の場合の事態の簡単化は特筆しなければならない:

Lemma 1.6. 整数 $m \geqq 2$ が自明な 1 と m 以外に約数を持たないとき素数 prime と呼ぶ. **素数に 1 は含めない**. 素数 p を法とすると次が保証される:
(a) $ab \equiv 0$ なら, $a \equiv 0$ 或いは $b \equiv 0$ である.
(b) $a \not\equiv 0$ 且つ $b \not\equiv 0$ なら, $ab \not\equiv 0$ である.
(c) $ab \equiv ac$ で $a \not\equiv 0$ なら $b \equiv c$ である. 即ち $a \not\equiv 0$ での除法が可能である.
(証明) (a) $ab \equiv 0$, 言い換えると ab が p の倍数なら, 素数 p は 2 つ以上の因数に分けられないから, a または b が p の倍数, 即ち $a \equiv 0$ 或いは $b \equiv 0$.
(b) 上の (a) の対偶として $a \not\equiv 0$ かつ $b \not\equiv 0$ なら $ab \not\equiv 0$. これは直接にも「a も b も素因数 p を含まなければ ab は素数 p の倍数ではあり得ない」と考えても納得される.
(c) $a(b-c) \equiv 0$ なら, (a) によって $a \equiv 0$ あるいは $b - c \equiv 0$ だが, $a \not\equiv 0$ なので $b - c \equiv 0$ 即ち $b \equiv c$ でなければならない. ■

この様に, 法 m が素数の場合と合成数の場合とでは算術演算の結果に非常に大きな隔たりがあり得る. これは定義された合同算法の与える数体系が「体」というものになるか, それともそれほど性質の良くはない「環」にとどまるかという違いから生じると後に把握されるけれど, この段階でその様な道具立てを持出すのは必要でも得策でもない. ただ, この差異を認識し, そして各時点での命題がどちらに関するものか, を常に明確に意識して進む事は大切なので, 以下では可能な限り素数の法の場合には上と同様に「法 p」の用語を, その限定がない場合には「法 m」の表記を当てる事にする.

整数係数の多項式 $f(z)$ に向かう. 変数 z が整数の場合の f の値の法 m での合同算法の目的からは次の定義は必然である:

定義 1.7. (a) 整数係数の多項式 $f(z),\ g(z)$ はすべての係数が法 m で等しい時「法 m で合同, $f(z) \equiv g(z) \pmod m$」と言う. 言い換えると, $f(z) \equiv g(z) \pmod m$ とは差 $f(z) - g(z)$ のすべての次数の z の係数が法 m で 0 に合同な事で定義され, それは $f(z) - g(z) \equiv 0 \pmod m$ とも記される.
(b) 特に整数係数多項式 $f(z)$ の係数は法 m で 0 ではないものだけを考え, 0 ではない係数を持つ z^j の j の最大値を「$f(z)$ の法 m での次数 $\deg\{f(z)\}$」と定義する. **(定義 1.7. 終り)**

しかしこの定義下で, 一般の法 m での数を係数とする多項式では奇妙な (と見える, 実はこちらの方が一般の) 事が起きる:

例 1.8. 法 8 では整数全体は $\{0, 1, 2, 3, 4, 5, 6, 7\}$ で代表される. これらの 2 乗を計算すると

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 \equiv 1,$$

$$4^2 \equiv 0, \quad 5^2 \equiv 1, \quad 6^2 \equiv 4, \quad 7^2 \equiv 1.$$

だから法 8 では 2 次方程式 $z^2-1=0$ の解が 4 つある. これはまた 2 次式 z^2-1 が法 8 で次の 2 通りの因数分解:

$$\begin{aligned} z^2-1 &\equiv (z-1)(z-7)=z^2-8z+7 \\ &\equiv (z-3)(z-5)=z^2-8z+15 \pmod 8 \end{aligned}$$

を持つ事を意味する. 2 通り所ではない; 次の成立も容易に見られる:

$$z^2-1\equiv(3z-1)(3z-7)\equiv(5z-3)(5z-5)\equiv\cdots \pmod 8.$$

素数でない法で係数を考えると整式は因数分解の一意性を保証されない. これは代数方程式の解の中に多項式の 1 つの因数分解で各因数を 0 にはしないのものもあり得る事に対応する. 上の例で言えば, 因数分解 $(z-1)(z-7)=0$ には $z-1=2,\ z-7=4$ 即ち $z=3$, 或いは $z-1=4,\ z-7=6$ 即ち $z=5$ の解もある, という複雑さになる. **(例 1.8. 終り)**

例 1.9. 法 6 では 1 と 5 だけが (法の数 6 とは共通因数を持たず) それぞれ逆数 (掛け合わせて法 6 で 1 になる数)$1^{-1}=1,\ 5^{-1}=5$ を持ち, 従って例えば $5a\equiv 5b$ なら $5(a-b)\equiv 0,\ a-b\equiv 5^{-1}0=0$ で $a\equiv b$ でなければならない. 一方 2,3,4 には掛け合わせて 0 になる奇妙な相手, それぞれ 3,2,3, がある. だから例えば $2a\equiv 2(a+3)$ の様な事が起き, 次も成り立つ:

$$2z^2+2z+2\equiv(2z-2)(z+2)\equiv(2z-2)(4z+5) \pmod 6.$$

言い換えると, 法 6 の計算では $2z^2+2z+2$ を $2z-2\equiv 2z+4$ で割るとき, 法 6 の意味でも商は一意ではない. また, z^2+z+1 は $2z-2$ では割る事ができない. **(例 1.9. 終り)**

素数の法 p ではこの様な事は起きない; 整数係数の多項式の因数分解は係数の法 p での合同の意味でただ一通り, 一意である. 上の例が示す様にこれは決して自明ではなく証明による確認が強く求められる. 少しだけ一般化した次の事柄から始めよう.

Corollary 1.10. 任意の整数 $m>0$ を法として, 整数係数の n 次多項式 $f(z)$ と $z-a$, a も整数, を考えれば, 次の「除法の等式」が成り立つ:

$$f(z)\equiv(z-a)q(z)+r \pmod m.$$

ここで整数係数 $n-1$ 次多項式の商 $q(z)$ と 0 次の定数の余り r は法 m で一意である.

(証明) 割る $z-a$ の z の係数が 1 だから, 任意の整数の法 m でも, 例えば $f(z)$ の最高次項を cz^n で $c\not\equiv 0,\ n\geqq 1$ とすれば, $f(z)-cz^{n-1}(z-a)$ は必ず $n-1$ 次以下の整数係数多項式になる. 割られる式の次数を低下させる様に「商」として立てる $n-1$ 次の cz^{n-1} の係数 $c\not\equiv 0$ は法 m の意味で一意である. これで以下, $z-a$ による割り算は普通の実数や複素数の場合と同様に法 m の整数係数の範囲でただ 1 通りに進む. 商の係数として法 m で同値な数をどう選ぼうと, その選択は係数の加減乗法で順次定まる他の係数や最後の余りには「法 m の意味で」影響を与えない; 整数の加減乗法では法 m での還元を計算のどの段階で取っても結果には影響しないからである. 言葉では見えにくいから法 8 の例で考えよう.

$$\begin{array}{rr|ll} & & 3z+1 & \\ \cline{3-3} z-2 &) & 3z^2+3z+1 & \cdots\ f(z) \\ & & \underline{3z^2-6z} & \cdots\ 3z\times(z-2) \\ & & z+1 & \cdots\ f(z)-3z\times(z-2) \\ & & \underline{z-2} & \cdots\ 1\times(z-2) \\ & & 3 & \cdots\ f(z)-(3z+1)\times(z-2) \end{array}$$

このように, 整数係数の割り算は割る 1 次式 $z-a$ より低次の定数 r が残る段階までただ一通りに進み, 余りの表現 $r=f(z)-$ 商 $\times(z-a)$ が得られる. 即ち除法の等式が法 m で一意な整数係数多項式である商 $q(z)$ と整数の余り r の間に成り立つ. ■

上の事柄の成立には割る式が $z-a$ である事, より一般には「最高次の係数が 1 の整数係数多項式である事が本質である. この「$f(z)$ の最高次の係数が 1」を特別に「$f(z)$ はモニック monic である」と言い表す. Corollary 1.10 は馴染み深い 2 つの命題を与える:

Corollary 1.11. (任意の整数の法 m での剰余の定理) 任意の整数の法 m で整数係数多項式 $f(z)$ を $z-a$ (a も整数) で割った余り r(定数, 0 次式) は $r\equiv f(a) \pmod m$ である.
(証明) Corollary 1.10 の割り算の等式で $z=a$ とすればよい. ■

Corollary 1.12. (任意の整数の法 m での因数定理) 任意の整数の法 m で整数係数多項式 $f(z)$ が $z-a$(a も整数) で割り切れる必要十分条件は $f(a)\equiv 0 \pmod m$ である.
(証明) 剰余の定理から明らか. ■

整数係数多項式 $f(z)$ が法 m で 2 つ以上, それぞれ 1 次以上の整数係数多項式の積に分解される時 $f(z)$ は「法 m で可約, 約分 (因数分解) 可能」と言い, その様に分解されない時「法 m で既約, 約分 (因数分解) 不可能」と言う. さあ, 法を素数 p に限って整式の合同算法での因数分解の次の意味の一意性を見よう.

定理 1.13. 素数の法 p で n 次の整数係数代数方程式 $f(z)\equiv 0$ の整数解は, 解の重複度を数えても法 p の意味で高々 n 個である.
(証明) $f(z)\equiv 0$ の整数解 $z\equiv a$ は上の因数定理 Corollary 1.11 によって $f(z)\equiv(z-a)g(z)$, $\deg\{g(z)\}=n-1$ を与える. 同様に $g(z)\equiv 0$ の整数解 $x\equiv b$ は $g(z)$ にも 1 次因数 $z-b$ を与え, $f(z)\equiv(z-a)(z-b)h(z)$, $\deg\{h(z)\}=n-2$ が成り立つ. 以下同様に繰返して $f(z)\equiv 0$ の m 個の解の 1 組 $\{a,b,\cdots,e\}$(これらの中には重解に相当して同じものがあるかもしれない) がある $m\leqq n$ に対して存在して, 因数分解を次の形まで進める事ができる:

$$f(z)\equiv(z-a)(z-b)\cdots(z-e)k(z). \tag{1.1}$$

$k(z)$ は整数根を持たない整数係数多項式[13]か, 或いは定数である. ここまでは法が素数でなくてもよいが法 p が素数である事はさらに m 個の $\{a,b,\cdots,e\}$ 以外の解は存在しないと保証する. 背理法で示そう. 仮に法 p で $\{a,b,\cdots,e\}$ とは異なる $f(z)\equiv 0$ の整数解 a' があるとすれば,

$$0\equiv f(a')\equiv(a'-a)(a'-b)\cdots(a'-e)k(a')$$

が成り立つが, 右辺は素数の法 p で 0 に合同ではない因数の積として 0 に合同ではあり得ず, 矛盾である. 素数の法 p では n 次整数係数多項式の根は n 個以下でなければならない. ■

一般に素数の法 p では整数係数多項式の既約因数分解は第 8.1. 節で説明される様に一意である.[16),17),18)] この事を使えば上の定理は遙かに透徹し, 証明も簡潔透明になる. これは下の Lemma 1.14.(c) についても同様である. しかし事柄は少し大掛かりな準備を要するので,

[13] $k(z)$ は法 p の範囲でもはや因数分解できない整数係数多項式 (法 p で既約な 2 次以上の整式) あるいはそれらの積である. 法が素数でなければ $k(z)$ としては 1 次式もあり得る; 例えば偶数の法での $k(z)=2z+1$ 等. 素数でない法では事柄はややこしい! しかし素数の法 p では整数係数 1 次方程式 $az+b\equiv 0, a\not\equiv 0, \pmod p$ は必ず整数解 $z\equiv -a^{-1}b$ を持つので $k(z)$ に 1 次の場合はない (次章参照).

ここでは初等性を優先し一般性は後に回して上の限定の強い結論や下の少し冗長な証明で止め, いくつかの有用な結果を付加して次へ移る.

Lemma 1.14. モニックな n 次 ($n \geqq 2$) の整数係数多項式

$$f(z) = z^n + b_1 z^{n-1} + b_2 z^{n-2} + \cdots + b_n$$

を考える.
(a) $f(z)$ が整数の範囲で因数分解可能なら, 任意の整数の法 $m > 0$ でも可約である.
(b) $f(z)$ がある整数 $m > 0$ を法として既約なら, 整数 $\boldsymbol{Z}$ の範囲でも $f(z)$ は既約である.
(c) **(アイゼンシュタイン Eisenstein)** 係数 $b_i,\ (1 \leqq i \leqq n)$ がすべて素数 p で割り切れ, しかも定数項 b_n が p^2 では割り切れなければ, $f(z)$ は整数係数で既約である.
(証明) (a) 整数係数多項式 $f(z)$ が 2 つの整数係数多項式 $g(z)$ と $h(z)$ の積に因数分解されるなら, $f(z)$ の最高次係数が 1 だから $g(z)$ と $h(z)$ もモニックで任意の整数の法 m で考えて $f(z), g(z), h(z)$ は 1 次以上である. 法 m での整数係数の算出は整数で普通に計算して最後に法 m を考えてよかった. だから因数分解 $f(z) = g(z)h(z)$ は法 m の意味でも成り立ち, $f(z)$ はすべての法 m で可約である.
(b) 上の (a) の対偶である.
(c) 係数に対する仮定から $f(z) \equiv z^n \pmod{p}$ である. 背理法を使い, 矛盾を導く様に $f(z)$ の整数の範囲での可約性, 2 つの 1 次以上の整数係数多項式 $g(z),\ h(z)$ による因数分解 $f(z) = g(z)h(z)$ を仮定すると, $g(z), h(z)$ はモニックで法 p でも $z^n = g(z)h(z) \pmod{p}$ となる. 故に $g(z) = z^j + \cdots + \alpha$, $h(z) = z^{n-j} + \cdots + \beta$ の形であり, $f(z) = g(z)h(z)$ の定数項は $\alpha\beta = 0 \pmod{p}$ だが, 素数 p の 2 乗はこの項を割り切れず α 又は β の一方だけが p の倍数である. 一般性を失う事なく p は β の方を割り切り α は p を含まないとしてよい. すると $h(z) = z^{n-j} + \cdots + \gamma z \pmod{p}$ で, $f(z) = g(z)h(z)$ の法 p での最低次項は $\alpha\gamma z$ である. これは法 p で 0, α は p では割り切れないから γ が p を含む. この議論は続き, 最後に αz^{n-j} が積 $f(z) = g(z)h(z)$ の法 p での最低次の, しかも法 p で 0 ではない項として残る. これは $f(z) \not\equiv z^n \pmod{p}$ となる矛盾であり, 可約性 $f(z) = g(z)h(z)$ の仮定から生じたもので, $f(z)$ は整数係数で可約ではあり得ず既約である. ■

問題 1.15. 整式 $f(z) = z^3 + 311z^2 + 6728z + 58343$, $g(z) = z^6 - 3z^5 + 12z^4 + 36z^2 - 102z + 312$ は整数係数で既約かどうか判定しなさい.
(解) 素数の法 2 で考えると $f(z) \equiv z^3 + z^2 + 1$ で計算してよい. $f(z)$ はモニックな 3 次式だから, 法 2 の整数係数で因数を持つとすれば必ず 1 次因数 $z - a$ を整数 $a \in \boldsymbol{Z}_2$ に対して含み $f(a) \equiv 0 \pmod{2}$ のはずである. しかし $f(0) \equiv 1,\ f(1) \equiv 3 \equiv 1$ はすべて 0 ではないから $\boldsymbol{Z}_2$ で $f(z)$ は既約で, Lemma1.14.(b) によって $f(z)$ は整数係数でも既約である.
$g(z)$ はその 5 次以下の係数は素数 $p = 3$ の倍数だが定数項 312 は $p^2 = 9$ で割り切れない. 故にアイゼンシュタインの判定で $g(z)$ は整数係数で既約である. **(問題 1.15 終り)**

1.3. 演習問題

定義や命題の確実な理解, そして次に待つ構造の概観を得るためにいくつかの演習を経由する. 主文中に問題を置くことは記述の連続や緊迫を幾分損なうが, 節の終りのひとまとめ

の問題と本文の間を往復するよりは理解の進みが滑らかと思われるので, 我々は演習問題を議論の展開の中に置くことを避けない.

問題 1.16. (a) 任意の数は 2 進数として表示できる. 365 を 2 進表示せよ.
(b) 0.2 を 2 進表示せよ.
(c) $365 \div 2^6$ を 2 進表示せよ.
(d) 一般にある数の 2^n での乗除は 2 進表示のどの様な操作になるか.
(e) 16 進表示では例えば

$$10 = (\mathrm{a})_{16},\ \ 11 = (\mathrm{b})_{16},\ \ 12 = (\mathrm{c})_{16},\ \ 13 = (\mathrm{d})_{16},\ \ 14 = (\mathrm{e})_{16},\ \ 15 = (\mathrm{f})_{16}$$

と表す事はよく知られている. 46538.3 を 16 進表示せよ.
(解) (a) $365 \div 2 = 182$ 余り 1 の関係は, $365 = 182 \times 2 + 1 = 1 \times 2^0 + (2^1 \text{ 以上})$ を意味するから, この 2 での割り算を縦に繰り返し, 各段階での余りを右に書けば, 次が得られる:

$$\begin{array}{rrl} 2 & \underline{)365} & \cdots\ 1 \times 2^0 \\ 2 & \underline{)182} & \cdots\ 0 \times 2^1 \\ 2 & \underline{)91} & \cdots\ 1 \times 2^2 \\ 2 & \underline{)45} & \cdots\ 1 \times 2^3 \\ 2 & \underline{)22} & \cdots\ 0 \times 2^4 \\ 2 & \underline{)11} & \cdots\ 1 \times 2^5 \\ 2 & \underline{)5} & \cdots\ 1 \times 2^6 \\ 2 & \underline{)2} & \cdots\ 0 \times 2^7 \\ 2 & \underline{)1} & \cdots\ 1 \times 2^8 \\ & 0 & \end{array}$$

勿論, 普通はこの最後の 0 を立てる部分は記さない. 結果は

$$\begin{aligned} 365 &= 1 \times 2^8 + 0 \times 2^7 + 1 \times 2^6 + 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 \\ &= (101101101)_2. \end{aligned}$$

最後の表現は縦組み割り算の余りの列を下から上に記して得られる.
(b) 自明な $0.2 \times 2 = 0.4,\ 0.4 \times 2 = 0.8,\ 0.8 \times 2 = 1.6,\ \mathit{0.6} \times 2 = 1.2,\ \cdots$ は次を意味する:

$$\begin{aligned} 0.2 &= 0.2 \times 2 \times 2^{-1} = 0.4 \times 2^{-1} = 0 \times 2^{-1} + 0.8 \times 2^{-2} \\ &= 0 \times 2^{-1} + 0 \times 2^{-2} + 1.6 \times 2^{-3} \\ &= 0 \times 2^{-1} + 0 \times 2^{-2} + 1 \times 2^{-3} + 1.2 \times 2^{-4} \\ &= \cdots\cdots\cdots. \end{aligned}$$

つまり小数点以下の数の 2 進表示は 2 倍 2 倍を続け, 出てくる整数部分 (0 または 1) を 0. 以下並べれば良い. もし同じ小数が再び出ればそこまでの $0, 1$ の並びが循環する. 答は

$$0.2 = (0.0011\ 0011\ 0011\ \cdots)_2 = (0.\dot{0}0\dot{1}1\dot{})_2.$$

これは「小数点以下の数への 2 の縦組みに記した掛け算」で次の様に計算される:

$$\begin{array}{rlll} 2\times & 0.2 & \cdots & 0\times 2^{0} \\ \hline & 0.4 & \cdots & 0\times 2^{-1} \\ & 0.8 & \cdots & 0\times 2^{-2} \\ & 1.6 & \cdots & 1\times 2^{-3} \\ & 1.2 & \cdots & 1\times 2^{-4} \\ & 0.4 & \cdots & 0\times 2^{-5} \\ & 0.8 & \cdots & 0\times 2^{-6} \\ & 1.6 & \cdots & 1\times 2^{-7} \\ & 1.2 & \cdots & 1\times 2^{-8} \\ & \cdots & \cdots & \cdots . \end{array}$$

即ち 2 倍 2 倍して得られる小数点以上の数 (0 または 1) を右に書き, それらを上から順に取れば 2 進の小数点以下が得られる.

(c) 上の問 (a) から

$$\begin{aligned} 365 \div 2^{6} &= 1\times 2^{2}+0\times 2^{1}+1\times 2^{0}+1\times 2^{-1}+0\times 2^{-2} \\ &\quad +1\times 2^{-3}+1\times 2^{-4}+0\times 2^{-5}+1\times 2^{-6} \\ &= (101.101101)_{2}. \end{aligned}$$

(d) 一般に 2^{n} を掛けると 2 進表示の小数点が n 桁下がる (右に移動する; 数自体は左へ移動 shift to the left する). 2^{-n} を掛けると (2^{n} で割ると) 小数点は n 桁上る, 或いは左移動 (数自体は右移動 shift to the right) する.

(e) 2 進表示同様に, 整数部分は 16 による縦組み割り算を下の様に行い, 各段階の余りを右に書き出して次の手続きで得られる:

$$\begin{array}{llll} 16 &)\ 46583 & \cdots & 10=(\mathrm{a})_{16} \quad \times 16^{0} \\ 16 &)\ 2908 & \cdots & 12=(\mathrm{c})_{16} \quad \times 16^{1} \\ 16 &)\ 181 & \cdots & (5)_{16} \qquad \times 16^{2} \\ 16 &)\ 11 & \cdots & 11=(\mathrm{b})_{16} \quad \times 16^{3} \\ & 0 & & \end{array}$$

$$\begin{aligned} 46538 &= 11\times 16^{3}+5\times 16^{2}+12\times 16^{1}+10\times 16^{0} \\ &= (\mathrm{b5ca})_{16}. \end{aligned}$$

0.3 についても 2 進の場合と同じ事で, 小数部分の 16 倍を繰返せばよい:

$$\begin{array}{rrll} 16\times & 0.3 & \cdots & 0\times 16^{0} \\ \hline & 4.8 & \cdots & 4\times 16^{-1} \\ & 12.8 & \cdots & 12\times 16^{-2} \\ & 12.8 & \cdots & 12\times 16^{-3} \\ & \cdots & \cdots & \cdots , \end{array}$$

即ち $0.3=(0.4\mathrm{ccc}\cdots)_{16}=(0.4\dot{\mathrm{c}})_{16}$. まとめて $46538.3=(\mathrm{b5ca}.4\dot{\mathrm{c}})_{16}$. **(問題 1.16. 終り)**

問題 1.17. 整数 $p, n\geqq 2$ に対し $p^{n}-1$ が素数になるためには, $p=2$ かつ n が素数である事が必要だが十分ではない. これを示せ.

(証明) $p^n-1=(p-1)(p^{n-1}+p^{n-2}+\cdots+1)$ だからこれが素数であるためには $p-1=1,\ p=2$ が必要である. 2^n-1 の形の素数をメルセンヌ Mersenne(素) 数と, その指数 n をメルセンヌ指数 Mersenne exponent と言う. 指数 n が合成数で $n=jk,\ j,k\geqq 2$ なら

$$2^{jk}-1=(2^j)^k-1=(2^j-1)\{(2^j)^{k-1}+(2^j)^{k-2}+\cdots\}$$

と因数分解されて 2^n-1 は素数にはなれないから n が素数である事も必要だが, 素数 n は必ずしも Mersenne 指数ではない. 簡単な反例は $2^{11}-1=2047=23\times 89$. ■

問題 1.18. IBM370 システムでは法 $m=2^{31}(=2147483648)$ に取った乗数 $a=65539$ の乗算合同法 $x_{k+1}=ax_k$ (即ち $x_k=a^kx_0 \mod 2^{31}$) が一様乱数ルーチンとして用いられた. 暫くの使用の後に乗数 a が $a=2^{16}+3$ の関係を満たす事が発見されたと言う. この関係から $a^2-6a+9\equiv 0 \pmod{2^{31}}$ が成り立ち, 系列 $\{x_k\}$ は漸化式

$$x_{k+2}-6x_{k+1}+9x_k\equiv 0 \pmod{2^{31}}$$

に従う事を導け. これは乱数系列として大変好ましくないが, 問題の感知の難しさも身につまされる事ではある.

(証明) $2^{16}=1024\times 64=65536$, 故に $a=2^{16}+3$. これから

$$a^2-6a+9=(a-3)^2=(2^{16})^2=2^{32}\equiv 0 \pmod{2^{31}}.$$

故に $x_{k+2}-6x_{k+1}+9x_k=x_k\times(a^2-6a+9)=2^{32}x_k\equiv 0 \pmod{2^{31}}$. ■

次の問題 1.19.(a),(b) は初等的だが, 乱数の乗算合同法の基礎として是非とも 1 度自ら手を動かして計算されるよう要請する.

問題 1.19.(a) 任意の整数は法 7 の乗法に関して集合 $T=\{0,1,2,3,4,5,6\}$ の元で代表される. T の元 x,y の積 xy の結果を 7 を法として (7 で割った余りを取って) 再び T の元で表す乗法を考える. この乗法表 (乗積表) を作れ. また 0 ではない x について, $xy\equiv 1 \pmod 7$ となる y を x の法 7 での逆元, 逆数と呼び x^{-1} と記す. 各 x の逆元も求めて表に記入せよ.

(解)

$x\backslash y$	0	1	2	3	4	5	6	x^{-1}
0	0	0	0	0	0	0	0	
1	0	1	2	3	4	5	6	1
2	0	2	4	6	1	3	5	4
3	0	3	6	2	5	1	4	5
4	0	4	1	5	2	6	3	2
5	0	5	3	1	6	4	2	3
6	0	6	5	4	3	2	1	6

7 で割って余りを取る計算自体は簡単だから困難は少ないが, 結果の次の点は注目に値する.
(i) 上の表で 0 以外の数 x に対する行, 0 を除く y に対する列はすべて, 1 から 6 までの数の並べ変えになっていて, 同じ数は出ていない. 特に各 x に対して $xy=1$ となる y はただ 1 つ必ず存在し, 同様に各 y に対して $xy=1$ となる x も一意に必ず存在して逆元は確定する. この構造の理由は次の章で理解されるだろう.
(ii) $x=6$ の行の規則性は $6\equiv -1 \pmod 7$ で -1 を掛けるのと同じと気付けば明快で, 関係 $6^{-1}\equiv 6 \pmod 7$ も理解される. **(問題 1.19.(a) 終り)**

問題 1.19.(b) 同じ法 7 での乗法に関して, 集合 $T^* = \{1,2,3,4,5,6\} := T - \{0\}$ を定義する. T^* の各元 x の冪 (べき) 乗 $x^n \pmod 7$, $(n = 1,2,\cdots,6)$ を計算して冪乗表を作れ.

(解)

$x\backslash n$	1	2	3	4	5	6	原始根
1	1	1	1	1	1	1	
2	2	4	1	2	4	1	
3	3	2	6	4	5	1	◯
4	4	2	1	4	2	1	
5	5	4	6	2	3	1	◯
6	6	1	6	1	6	1	

上では x^n を計算してから 7 で割って余りを取る必要はない; 計算のどの段階で法 7 で簡約してもよい (Lemma 1.3(b)) のだから, 直前の $1 \leqq x^{n-1} \leqq 6$ の結果に x を掛けて x^n を求めれば十分である. **(問題 1.19.(b) 終り)**

冪乗表では次の点に注目する.

(i) すべての x が上の表で $x^6 \equiv 1$ を与えるから, このあと $n \geqq 7$ に対する冪乗は $n - 6 = 1,2,\cdots,6;\ n - 2\times 6 = 1,2,\cdots$ の結果, 即ち法 6 で n を $0,1,\cdots,5$ に還元した計算での結果の繰返しになる. 言い換えると T^* の任意の数 a が法 7 で作る冪乗の数列では 6 は必ず周期の 1 つである. すべての $x \in T^*$ が $x^6 \equiv 1 \pmod 7$ を与える事はフェルマー Fermat の小定理と呼ばれる. まもなくこの証明を我々は見る.

(ii) T^* の数 x の中には $x = 3,5$ の様に $7-1=6$ 乗して初めて 1 に合同になるもの, 即ち冪乗数列 $\{x^k \pmod 7 | k = 0,1,2,\cdots\}$ の (最短) 周期が実際に $7-1=6$ であるものがある. これらは法 7 での原始根 primitive root と呼ばれ, 冪乗表の右端に ◯ を付けて示してある. 原始根でない x は 6 乗以前に 1 に合同になり, その冪乗数列の法 7 での周期は 6 より小さい. 一般に素数の法 p での冪乗数列の周期は $p-1$ の約数 (今の場合 6 の約数 1,2,3,6) に限られ (ラグランジュLagrange の定理), 原始根による最長周期 $p-1$ を持つものが必ず含まれる.

(iii) $x = 6$ の冪乗の結果は, $6 \equiv -1 \pmod 7$ に注目すればよい. 構造は普通の $(-1)^n$ と全く同じである. これが素数とは限らない法 m でも成り立つ事は 2 項展開 $(m-1)^k = (-1)^k + m$ の倍数 からも容易に理解されるが.

1.4. フェルマーの小定理とオイラーの関数

乱数生成の乗算合同法の殆どすべての内容は上の問題 1.19.(a),(b) に含まれる. そこでは 1 から $m-1 \equiv 6 (\equiv -1 \pmod 7)$ までの T^* のすべての数を $1 \leqq k \leqq m-1$ の範囲のべき (冪) 乗 a^k で掃過 sweep する原始根 $a = 3,5$ があった. 次の簡単な事実に注意しよう:

Lemma 1.20. 一般の素数 p についても $p-1$ 乗して初めて法 p で 1 に合同になる整数を法 p での原始根と言う. 任意の素数の法 p での原始根 a は, もしあるとすれば, $1 \leqq j,k \leqq p-1$ の範囲で $j \neq k$ なら $a^j \neq a^k$, 即ち $a^j - a^k \not\equiv 0 \pmod p$ を満たす.

(証明) 背理法を使う. もし $a^j \equiv a^k$ となるこのような $1 \leqq j < k \leqq p-1$ があれば $0 \equiv a^k - a^j = a^j(a^{k-j} - 1) \pmod{\text{素数}\, p}$. しかし a^j は素数 p を含めないから $a^{k-j} - 1$ が p の倍数, 即ち $a^{k-j} \equiv 1 \pmod p$ が成り立つ. $1 \leqq k - j \leqq p-2$ だからこれは a が原始根である事, $p-1$ 乗ではじめて 1 に合同になる事, に反する. ■

故に T^* の任意元 $x_0 \neq 0$ に対して素数の法 p で $(a^j - a^k)x_0 = a^j x_0 - a^k x_0 \neq 0$, 即ち $a^j x_0 \neq a^k x_0$ であり, 法 p が素数 (ここでは 7) の時, 原始根 a を乗算合同法の乗数に選ぶと,

$$x_0,\ x_1 = ax_0,\ x_2 = a^2x_0, \cdots,\ x_k = a^k x_0, \cdots$$

は $1 \leqq k \leqq p-1$ に対して法 p ですべて異なり, 系列 $\{x_0, x_1, x_2, \cdots, x_k, \cdots, x_{p-1}\}$ には「種 seed」 $x_0 \in T^*$ の選択に関係なく T^* のすべての元が必ず 1 度ずつ出現する. これは乱数にとって好ましく重要な性質である. 法 7 では計算によって原始根 3,5 の存在が判った. 任意の素数 p に対しても $p-1$ 乗で始めて法 p で 1 になる原始根はあるだろうか. あるとすればどの様にして乱数生成に使う非常に大きい素数 p, 例えば $p = 2^{31} - 1 = 2147483647$ に対する原始根[14]を求めればよいか.

これらの問題の含む構造の最も明快な見通しは, 素数の法 p での整数の p 個のクラス (のうち 0 に合同でない $p-1$ 個) と同じ乗法構造を持つものの全体, 乗除法の定義された「群 group」と呼ばれる数 (や物) の集合, を一般に考えて得られる (次章). その準備ともして, この章を重要, 有名, 有用でしかも理解の容易なフェルマーの小定理とオイラー Euler の関数の構造とで締めくくる. 証明解析はどちらも短く楽しい.

フェルマーの小定理 1.21. p は素数, $T^* := \{1, 2, \cdots, p-1\}$ とすると, T^* の任意元 a に対して $a^{p-1} \equiv 1 \pmod{p}$ が成り立つ.

(証明) 我々は法 7 の算法に今までの演習問題で慣れたから, まず $p = 7$ の場合を取ろう. 乗法を普通の記号 $\cdot$ で記して, T^* の任意元 a から数

$$a \cdot 1,\ a \cdot 2,\ a \cdot 3,\ a \cdot 4,\ a \cdot 5,\ a \cdot 6$$

を作る. この中に 7 の倍数 (0 と合同なもの) はなく, しかも問題 1.19.(a) の乗積表の各行が示す様にこれらは $a \in T^*$ に関係なく互いにすべて異なり, T^* の元の並べ換え (置換) である. 積の順序を変えても法 7 の結果には関係しないから, 法 7 で次の合同式が成り立つ:

$$(a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdot (a \cdot 4) \cdot (a \cdot 5) \cdot (a \cdot 6) \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7}.$$

しかし明らかに 左辺 $= a^6 \cdot (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)$ である. 積 $P = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$ は素数 7 を含めず 7 の倍数ではない ($P \not\equiv 0 \pmod{7}$) から P で割って, 或いはこの 2 式の差を取って

$$(a^6 - 1)P \equiv 0 \to (a^6 - 1)P \text{ が } 7 \text{ の倍数} \to a^6 - 1 \text{ が } 7 \text{ の倍数} \to a^6 \equiv 1 \pmod{7}.$$

これで法 7 の証明を終る. 一般の素数 p の法を考えよう. その場合 $T^* = \{1, 2, \cdots, p-1\}$ の任意の 3 つの数 a, b, c, 但し $b \not\equiv c \pmod{p}$, について, a と $b - c$ は 0 に合同 (素数 p の倍数) ではなく $a \cdot (b - c) \not\equiv 0 \pmod{p}$, 即ち $a \cdot b \not\equiv a \cdot c$ が成り立つ. 故に $p-1$ 個の

$$a \cdot 1,\ a \cdot 2,\ \cdots,\ a \cdot (p-2),\ a \cdot (p-1)$$

は法 p ですべて異なる T^* の元, 従って T^* の元全体の置き換え (置換) で,

$$(a \cdot 1)(a \cdot 2) \cdots a \cdot (p-1) = a^{p-1} 1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv 1 \cdot 2 \cdot \cdots \cdot (p-1) \pmod{p}.$$

[14] $p = 2^{31} - 1$ は 4 バイト $= 32$ ビット のうち 1 ビットを符号に使うと, 4 バイト内で最大の素数であり, 4 バイト内で最大の Mersenne 素数 (問題 1.17.) である.

積 $P = 1 \cdot 2 \cdots (p-1)$ には素因数 p はない, p の倍数ではない, $P \not\equiv 0 \pmod p$. だから両辺を $P \not\equiv 0$ で割る事ができて, $a^{p-1} \equiv 1 \pmod p$. ■

重要ないくつかの表記法と Euler の関数 $\phi(n)$ とを導入する:

定義 1.22. 正整数 m, n について
(a) m, n の最大公約数 GCD を (m, n) と記し, (m, n)=1 の時「m, n は (互いに) 素」と言う. 言い換えれば「互いに素」とは「共通な素因数 $2, 3, \cdots$ を持たない」事である.
(b) 「m が n を割り切る, (m, n)=m である」事を「$m|n$」と記す (ランダウの記号).
(c) n に対して, $m \in \{1, 2, \cdots, n\}$ でかつ n と素であるものの個数を $\phi(n)$ と記しオイラー Euler の関数と呼ぶ. **(定義 1.21. 終り)**

集合の元の個数を $\sharp$ で表すと $\phi(n)$ の始めの幾つかは

$$\phi(1) = \sharp\{1\} = 1,\ \phi(2) = \sharp\{1\} = 1,\ \phi(3) = \sharp\{1, 2\} = 2,$$

$$\phi(4) = \sharp\{1, 3\} = 2,\ \phi(5) = \sharp\{1, 2, 3, 4\} = 4,$$

$$\phi(6) = \sharp\{1, 5\} = 2,$$

と見る事ができる. 一般に次が成り立つ:

定理 1.23. (a) オイラーの関数 ϕ は**乗法的 multiplicative** である. 即ち互いに素な (最大公約数 $\mathrm{GCD}(m, n) = (m, n) = 1$ の) 正整数 m, n に対し次が成り立つ:

$$\phi(mn) = \phi(m)\phi(n). \tag{1.2}$$

(b) 整数 $n \geqq 2$ の素因数分解を $n = a^r b^s \cdots f^u$ とすると

$$\phi(n) = n(1 - \frac{1}{a})(1 - \frac{1}{b}) \cdots (1 - \frac{1}{f}). \tag{1.3}$$

(証明) (a) $m = 1$ の場合は自明. $m \geqq 2$ と仮定する. $1 \leqq k \leqq mn$ の範囲の整数 k を $m \times n$ の行列へ組み上げる [19]:

	第 1 列	第 2 列		第 j 列		第 n 列
第 0 行	1	2	$\cdots$	j	$\cdots$	n
第 1 行	$n+1$	$n+2$	$\cdots$	$n+j$	$\cdots$	$n+n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
第 i 行	$in+1$	$in+2$	$\cdots$	$in+j$	$\cdots$	$in+n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
第 i' 行	$i'n+1$	$i'n+2$	$\cdots$	$i'n+j$	$\cdots$	$i'n+n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
第 $m-1$ 行	$(m-1)n+1$	$(m-1)n+2$	$\cdots$	$(m-1)n+j$	$\cdots$	$(m-1)n+n$

列を第 1–第 n 列, 行を第 0–第 $(m-1)$ 行と呼ぼう. 第 j 列の数の全体 $\{in + j |\ 0 \leqq i \leqq m-1\}$ は n で割った余りがみな等しい法 n で合同な数ばかりで, この表の数が n と素かそうでないかは所属の列番号 j で決まる. 故に mn と素 (当然 n と素) な数はすべて第 1 行成分 j が n と

素な $\phi(n)$ 個の列の中だけにある. この様な列の 1 つを第 j 列とするとその第 i, i' 行 $(i < i')$ 成分はそれらの差の形

$$(i'n + j) - (in + j) = (i' - i)n, \quad 1 \leqq i' - i \leqq m - 1$$

と $(m, n) = 1$ とによって互いに法 m で不合同である. だからこの第 j 列の $m - 1$ 個の成分全体は法 m で $\{1, 2, \cdots, m - 1\}$ 全体と同一で, これらの中に $m \geqq 2$ と素な数は j が何であっても常に $\phi(m)$ 個ある. 従って $\phi(mn) = \phi(m) \times (j \text{ の個数}) = \phi(m)\phi(n)$.
(b) 素数 a に対して $\{1, 2, \cdots, a^r\}$ の中で a^r と素な数は a の倍数の全体 $\{ax | \ 1 \leqq x \leqq a^{r-1}\}$ を除く全てで,

$$\phi(a^r) = a^r - a^{r-1} = a^r(1 - \frac{1}{a}).$$

素数 $b, c, \cdots$ についても同様だからこれは (a) によって (1.3) 式を証明する. ■

2. 群, 特に巡回群

群 group は数の集合, 或いはその他ものの集合 G で, その任意の 2 要素 (元, elements)x, y が「乗法,[15] 積」と呼ぶ規則或いは算法 $*$ によってある G の元 $x*y$ を作るものである. これを

> 群 G とは, その任意の 2 元の間に「(2 項) 算法 (binary) operation $*$」が定義され,
> この「乗法 $*$」について 2,3 の公理 (「良い性質」或いは制限) が成り立つもの,

という言葉で表現する. 群の代表の 1 つは「行列式 $\neq 0$ の (即ち正則な, 逆行列を持つ)n 次の (或いは $n \times n$ の) 複素行列の全体で行列積を $*$ とする」ものである. これは「複素一般線形群 complex general linear group $GL_n(\boldsymbol{C})$」と呼ばれる.[16] 一般に 2 次以上の行列 A, B の積 $A*B := AB \neq BA$ である事はよく知られている. 例えば

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}.$$

$n \geqq 2$ について $GL_n(\boldsymbol{C})$ は「非可換な乗法を持つ群, 非可換群 non-commutative group」である. もっと身近なものには, 前節で導入した「素数 p を法とする積 $*$」について, 0 を除く数の集合 $T^* = \{1, 2, \cdots, p-1\}$ がある. これは乗法が可換な「可換群 commutative group, アーベル群 Abelian group」の典型である. さらに, 一般に素数とは限らない m に対する 0 も含む集合 $T = \{0, 1, 2, \cdots, m-1\}$ について, mod m の加法を「群の乗法 $*$」と考える[17]ならこれもアーベル群である. 加法の群の姿は一見余りに簡単だが, ある対応を考えると多くの乱数問題はこれを最も重要な基礎構造としている事も見られる. 群は別に数の集合, 行列の集りに限らない. n 個のものの置換 permutations という数とは一見全く関係ないものの全体も, 「乗法」は相続く置換の「合成」に取って, 一般の群の (行列の群と並ぶ) もう 1 つのしかも最も由緒正しい総代表である.

色々な試みとその結果の比較から, ここでは一番わかりやすい道として数学の抽象手順に少しの間従い, 具体的幾何学的な説明から入る事は避ける. 我々は

(a) 群を公理系で定義し,
(b) それに我々の知るどの様なものが含まれるかを見て,
(c) そして群の定義から導かれる性質を議論する.

この組み立ては無味乾燥に見えるが, 経験的には我々が必要以上に理解に悩む事をむしろ防いでいて, しかも得られる結論には群を実際に構成するものが何か, 乗法がどう定義されたかに全く無関係に成立つ強さを与える. このような考え方の力にも注目しながら進む事にしよう.

2.1. 群の定義

[15] 乗法という名前は, 以下の定義に合ってさえいれば, 我々の常識の乗法と一致する事までは求めない.
[16] 複素数 complex numbers の全体は $\boldsymbol{C}$ と記される.
[17] 加法も, 確かに, T の任意の 2 つの要素 x, y から T の要素 $x+y$ を作る, という意味で「積, 2 項算法 $*$」の定義に適っている.

乱数生成には専ら乗法の可換な群が用いられるが, その限定は議論の上で余り重要ではなく, むしろ引き換えに大きな一般性を見逃す恐れが大きい. そこで暫く, 乗法を可換とは仮定せず進む. 次の簡単な公理系はこの一般の群を定義する.

定義 2.1. (a) 集合 $= \{x, y, z, \cdots\}$ が次の 4 公理をすべて満たす時群 group と言う:

(公理 0) 任意の 2 元 $x, y \in G$ にそれらの「積 product」$x * y$ が定義され, $x * y \in G$ が成り立つ.[18]

(公理 1) (結合法則) 任意の $x, y, z \in G$ について $(x * y) * z = x * (y * z)$.

(公理 2) (右単位元の存在) ある $e \in G$ があって, すべての $x \in G$ に対して $x * e = x$ が成り立つ.

(公理 3) (右逆元の存在) 任意の $x \in G$ にはある $x^{-1} \in G$ があって, $x * x^{-1} = e$ が成り立つ.

(b) 有限個の元からなる群を有限群 finite group という. 有限群 G の元の総数を「位数 order」と呼び $\mathrm{ord}(G)$ と記す. 元の数が無限の群では $\mathrm{ord}(G) = \infty$ とする.

(c) 群の乗法が可換, 即ち全ての $x, y \in G$ に対し $x * y = y * x$ の場合, G を「可換群, アーベル群 Abelian group」という. **(定義 2.1. 終り)**

言葉だけ見ると何の特徴もないものに見えるが, なかなかどうして, これらの公理の組の全体は誠に面白い沢山の構造をしっかりその相互の網のなかに包み込んでいる. またそれぞれの言明は随分弱い形 (例えば右単位元, 右逆元だけの存在) に与えられているけれども, 結果的には十分強い制限を与えている. 群の構造の特徴を掴むためにそのいくつかの要点を見て, さらに重要な後節の部分群構造へ進む足掛りとしよう. これからは乗法を特に強調する場合を除き, 積を単に xy の様に記して, 乗法記号 $*$ は省略する.

Corollary 2.2. (a) 群の元 x, y, z について $zx = zy$ 或いは $xz = yz$ となるのは $x = y$ の場合に限る.

(b) 右単位元 e は左単位元でもある. 即ちすべての $x \in G$ について $xe = ex = x$. また単位元 e は一意である.

(c) 任意の $x \in G$ に対し x^{-1} は左逆元でもあって, $x^{-1}x = e$, 即ち $(x^{-1})^{-1} = x$. また逆元は一意である.

(d) $x \in G$ について

$$xG := \{xy |\ y \in G\},\ Gx := \{yx |\ y \in G\},\ G^2 := \{xy |\ x, y \in G\},\ G^{-1} := \{x^{-1} |\ x \in G\},$$

と記す. 任意の $x \in G$ に対し $xG = Gx = G^2 = G^{-1} = G$ が成り立つ.

(証明) (c) から始める. 成立を仮定された公理 1 の結合法則から $x^{-1} = x^{-1}e = x^{-1}(xx^{-1})$ $= (x^{-1}x)x^{-1}$. 公理 3 によって x^{-1} は G の元であり, その右逆元 y は存在するからそれを上の式の右に掛けて,

$$e = x^{-1}y = \{(x^{-1}x)x^{-1}\}y = (x^{-1}x)(x^{-1}y) = (x^{-1}x)e = x^{-1}x.$$

即ち x^{-1} は左逆元でもあり, $(x^{-1})^{-1} = x$ である事もわかる. 故に任意の $x \in G$ に対して x $= xe = x(x^{-1}x) = (xx^{-1})x = ex$ が成り立ち, e は「左単位元でもある」. x, y, z が G の任意元で $zx = zy$, 或いは $xz = yz$ だとすると, 「左から z の左逆元 z^{-1}」, 或いは「右から z の

[18] 添加された乗法 $*$ を明示するのに「群 $(G, *)$」とも記す.

右逆元 z^{-1}」を作用して e が左右両方の単位元である事を用いて

$$z^{-1}(zx) = (z^{-1}z)x = ex = x = z^{-1}(zy) = (z^{-1}z)y = ey = y,$$
$$(xz)z^{-1} = x(zz^{-1}) = xe = x = (yz)z^{-1} = y(zz^{-1}) = ye = y$$

を得る. これが (a) である. 故に単位元 e, 逆元は一意である: 実際 e 以外の単位元を f とすると, $xe = xf = x$ だから (a) によって $e = f$ だし, x の逆元が x^{-1} 以外に y もあれば $xx^{-1} = e = xy$, 故に (a) から $x^{-1} = y$. これで (a),(b),(c) の証明を終る.
(d) 集合 xG の一般元 xy, $y \in G$ は任意, はやはり G の元で $xG \subset G$.[19] これは $x^{-1}G \subset G$ も意味し, $G = eG = (xx^{-1})G = x(x^{-1}G) \subset xG \subset G$ で $xG = G$. 同様に $Gx = G$ も示される. $G = xG \subset G^2 \subset G$ から $G^2 = G$. 最後に $G^{-1} \subset G$ は明らかだが, 任意の $x \in G$ については $x = (x^{-1})^{-1} \in G^{-1}$ でもあるから $G \subset G^{-1}$, 即ち $G = G^{-1}$. ■

以下の主役である位数有限の群に関しては公理 3 の次の置き換えも便利である:

Corollary 2.3. 有限集合 G が群である必要十分条件は公理 $0-2$ と次の成立である:
(公理 3') $x, y, z \in G$ について $xy = xz$ なら $y = z$.
(証明) 群 G では Corollary 2.2.(a) から公理 3' は成り立つ (必要性). 逆に公理 3' 或いはその対偶「$y \neq z$ なら $xy \neq xz$」が公理 0,1,2 と共に成り立つとすると, 有限集合 G の元の 1 列化 $G = \{a, b, \cdots\}$ を考えて, 任意の $x \in G$ に対して $xa, xb, \cdots$ はすべて異なり, G の元全体の置換で, 公理 2 から必ず $xc = e$ となる x の右逆元 c が存在し G は群である (十分性). ■

2.2. 演習問題

乱数に関係の深いアーベル群の重要な例, 反例で群の定義や命題を反芻する.

問題 2.4. 記法 $\boldsymbol{Z}/m := \{0, 1, 2, \cdots, m-1\}$ を導入する.[20] 任意の正の整数 m(素数でなくてよい) に対し, $\boldsymbol{Z}/m$ は法 m の加法 $+(\mathrm{mod}\ m)$ についてアーベル群である. これを示せ.
(証明) 任意の $x, y, z \in \boldsymbol{Z}/m$ を取って群の公理 (0-3) がすべて成立する事を示せばよい. それぞれ次の様になる:
(公理 0) $x + y$ を m で割った余りは 0 から $m-1$ までの数で, 法 m での和 $x + y \in \boldsymbol{Z}/m$, 即ち「$\boldsymbol{Z}/m$ は法 m の加法で閉じている」.
(公理 1) 通常の和で結合法則 $(x + y) + z = x + (y + z)$ は成立する. Lemma1.3.(b) によれば m で割った余りはどの計算段階でも何回でも取ってよいから, $(x + y)$, $(y + z)$ それぞれの段階で法 m の値としても結果は同じで,

$$\{x + (\mathrm{mod}\ m)y\} + (\mathrm{mod}\ m)z \equiv x + (\mathrm{mod}\ m)\{y + (\mathrm{mod}\ m)z\},$$

[19] 集合 S, S' について S' が S の部分集合である, $S' \subset S$ とは, S' の任意元は S の元である事, 即ち「$x \in S'$ なら $x \in S$ が成り立つ」, で定義される. また $S' \subset S$ で同時に $S \subset S'$ でもある事を「集合 S, S' は等しい」と定義して $S = S'$ と記す.
[20] 記号 $\boldsymbol{Z}$ は通常整数全体を表し, $\boldsymbol{Z}/m$ は「整数全体を m で割った余りとなる数の集合」で $\boldsymbol{Z}/m\boldsymbol{Z}$ とも書かれる. もっと一般には, 整数全体 $\boldsymbol{Z}$ を m で割った余りで分類して同じ余りの数は同一のクラス (類) を構成すると考える方がよい. この場合の同一の類 (集合) を「法 m での剰余類」と呼び, $\boldsymbol{Z}/m$ はこれらの剰余類の集合 (集合の集合) を表すと見る事になる. 考えるのに困難さえなければこの後者の方が便利なので次第にこの考え方に移行する.

即ち結合法則も成り立つ.
(公理 2) (右) 単位元として $e=0$ が存在する. 実際任意の $x \in \boldsymbol{Z}/m$ について $x+0=x$.
(公理 3) 任意の $x \in \boldsymbol{Z}/m$ に対して, $x=0$ なら $0+0=0=e$ によって $x^{-1}=0$, $x \neq 0$ なら $m-x$ は $\boldsymbol{Z}/m$ の数で $x+(m-x)=m \equiv 0=e \pmod m$, 即ち:

法 m での加法に関する逆元 $x^{-1}=m-x$ が $\boldsymbol{Z}/m$ のすべて元 x に存在する.

最後に, $x+y=y+x$ から「群乗法 $+(\mathrm{mod}\, m)$ の可換性」$x+(\mathrm{mod}\, m)y=y+(\mathrm{mod}\, m)x$ は明らか. ■

勿論, これからはややこしい「$x+(\mathrm{mod}\, m)\, y$」の様な書き方はやめて $x+y$ とし, 高々間違いやすそうな所で計算の最後に $(\mathrm{mod}\, m)$ 等と記す事にする.

問題 2.5. 素数 $p=2,3,5,\cdots$ に対して記法 $\boldsymbol{Z}_p^* := \boldsymbol{Z}/p-\{0\}=\{1,2,\cdots,p-1\}$ を導入する.[21] $\boldsymbol{Z}_p^*$ は法 p の乗法 $\times(\mathrm{mod}\, p)$ について位数 $p-1$ のアーベル群である. これを示せ.
(証明) 任意の $x,y,z \in \boldsymbol{Z}_p^*$ を取る. 群の公理の成立は次の通り:
(公理 0) 積 xy には素因数 p がなく p で割った余りは 1 から $p-1$, 即ち $x \times y(\mathrm{mod}\, p)$ は $\boldsymbol{Z}_p^*$ に属している. 故に「$\boldsymbol{Z}_p^*$ は法 p の乗法で閉じている」.
以下 $\times$ は省略する.
(公理 1) 普通の積で結合法則 $(xy)z=x(yz)$ は成立するし, Lemma 1.3.(b) によって p で割った余りをどの計算段階で取っても結果は変らないから $(xy)z \equiv x(yz) \pmod p$, 結合法則は成り立つ.
(公理 2) 乗法での (右) 単位元 $e=1 \in \boldsymbol{Z}_p^*$ が存在する.
(公理 3') $xy \equiv xz \pmod p$ 即ち $x(y-z)=p$ の倍数なら, x は素因数 p を含まないから $y-z$ が p の倍数であり, $y \equiv z$. 最後に $xy=yx$ から可換性 $xy \equiv yx \pmod p$ も明らか. ■

問題 2.6. 整数 $m>0$ が素数でなく合成数なら, $T^* := \boldsymbol{Z}/m-\{0\}=\{1,2,\cdots,m-1\}$ は $\times(\mathrm{mod}\, m)$ について群ではない. これを示せ.
(証明) 群でない事は公理 0–3 の任意の 1 つの不成立を言えば示される. 今の場合 m は合成数だから $2 \leqq x,y<m,\ xy=m$ となる整数 $x,y \in T^*$ がある. しかし法 m での積 $xy=m \equiv 0$ は T^* に属さない. T^* は「乗法で閉じない」ので群の公理 0 を満たさない. ■

問題 2.7. 正の任意の整数 m に対して次の集合を定義する:

$$\boldsymbol{Z}_m^* := \{k|\ (k,m)=1,\ 1 \leqq k \leqq m\}.$$

即ち $\boldsymbol{Z}_m^*$ は 1 から m までの整数で m とは素なもの, 言い換えると m とは共通な素因数を全く持たないものの集りである.[22] 法 m の乗法ではアーベル群であり, 位数は $\phi(m)$ である. また m が素数 p の場合

$$\boldsymbol{Z}_m^* = \boldsymbol{Z}_p^* = \{1,2,\cdots,p-1\}$$

[21] 集合 S から集合 S' に属する元を除外した集合は $S-S'$ でもよいが明確のため $S \backslash S'$ と記され, 記号 $\backslash$ は setminus という TeX 名までも持つ. しかし以下では $S' \subset S$ の場合しか扱わないから単純な $S-S'$ を用いる. なお素数の法 p での数の全体 $\boldsymbol{Z}/p=\{0,1,\cdots,p-1\}$ は集合として $\boldsymbol{Z}_p^*$ と非常に近く, 次の問題 2.7. の素数ではない m での $\boldsymbol{Z}_m^*$ と $\boldsymbol{Z}/m$ との乖離とは大いに異なる. 以後素数 p では $\boldsymbol{Z}/p$ を $\boldsymbol{Z}_p$ とも記して視覚化し, 記法も簡単化する.

[22] $\boldsymbol{Z}/m$ を整数全体を m で割った剰余で類別した剰余類 (集合) を元とする「集合の集合」と見, そのうち m と素な剰余で代表される剰余類だけの集合が $\boldsymbol{Z}_m^*$ だとすると応用が広い. この見方を以下次第に多用する.

が成り立つ. これらを示せ. $\boldsymbol{Z}_m^*$ は「法 m の既約剰余群」と呼ばれる.
(証明) m が素数 p の場合, 定義から $\boldsymbol{Z}_m^* = \{1, 2, \cdots, p-1\}$ であり, これが既に記された $\boldsymbol{Z}_p^*$ である事は明らかで $\boldsymbol{Z}_p^*$ が群である事は示されている. これを予期して $\boldsymbol{Z}_p^*$ と同じ記号 $\boldsymbol{Z}_m^*$ を用いた. 一般の正の整数 m を考えよう. 任意の $x, y, z \in \boldsymbol{Z}_m^*$ について:
(公理 0 の成立) $\boldsymbol{Z}_m^*$ の任意元 x, y も, 従って積 xy も m と共通な素因数を持たないから $xy \in \boldsymbol{Z}_m^*$ である. 詳しく言えば m による xy の割り算 $xy = qm + r$ での余り r が xy を法 m で代表する数だが, 仮に r と m が共通な素因数 a を持ば xy も a で割り切れて矛盾だから r も m とは共通素因数を持てない. 故に $xy \in \boldsymbol{Z}_m^*$ であり, 「法 m の乗法で $\boldsymbol{Z}_m^*$ は閉じている」.
(公理 1 の成立) 通常の積で結合法則 $(xy)z = x(yz)$ は成立する. Lemma 1.3.(b) によれば m で割った余りを計算のどの段階で取ってもよいから, $(xy)z \equiv x(yz) \pmod{m}$, 結合法則が成り立つ.
(公理 2 の成立) 乗法での (右) 単位元 1 はどんな法 m に対しても最大公約数 $(1, m) = 1$ の意味で m とは素で, 必ず $\boldsymbol{Z}_m^*$ の中に存在する. これは Euler の関数の定義で見た通りである.
(公理 3' の成立) $zx \equiv zy \pmod{m}$ 即ち $z(x-y) = m$ の倍数なら, z は m と共通な素因数を含まないから $x - y$ が m の倍数であり, $x \equiv y \pmod{m}$ でなければならない. 対偶として $x \not\equiv y \pmod{m}$ なら $zx \not\equiv zy$ が成立する.
勿論 $xy = yx$ から法 m での可換性 $xy \equiv yx$ が出るし, オイラーの関数 $\phi(m)$ の定義は集合 $\boldsymbol{Z}_m^*$ の元の数そのものであって, $\sharp \boldsymbol{Z}_m^* = \phi(m)$ は明らか. ■

問題 2.8. 正の任意整数 m を取り $a = \exp \dfrac{2\pi i}{m}$ とする. 1 の複素 m 乗根の全体

$$G_m := \{b_0, b_1, \cdots, b_{m-1}\} = \{b_j := a^j = \exp \frac{2j\pi i}{m} | \ j \in \boldsymbol{Z}/m = \{0, 1, \cdots, m-1\}\}$$

は普通の乗法 $\times$ について位数 m のアーベル群である事を示せ.

(証明) 1 の m 乗根である複素数 b を極表示で $b = re^{i\theta}$ とすれば $b^m = r^m e^{im\theta} = 1$. 故に $r = 1$, $\theta = \dfrac{2j\pi}{m}$, j は整数, つまり b は上の $b_j = a^j$ の形に限る. 整数 j, k に対し

$$b_j \times b_k = \exp \frac{2j\pi i}{m} \exp \frac{2k\pi i}{m} = \exp \frac{2(j+k)\pi i}{m} = b_{j+k}$$

は明らか. また $j \equiv k \pmod{m}$, 即ち $j = k + sm$ (s は整数) なら

$$b_j = a^{k+sm} = b_k \times (a^m)^s = b_k \times 1 = b_k.$$

故に異なる b_j の代表として m 個の

$$\{b_j | \ j \in \{0, 1, \cdots, m-1\} = \boldsymbol{Z}/m\} = G_m$$

だけを考えれば十分で, G_m は 1 の m 乗根のすべてである事もよく知られている. 群の公理の成立を見よう.
(公理 0 の成立) $j, k \in \boldsymbol{Z}/m$ について $(b_j \times b_k)^m = {b_j}^m \times {b_k}^m = 1 \times 1 = 1$, $b_j \times b_k \in G_m$, G_m は乗法 $\times$ で閉じている.
(公理 1 の成立) 結合法則は複素数の乗法 $\times$ で成立つのだから当然 G_m でも成立つ.
(公理 2 の成立) 単位元 e として $b_0 = b_m = 1$ が存在する.
(公理 3 の成立) 任意の $b_j \in G_m$ の逆元は, $b_0 = 1$ なら明らかに自分自身だが b_m としてもよい. $j > 1$ の b_j については $b_{m-j} \in G_m$ である. 実際

$$b_j \times b_{m-j} = b_{j+(m-j)} = b_m = 1 = e.$$

最後に, 通常の積の可換性から G_m はアーベル群である. ■

基本的な事項は上で大体見られるが, さらに群の定義に実例で慣れる様に以下の問題や証明をそれぞれ試して頂きたい.

問題 2.9.(a) 法 $m = 8$ では 8 で割った余り, $\boldsymbol{Z}/8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, によって整数の全体は代表される. 法 8 の乗積表を算出せよ.
(解) 法 8 の乗積表は次の通り:

$x\backslash y$	0	1	2	3	4	5	6	7	x^{-1}
0	0	0	0	0	0	0	0	0	
1	0	1	2	3	4	5	6	7	1
2	0	2	4	6	0	2	4	6	
3	0	3	6	1	4	7	2	5	3
4	0	4	0	4	0	4	0	4	
5	0	5	2	7	4	1	6	3	5
6	0	6	4	2	0	6	4	2	
7	0	7	6	5	4	3	2	1	7

$x = 2, 4, 6, 8$ には掛け合わせて 1 になる「逆数」が存在しない. **(問題 2.9.(a) 終り)**

問題 2.9.(b) 上の (a) の結果を用いて $T^* := \boldsymbol{Z}/8 - \{0\} = \{1, 2, 3, 4, 5, 6, 7\}$ に法 8 の乗法を添加した $(T^*, \times \pmod 8)$ は群にはならない事を示せ.
(証明) 群でない事は公理 0–3 のどれかが満たされない事を示せば十分である. 実際,
(i) 問 (a) の乗積表の x 或いは $y = 0$ を除く部分を見れば, T^* の数 2,4,6 は他の偶数との掛け算で T^* には属さない 0 を与えている. 即ち T^* は法 8 の乗法で閉じず, 公理 0 を満たさない.
(ii) 或いは問 (a) の乗積表によって T^* の数 2,4,6 は逆元を持たず, 公理 3 は成立しない.
このどちらを考えても, T^* は群ではない. ■

問題 2.9.(c) $\boldsymbol{Z}/8$ の数の中から法の $8 = 2^3$ とは素なもの (即ち素因数 2 を含まないもの, 奇数) だけを集めた $\boldsymbol{Z}_8^* = \{1, 3, 5, 7\}$ の乗積表を抜き出し, それに基づいて既約剰余群 $\boldsymbol{Z}_8^*$ は法 8 の乗法で群を作る事を直接示せ.
(証明) $\boldsymbol{Z}_8^*$ の乗積表は次の通り:

$x\backslash y$	1	3	5	7	x^{-1}
1	1	3	5	7	1
3	3	1	7	5	3
5	5	7	1	3	5
7	7	5	3	1	7

群である事を示すには公理 0–3 の全てが満たされている事を言わなければならない. 任意の正の整数 $m \geqq 2$ について $\boldsymbol{Z}_m^*$ が群である事は既に示されているが, ここでは上の表だけから議論してみる.
(公理 0 の成立) $\boldsymbol{Z}_8^*$ の数はすべて奇数だからそれらの乗法の結果も奇数で, 8 で割った余り

は $\boldsymbol{Z}_8^*$ の数ばかりである. $\boldsymbol{Z}_8^*$ は法 8 の乗法で閉じている.[23]
(公理 1 の成立) 結合法則は任意の整数の乗法での成立から法 8 でも成り立つ.
(公理 2 の成立) 単位元 1 は $\boldsymbol{Z}_8^*$ に入っている. そして
(公理 3 の成立) 逆元が乗積表のすべての x の行に必ず存在する, 或いは
(公理 3' の成立) すべての行は $\boldsymbol{Z}_8^*$ の元の置換であり, $xy = xz$ となるのは $y = z$ に限る.
故に $\boldsymbol{Z}_8^*$ は群の公理をすべて満たし, 群である. ■

$\boldsymbol{Z}_7^*$ や上の $\boldsymbol{Z}_8^*$ で見たように, 有限群の乗積表の各行, 各列には群のすべての元が整列して必ず 1 度ずつ現れ, 現れない元や 2 度以上登場する元は存在しない. n 個の文字や数の n 行 n 列の行列は方陣 square と呼ばれ, その中でこの「各文字は全ての行や列に 1 度そしてただ 1 度だけ必ず現れる」という性質を持つものはラテン方陣 Latin square と名付けられて多くの応用を持つ.[56)]

2.3. 巡回群

前節の問題 2.8 の 1 の m 乗根の群 G_m はそのただ 1 つの元 $a = b_1 = \exp\dfrac{2\pi i}{m}$ の「冪乗」ですべての元が生成された. この特別な性質を持つ群は「巡回群」と呼ばれ, 現在の乱数生成問題や多くの他の応用で重要な役割を演じる. いくつかの言葉を明確に定義し, その関連する 2,3 の性質を見て後に備えよう.

定義 2.10. (a) 群 G の任意元 x について, $x^1 = x,\ x^2, \cdots$ と冪乗して h 乗で $x^h = e$ になる最小の $h \geqq 1$ が存在すれば h を「x の位数 order」といい $h = \mathrm{ord}(x)$ と記す. その様な有限の h が存在しない時には, 位数 $h := \infty$ と定義する.
(b) 群 G の元の中にその冪乗で G 全体を生成するもの a が存在する時, G を巡回群 cyclic group と言う. またこの元 a を「群 G の生成元 generator」と言う. **(定義 2.10. 終り)**

前に「群の元の数」に使われた位数 order という言葉がここでは「冪乗して初めて e になる指数」に用いられる. これは混乱ではなく意味のある用語だがその大切な認識には少し準備がいる. 既出の事の繰り返しも含めて, 次から考えをまとめ始めよう.

Lemma 2.11. 群 G の任意の元 x が位数 $h = \mathrm{ord}(x)$ を持つとする.
(a) h が有限なら $\{x^1, x^2, \cdots, x^h = e\}$ はすべて異なり, $h = \mathrm{ord}(x)$ は x **の冪乗で作られる異なる元の総数と等しい**. $h = \infty$ の時も x のべき乗 $\{x^1, x^2, \cdots\}$ はすべて異なる.
(b) h が有限の時, $x^n = e$ となる正整数 n の全体は h の倍数の全体である.
(c) 群 G の位数が有限 $\mathrm{ord}(G) = g < \infty$ の時, $a \in G$ で位数 $\mathrm{ord}(a)$ が g に等しいものがある事は群 G が巡回群で (そして a がその生成元で) ある事の必要十分条件である.
(d) なお, 群 G が巡回群なら G はアーベル群である.
(証明) (a) 群 G の任意元 x について $xx^{-1} = x^{-1}x = e$ なので x と x^{-1} とは可換な事を注意すると, 結合法則から $x^j(x^{-1})^j = (xx^{-1})^j = e^j = e$, つまり $(x^j)^{-1} = (x^{-1})^j$ が見られる. さて $\mathrm{ord}(x) = h$ が有限の場合 $x^j = x^k$ となる番号 $1 \leqq j \leqq k \leqq h$(当然 $0 \leqq k - j \leqq h - 1$) の存在を仮定すれば $x^j = x^k$ に $(x^j)^{-1} = (x^{-1})^j$ をかけて $e = x^k(x^{-1})^j = x^{k-j}$ が成り立つ. し

[23] もっと一般的性のある言い方をすると, 「$\boldsymbol{Z}_8^*$ の数は法の 8 の素因数 2 を持たないからそれらの積も 8 とは素で $\boldsymbol{Z}_8^*$ を出ず, $\boldsymbol{Z}_8^*$ は法 8 の乗法で閉じている」.

かし $k-j \leqq h-1$ であり h は $x^h=e$ となる最小の正の整数なので $k-j=0$ 以外はあり得ず, $x^1, x^2, \cdots, x^h=e$ はすべて異なる. $x^h=e$ 以後は $x^{h+1}=ex=x,\ x^{h+2}=ex^2=x^2$ と $x, x^2, \cdots, x^h=e$ の繰返しだから, h は x の冪乗が生成する異なる元の総数である. 位数 h が無限の場合にも $1 \leqq j \leqq k$ の有限の番号 j,k(当然 $0 \leqq k-j < \infty$) で $x^j=x^k$ となるものの存在を仮定すれば, 上の手順で有限の $k-j \geqq 0$ で $x^{k-j}=e$ となるものが得られ, 位数無限の仮定から $k-e=0$ に限られる. 故に冪乗 $\{x^1, x^2, \cdots\}$ はすべて異なる.
(b) 上の (a) の通り群 G の元の列 $\{x^1, x^2, \cdots\}$ は $x^h=e$ からは繰返しで, 全体は

$$x^1, x^2, \cdots, x^h=e, x^{h+1}=ex=x^1, x^{h+2}=x^2, \cdots, x^{h+h}=x^h=e, \cdots,$$

となり $x^1, x^2, \cdots, x^h=e$ はすべて異なる. 特に $x^1, x^2, \cdots, x^{h-1} \neq x^h=e$ だから, $x^n=e$ となる n は $n=kh,\ k$ は整数, の形以外にはない. 逆に任意の正の整数 k について $n=kh$ の形なら $e=e^k=(x^h)^k=x^{kh}$ は明らかで, 命題は示された.
(c) 必要性は巡回群の定義と (a) から明らか. 逆に $\mathrm{ord}(a)=\mathrm{ord}(G)=g$ を仮定すると, 上の (a) によって $a^1, a^2, \cdots, a^g=e$ はすべて異なる G の元 g 個で, それは G の元の全体である. 故に a は生成元, G は巡回群である (十分性).
(d) 巡回群 G の 2 元 x,y は生成元 a の冪乗で $x=a^j,\ x=a^k$ と表され, 結合法則から $a^ja^k=$「a の $j+k$ 個の積 a^{j+k}」$=a^ka^j$ となり, 巡回群は必ず可換群, アーベル群に限られる. ■

上の Lemma 2.11.(d) の逆は必ずしも成り立たず, アーベル群は巡回群とは限らない. これは次の問題で確認する.

問題 2.12. 法 $m=8=2^3$ について m と素な (m と共通な素因数 2 を持たない) 数の全体, 8 の既約剰余群 $\boldsymbol{Z}_8^* := \{1,3,5,7\}$ を再び考えよう. 問題 2.9.(c) で見たその乗積表は:

$x\backslash y$	1	3	5	7	x^{-1}
1	1	3	5	7	1
3	3	1	7	5	3
5	5	7	1	3	5
7	7	5	3	1	7

冪乗表を作り, $\boldsymbol{Z}_8^*$ の元の中にべき乗で $\boldsymbol{Z}_8^*$ 全体を生成するものがあるか, $\boldsymbol{Z}_8^*$ は巡回群であるかを判定しなさい.
(解) $x \in \boldsymbol{Z}_8^*$ の冪乗 x^n の表は次の通り:

$x\backslash n$	1	2	3	4	位数
1	1	1	1	1	1
3	3	1	3	1	2
5	5	1	5	1	2
7	7	1	7	1	2

3,5,7 の位数はすべて 2 で, $\boldsymbol{Z}_8^*$ には冪乗で $\boldsymbol{Z}_8^*$ のすべての数を生成するものはない. $\boldsymbol{Z}_8^*$ は巡回群ではない. **(問題 2.12. 終り)**

乗算合同法乱数では巡回群とそれに深い関係を持つオイラーの関数との役割が本質的である. この事は次の章で詳しく議論するが, 先立つ準備としてそれらの姿に 1 の m 乗根の群 G_m とすぐ後の別の簡単な例で触れる.

問題 2.13. 次の各事項を示せ.

(a) 一般の正の整数 m と $1 \leqq j \leqq m$ とに対して, $a^j = \exp \dfrac{2j\pi i}{m}$ を一般元とする 1 の m 乗根の巡回群 G_m での a^j の位数は j と m の最大公約数を (j,m) として $\mathrm{ord}(a^j) = \dfrac{m}{(j,m)}$ である.

(b) 任意の整数 $m > 0$ に対し 1 の原始 m 乗根の総数は Euler の関数 $\phi(m)$ で与えられる.

(c) 特に m が素数 p なら, 1 の p 乗根のうち 1 以外のものはすべて原始 p 乗根, p 乗して初めて 1 になる数, 即ち群 G_p の生成元である.

(証明) (a) 1 の m 乗根で異なるものの全体が $\{a^j = \exp \dfrac{2j\pi i}{m} |\ 1 \leqq j \leqq m\}$ である事は見た. もし j が m と素なら, j と m とに共通の素因数はないから $j, 2j, 3j, \cdots, (m-1)j$ は m で割り切れない. だから $\{(a^j)^h = a^{jh} = \exp(\dfrac{2jh\pi i}{m}) |\ 1 \leqq h \leqq m-1\}$ は 2π の整数倍ではない偏角しか持てずすべて 1 とは異なり, $(a^j)^m$ で初めて 1 になって a^j は 1 の原始 m 乗根である. 最大公約数 $(j,m) = d \geqq 2$ の場合, $j = j'd,\ m = m'd$ と表すと $(j', m') = 1$ で $\dfrac{2j\pi i}{m} = \dfrac{2j'\pi i}{m'}$ となる. $a^j = \exp \dfrac{2j'\pi i}{m'}$ は上の事から 1 の原始 $m' = \dfrac{m}{(j,m)}$ 乗根で $\mathrm{ord}(a^j) = \dfrac{m}{(j,m)}$ である.

(b) 1 の m 乗根は G_m の元だから G_m の生成元 a によって $a^j,\ 1 \leqq j \leqq m$ と表され, (a) で見た通りそれに対応した位数 $\dfrac{m}{(j,m)}$ を持つ. 故に原始 m 乗根は $1 \leqq j \leqq m$ で m と素な j, 即ち $(j,m) = 1$ となる j, に対する a^j がそのすべてである. Euler の関数 $\phi(m)$ は「m と素な m 以下の正の整数の総数」だからこれが原始 m 乗根の総数である.

(c) m が素数 p なら $\phi(p) = \sharp\{1, 2, \cdots, p-1\} = p-1$ で, (c) は (b) の特別の場合である. ■

2.4. 部分群, 剰余類, Lagrange の定理

群の部分集合に群の乗法で閉じている「部分群」があれば, もとの群の構造には大きな限定が存在する. この情報の解析がこの節のテーマである. まず部分群を特定しよう.

Lemma 2.14. 群 G の部分集合 H が G の群乗法でそれ自体群を構成するとき, 「H は G の部分群 subgroup である」という.

(a) 部分集合 $H \subset G$ が部分群であるための必要十分条件は[24],

$$\text{任意の } x, y \in H \text{ について } xy^{-1} \in H.$$

(b) H が G の部分群なら任意の $x \in H$ について[25]

$$xH = Hx = H^2 = H^{-1} = HH^{-1} = H.$$

(c) $H \subset G$ が G の部分群であるもう 1 つの有用な必要十分条件は

[24]下で y は H の元だが H を群とは仮定しないから y^{-1} が H に入るかどうかわからない. しかし G の元として積 xy^{-1} を作る事ができ, その結果が必ず H に入れば H は群だというのである.

[25]集合 $xH,\ Hx,\ H^2,\ H^{-1},\ HH^{-1}$ の定義については Corollary 2.2. を参照.

$$H^2 \subset H \text{ かつ } H^{-1} \subset H.$$

(証明) (a) 部分群なら H は群だから $xy^{-1} \in H$ は当然成立ち, 条件は必要である. 逆に G の部分集合 H の任意の 2 元 x, y が $xy^{-1} \in H$ を満たすとして H が群である事, 十分性を示そう. まず仮定で $y = x$ として $xx^{-1} = e \in H$, H に単位元が所属している事が判る (公理 2 の成立). 故に仮定で $x = e$ と置く事もできて任意の $y \in H$ に対して $ey^{-1} = y^{-1} \in H$, H のすべての元 y の逆元も H に入っている (公理 3 の成立). 任意の $x, y \in H$ について $y^{-1} \in H$ はわかったから, 再び仮定を用いて $x\{(y^{-1})^{-1}\} = xy \in H$, H は乗法で閉じている (公理 0 の成立). 結合法則はもとの群 G で成り立つので H でも成立つ (公理 1 の成立). 故に H は群である. (十分性証明終り)
(b) H はそれ自身群だから Corollary 2.2. の群の性質 (d) によってすべて明らか.
(c) 上の (b) の $H^2 = H^{-1} = H$ は $H^2 \subset H$ と $H^{-1} \subset H$ も意味し, $H^2 \subset H$ 及び $H^{-1} \subset H$ は H が部分群であるために必要である. 十分性については, $H^2 \subset H$ かつ $H^{-1} \subset H$ である時, 任意の $x, y \in H$ を取ると $xy^{-1} \in HH^{-1} \subset HH = H^2 \subset H$. 故に $xy^{-1} \in H$ であり, (a) によって H は部分群である. これで示された. ■

以下の多くの議論で本質的な役割を演じる Lagrange の定理に向かう. 余りにも平凡に見える群の公理が, 可換乗法だろうと非可換だろうと, この定理で均等にしかも強く縛られているのは不思議だが, 事実は次の簡単な事柄から生じる:

Corollary 2.15. 群 G とその任意の部分群 H, そして G の任意の 2 元 x, y に対して次が成り立つ:
(a) $xH = yH$ であるか, それとも $xH \cap yH = \phi$ か[26], の二者択一である.
(b) $Hx = Hy$ であるか, それとも $Hx \cap Hy = \phi$ か, の二者択一である.
(証明) (a) $xH \cap yH \neq \phi$ なら, ある $h, k \in H$ を取って共通集合のある元を $xh = yk$ と表せる. $x = ykh^{-1}$, kh^{-1} は H の元だから Lemma 2.14.(b) によって $kh^{-1}H = H$ であり, $xH = y(kh^{-1}H) = yH$. 逆に $xH = yH$ なら $xH \cap yH \neq \phi$ は明らかで, $xH = yH$ と $xH \cap yH \neq \phi$ とは同じ (同値) である. $xH \cap yH \neq \phi$ であるか $xH \cap yH = \phi$ かの二者択一なのは自明だから, 命題通り $xH = yH$ であるか $xH \cap yH = \phi$ かのどちらかである.
(b) 上の (a) の証明と全く同じだから省略する. ■

G の任意元 x に対し, xH の形の集合を「H に関する左剰余類 left coset」, Hx の形の集合を「右剰余類 right coset」と呼ぶ.[27] 可換群 (アーベル群) の場合この左右の剰余類の区別は消失する. もし群 G が部分群 H を持てば, 上の (a),(b) は G が互いに交わり (共通元) のない左及び右剰余類の集合

$$G/H := \{eH = H, xH, yH, \cdots\} \text{ 及び } G\backslash H := \{He = H, Hx', Hy', \cdots\}$$

を持つ事を意味するが, 実は群 G はこれらによって余す元なく切り分けられると示されたのである. 群の部分群が作るこの重要な構造を次の形でまとめておこう:

Lemma 2.16. 任意の群 G 及びその任意の部分群 H について,
(a) 任意の $x \in G$ について $x \in xH$, $x \in Hx$ であり, G の任意元は H のある左剰余類に属

[26] $\cap$ は 2 つの集合の共通部分を, ϕ は空集合, 要素を含まない集合, をそれぞれ意味する. だから $xH \cap yH = \phi$ とは xH と yH の両方に属している元が 1 つもない事である.
[27] 左右の剰余類の定義をこれと逆にする教科書もある.

す. 即ち H の左剰余類は余す所も共通元もない G の完全な分割

$$G = H + aH + bH + \cdots$$

を与える. 同じ事が H の右剰余類について成り立つ.
(b) $x, y \in G$ が部分群 H に関する同一の左剰余類に属する必要十分条件は $x^{-1}y \in H$ の成立である.
(c) $x, y \in G$ が部分群 H の同一の右剰余類に属す必要十分条件は $xy^{-1} \in H$ である.
(証明) (a) H は部分群だから $e \in H$. 故に $xH \ni xe = x, Hx \ni ex = x$ で, G の任意元 x は必ずどれかの (左及び右の) 剰余類に属している. それが判れば Corollary 2.15.(a) から G が共通元もなく余す所もなく分割されてしまう事は明らか.
(b) (十分性の証明) $x^{-1}y \in H$ なら $y = x(x^{-1}y) \in xH$, 即ち y は x の属す左剰余類 xH に入っている. (必要性の証明) x は左剰余類 xH に, y は左剰余類 yH に属すから, x と y が同一の左剰余類に属すとすれば Corollary 2.15.(a) によって $xH \cap yH = \phi$ ではなく集合として $xH = yH$ である. 故に $h, k \in H$ が存在して $xh = yk$ が成り立つべきであり, $h = x^{-1}yk$, 即ち $x^{-1}y = hk^{-1}$ は H の元でなければならない.
(c) 上の (b) と同じ証明である. ■

この節の大眼目, ラグランジュの定理に達した:

定理 2.17.(Lagrange の定理) G は有限群, その元の数 (位数 order) を g とする. G の任意の部分群 H の位数 h は g を割り切る (g の約数である).
(証明) 群 G は互いに交わりのない左剰余類 $\{H, aH, bH, \cdots\}$ に切り分けられる. 剰余類 aH の 2 元は ax, ay (x, y は H の元) の形で, しかも群 G 内で一般に $ax = ay$ となるのは $x = y$ に限る (Corollary 2.2.(a)) から, $aH, bH, \cdots$ はすべて H と同じ h 個の異なる元を持つ. 故に G が位数有限の群の場合 $g = h \times$ (左剰余類の数) で, g は h の倍数である.[28] ■

証明は誠にあっけなく, 定理の姿は無味乾燥, 殆ど trivial で一見誠に頼りない. しかし乱数問題でのこの定理の役割は天網そのもので, それが以下の要所で与える限定は「疎にして漏らさず」と実感される事になる. 例えばすべての群には必ず次の部分群が含まれ, それが重要な限定を意味する:

定理 2.18. (巡回 (部分) 群 cyclic group) 有限の位数 g を持つ[29]群 G の任意元 x に対して G の部分集合 $H_x := \{x, x^2, x^3, \cdots\}$ を定義する.
(a) H_x は G の可換な部分群であり, 巡回群である. これを「x で生成される巡回群」と呼ぶ.
(b) 巡回群 H_x の位数 (元の数)h は「元 $x \in G$ の位数 order, $x^n = e$ となる整数 n の正の最小値」に等しい.
(c) 任意元 $x \in G$ の位数 (即ち巡回部分群 H_x の位数)h は g の約数に限られる. 特に $x^g = e$ がつねに成り立つ.
(証明) 以前我々は「群全体が 1 つの元 a の冪乗で生成される」という場合として「巡回群」をぼんやりと見た. ここでは x の冪乗の全体である H_x が群である事の証明から取り掛かる. 既に行われたいくつかの議論も確実な理解を求めて重複を恐れず再確認する.

---

[28] 部分群 H の剰余類の総数 g/h は「部分群 H の指数 index」と呼ばれる.
[29] ここでは下の「巡回 (部分) 群」を我々が主として応用を考える有限群 G の場合有効な形に取った. より一般に, 群 G の位数が ∞, 特に元 x の位数が ∞ の場合は $H_x := \{x^n | \ n = 0, \pm 1, \pm 2, \cdots, \ x^{-n} := (x^{-1})^n \ (n > 0)\}$ とおいて巡回群が定義される.

(a) 正整数 m, n について x^m は x を m 個掛合わせたものだから, G での結合法則により可換な指数法則 $x^m x^n = x^{m+n} = x^n x^m$ の成立は明らか. 故に H_x の 2 元 x^m, x^n に対して $x^m x^n = x^{m+n}$ は再び H_x の元で, H_x は G の群乗法で閉じている (公理 0 の成立). 結合法則は H_x を含む G で成り立つから H_x の元の間だけでも成立する (公理 1 の成立). G の異なる元は有限の g 個しかないのだから $H_x = \{x, x^2, x^3, \cdots\}$ がすべて異なる事はなく, $x^m = x^{m+n}$ となる $m, n \geqq 1$ は必ず存在し, 両辺に $(x^{-1})^m$ を掛けて $e = x^n$ となる $n \geqq 1$ の存在がわかる. この様な n の正の最小値 $h \geqq 1$ に対して

$$H_x = \{x, x^2, \cdots, x^{h-1}, x^h = e\}$$

である; 実際 $x^1, \cdots, x^h$ の中に同じものはなく[30] これから先は $x^{h+1} = ex = x$, $x^{h+2} = x^2, \cdots$ の繰り返しだから, である. H_x には単位元 $e = x^h$ が存在する (公理 2 の成立). $x^h = e$ の逆元はそれ自身だから $x^0 := e = x^h$ と定義すると, $1 \leqq j \leqq h$ の任意の j に対して x^j も x^{h-j} も H_x に所属して $x^j x^{h-j} = x^h = e$ が成り立ち, H_x のすべての元には逆元が存在する (公理 3 の成立). 故に H_x はアーベル群, G の可換な部分群である.
(b) Lemma 2.11.(a) の議論を上で繰り返して見た様に, $x^n = e$ となる n の正の最小値 h は巡回部分群 H_x の元の総数に等しい.
(c) Lagrange の定理 2.17. によって G の部分群である巡回部分群 H_x の位数, 即ち元 x の位数 h は g の約数に限られる. 故に $g = hg''$ となる正の整数 g'' があり, $x^g = (x^h)^{g''} = e^{g''} = e$ が成り立つ. ■

群 G を「素数 p に対する法 p の乗法の既約剰余群 $Z_p^* = \{1, 2, \cdots, p-1\}$」(問題 2.5.) に取れば位数 $g = p - 1$ で, 定理 2.18.(c) 後半はフェルマーの小定理 1.21 と同じ結論,

$$\text{「}Z_p^* = \{1, 2, \cdots, p-1\} \text{ の整数 } x, \text{ 或いは } p \text{ の倍数ではない}$$
$$\text{任意の整数 } x \text{ について } x^{p-1} \equiv 1 \pmod{p}\text{」}$$

を与える. 勿論, 一般に非可換な任意の群の巡回部分群と剰余類の構造とについてラグランジュの定理が意味する透視は, この結果の遥かな一般化である. ラグランジュの定理はフェルマーの小定理の次の様な方向への重要な一般化も容易に与える:

Corollary 2.19. 素数とは限らない一般の整数 m に対し, 整数 x で m と素な (共通素因数を持たない, $(x, m) = 1$ の) 任意のものは $x^{\phi(m)} \equiv 1 \pmod{m}$ を満たす.
(証明) m と素な任意の整数 x, $(x, m) = 1$, は位数 $\phi(m)$ の既約剰余群 $\boldsymbol{Z}_m^*$ の元である (問題 2.7.) から, 定理 2.18.(c) によって $x^{\phi(m)} \equiv 1 \pmod{m}$. ■

2.5. 演習問題

問題 2.20. (a) 素数の法 13 での乗法に関して $\boldsymbol{Z}_{13}^* = \{1, 2, \cdots, 12\}$ が群である事は一般に示されている. しかし抽象論では頭に入りにくい. 手を使って群の積の計算を行い, $\boldsymbol{Z}_{13}^*$ の 2 数 x, y の乗積表を算出せよ.

[30] Lemma 2.11.(a) で見た通り, 仮に $x^p = x^q$, $1 \leqq p \leqq q \leqq h$ となる整数 p, q があれば $x^{q-p} = e$, $0 \leqq q - p \leqq h-1$ となって $h > 0$ の最小性から $q - p = 0$.

(b) $\boldsymbol{Z}_{13}^*$ の任意の数 x のべき (冪) 乗 x^n の表も $1 \leqq n \leqq 12$ について作り, 各 x の位数 (法 13 で $x^h \equiv 1$ となる最小の $h \geqq 1$) を求めよ.

(解) (a) 乗積表は次の通り:

$x\backslash y$	1	2	3	4	5	6	7	8	9	10	11	12	逆数 x^{-1}
1	1	2	3	4	5	6	7	8	9	10	11	12	1
2	2	4	6	8	10	12	1	3	5	7	9	11	7
3	3	6	9	12	2	5	8	11	1	4	7	10	9
4	4	8	12	3	7	11	2	6	10	1	5	9	10
5	5	10	2	7	12	4	9	1	6	11	3	8	8
6	6	12	5	11	4	10	3	9	2	8	1	7	11
7	7	1	8	2	9	3	10	4	11	5	12	6	2
8	8	3	11	6	1	9	4	12	7	2	10	5	5
9	9	5	1	10	6	2	11	7	3	12	8	4	3
10	10	7	4	1	11	8	5	2	12	9	6	3	4
11	11	9	7	5	3	1	12	10	8	6	4	2	6
12	12	11	10	9	8	7	6	5	4	3	2	1	12

(b) べき (冪) 乗 x^n の表は上の乗積表からも見られるが, x^{n-1} に x を掛けて行けばよいのだから直接計算の方が簡単で, 特に $12 \equiv -1,\ 11 \equiv -2,\ \cdots$ 等の置き換えが役に立つ:

$x\backslash n$	1	2	3	4	5	6	7	8	9	10	11	12	x の位数
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	3	6	12	11	9	5	10	7	1	12
3	3	9	1	3	9	1	3	9	1	3	9	1	3
4	4	3	12	9	10	1	4	3	12	9	10	1	6
5	5	12	8	1	5	12	8	1	5	12	8	1	4
6	6	10	8	9	2	12	7	3	5	4	11	1	12
7	7	10	5	9	11	12	6	3	8	4	2	1	12
8	8	12	5	1	8	12	5	1	8	12	5	1	4
9	9	3	1	9	3	1	9	3	1	9	3	1	3
10	10	9	12	3	4	1	10	9	12	3	4	1	6
11	11	4	5	3	7	12	2	9	8	10	6	1	12
12	12	1	12	1	12	1	12	1	12	1	12	1	2

結果から見ると, 12 の約数 $\{1, 2, 3, 4, 6, 12\}$ のすべてがそれぞれ {1,1,2,2,2,4} 回ずつ $\boldsymbol{Z}_{13}^*$ の数の位数として登場している. **(問題 2.20. 終り)**

巡回群 $\boldsymbol{Z}_{13}^*$ の冪乗表の簡単な構造も, 乱数の立場から巡回群の特徴を見通させるよい例である:

問題 2.21. 冪乗表によれば, 群 $\boldsymbol{Z}_{13}^*$ の位数 (元の総数)$g = 12$ の任意の因数 $h = 1,\ 2,\ 3,\ 4,\ 6,\ 12$ の各々にはそれを位数に持つ $\boldsymbol{Z}_{13}^*$ の元 x が存在する. $\boldsymbol{Z}_{13}^*$ は巡回群である. この群の中の位数 h の元の個数を考える. $\boldsymbol{Z}_{13}^*$ の生成元の任意の 1 つを a, 例えば $a = 2$ を用いればこの群

の任意の元 x を $x=a^j$, $(1\leqq j\leqq g=12)$ と表す事 (巡回表現) ができる. Lemma 2.11.(a) により $1\leqq j<k\leqq g$ のすべての j,k について $a^j\neq a^k$ である. また Lemma 2.11.(b) は $(a^j)^h=a^{jh}\equiv 1$ となる jh を 12 の倍数以外にはないと限定し, j と $g=12$ の最大公約数を $d=(j,g)=(j,12)$ と置けば, $j=j'd,\ g=12=g'd$ として

$$jh=j'dh=g\text{ の倍数},\quad \frac{j'dh}{g}=\frac{j'dh}{g'd}=\frac{j'h}{g'}\text{ が整数,}$$

となる h の最小の正値が元 $x=a^j$ の位数である. j' と g' に共通因数はないからこの様な最小の正の h は $h=g'$ であり, $x=a^j\in \boldsymbol{Z}_{13}^*$ の位数 h は

$$h=g'=\frac{g}{(j,g)}=\frac{\text{群の位数 }g}{j\text{ と }g\text{ の最大公約数}}=\frac{12}{(j,12)}$$

で与えられる. 元 $x=a^j$ のこの位数 h は, $h(j,g)=g$ の関係からも定理 2.18.(b) からも, g の約数でなければならない.

視点を変えて群の位数 g の約数である任意の h を固定し, これを位数に持つ様な $\boldsymbol{Z}_{13}^*$ の元 x の個数を考えよう. $h|g$ だから今度は $g=12=g''h$ と分解すると見やすい. 位数 h を持つ元の冪乗表現 $x=a^j$ を考えると, 上の議論からその指数 j は関係式

$$h=\frac{\text{群の位数 }g}{j\text{ と }g\text{ の最大公約数}}=\frac{g}{(j,g)},\quad \text{即ち } (j,g)=(j,g''h)=\frac{g}{h}\text{=}g''$$

を満たすものであり, その様なもの以外にはない. 即ち j は h と素な数 j'' と g'' との積で, かつ $1\leqq j=j''g''\leqq g=g''h=12$ の範囲にあるものである. こうして位数 h の a^j を与える j の総数は $1\leqq j''\leqq h$ であって h とは素な j'' の総数, オイラーの関数の値 $\phi(h)$ の定義そのもの, に等しいとわかった. まとめれば

(a) 巡回群 $\boldsymbol{Z}_{13}^*$ の数 x の位数は $g=12$ の約数 h に限られ,

(b) 群の位数 $g=12$ の任意の約数 h に対して, 位数 h の元は群の中に $\phi(h)$ 個存在する.

12 の因数 1, 2, 3, 4, 6, 12 の各々を位数に持つ $\boldsymbol{Z}_{13}^*$ の元 x とその総数を上の議論で算出し, 冪乗表と対照しなさい.

(解) (i) 「$\boldsymbol{Z}_{13}^*$ の位数 $h=1$ の数の総 数」$=\phi(1)=\sharp\{1\}=1$, $j''=1$, $j=j''\dfrac{g}{h}=j''\times 12=12$, $\quad x=2^j=2^{12}\equiv 1$.

(ii) 「$\boldsymbol{Z}_{13}^*$ の位数 $h=2$ の数の総 数」$=\phi(2)=\sharp\{1\}=2(1-\dfrac{1}{2})=1$, $j''=1$, $j=j''\dfrac{g}{h}=j''\times 6=6$, $\quad x=2^j=2^6\equiv 12\equiv -1$.

(iii) 「$\boldsymbol{Z}_{13}^*$ の位数 $h=3$ の数の総 数」$=\phi(3)=\sharp\{1,2\}=3(1-\dfrac{1}{3})=2$, $j''=1,\ 2$, $j=j''\dfrac{g}{h}=j''\times 4=4,\ 8$, $\quad x=2^j=2^4\equiv 3, 2^8\equiv 9$.

(iv) 「$\boldsymbol{Z}_{13}^*$ の位数 $h=4$ の数の総 数」$=\phi(4)=\sharp\{1,3\}=4(1-\dfrac{1}{2})=2$, $j''=1,\ 3$, $j=j''\dfrac{g}{h}=j''\times 3=3,\ 9$, $\quad x=2^j=2^3\equiv 8, 2^9\equiv 5$.

(v) 「$\boldsymbol{Z}_{13}^*$ の位数 $h=6$ の数の総 数」$=\phi(6)=\sharp\{1,5\}=6(1-\dfrac{1}{2})(1-\dfrac{1}{3})=2$, $j''=1,\ 5$,

$j = j'' \dfrac{g}{h} = j'' \times 2 = 2,\ 10, \quad x = 2^j = 2^2 \equiv 4,\ 2^{10} \equiv 10.$

(vi) 「$\boldsymbol{Z}_{13}^*$ の位数 $h = 12$ の生成元の総 数」$= \phi(12) = \sharp\{1, 5, 7, 11\} = 12(1 - \dfrac{1}{2})(1 - \dfrac{1}{3})$
$= 4$, $j'' = 1,\ 5,\ 7,\ 11$, $j = j'' \dfrac{g}{h} = j'' = 1,\ 5,\ 7,\ 11, \quad x = 2^j = 2^1 \equiv 2,\ 2^5 \equiv 6,\ 2^7 \equiv 11,$
$2^{11} \equiv 7.$

これらは冪乗表の通りである. また総数 $1 + 1 + 2 + 2 + 2 + 4 = 12$ は $\boldsymbol{Z}_{13}^*$ の位数 (元の総数) と合致する. この最後の内容は次の章の Lemma 3.3. でオイラーの関数の一般的性質として理解される. **(問題 2.21. 終り)**

問題 2.22. 群 G の位数を $g = \mathrm{ord}(G) \geqq 2$ として,
(a) 群 G の位数 g が素数 $2, 3, 5, \cdots$ なら G は巡回群でありアーベル群であって, 単位元以外の $g - 1$ 個の任意元 x は生成元である事を示せ.
(b) 任意の群 G に対して, 単位元だけの集合 $\{e\}$ は G の部分群で, また $G \subset G$ でもあるから G 自身は自分の部分群ではある. 全体 G と $\{e\}$ とは群 G の「自明な部分群」と呼ばれる. 位数 2 以上の群 G が自明な部分群以外に部分群を持たない事と, 群 G の位数が素数である事は同値である. これを示せ. なおこの時 G は巡回群である事も示せ.
(証明) (a) $g \geqq 2$ だから単位元 e 以外の元がある. その任意の 1 つを x とすると, x の生成する巡回群 H_x の位数 h は 1 より大きい g の約数であり, g が素数だから $h = g$ 以外はあり得ない. 故に $\mathrm{ord}(x) = \mathrm{ord}(G)$, であり, Lemma 2.11.(c) によって x は G の生成元, G は巡回群でアーベル群である. $\mathrm{ord}(x) = \mathrm{ord}(G)$ のこの議論は x が単位元でなければ成り立つから, 素数位数 g の群 G の e 以外の $g - 1$ 個の元は皆生成元である.
(b) 自明な部分群以外持たない群 G の位数が 2 以上だとする. G には単位元以外の元 x があってその位数は 2 以上, x の生成する巡回部分群 H_x の元の総数は必ず 2 以上である. 故に H_x は自明な部分群 $\{e\}$ ではなく, 残る唯一の部分群 G そのもので $H_x = G$ が成り立つ. 即ち G は単位元以外の任意の元を生成元とする巡回群である. 仮に $g = \mathrm{ord}(G)$ が素数でなく因数 $m, n \geqq 2$ で $g = mn$ と分解されるなら, 任意の $x \neq e$ について $\mathrm{ord}(x) = g = mn$, かつ $y = x^m \neq e$ の作る巡回部分群 H_y の位数は $n = \dfrac{g}{m}$, $2 \leqq n \leqq \dfrac{g}{2} < g$ で G の自明でない部分群であって, G の部分群についての仮定に矛盾する. 故に G の位数 g は素数でなければならない. 逆に G の位数 $g \geqq 2$ が素数なら, G の任意の部分群 H の位数 h は g の約数なのだから (Lagrange の定理 2.17.)$h = g$ 或いは $h = 1$ で H は G であるか $\{e\}$ かであり, 群 G には自明な部分群以外存在しない. ■

勿論, 巡回群の位数が常に素数なのではなく, 我々の用いる多くの巡回群の位数は合成数である. 法 13 での乗法群 $\boldsymbol{Z}_{13}^*$ は位数 $g = 12$ で, g の約数と対応する部分群の多い良い例だった. その部分群による剰余類構造も直接目で見ておこう.

問題 2.23. $\boldsymbol{Z}_{13}^*$ の数 5 のべき (冪) 乗全体を $H_5 := \{5, 5^2, 5^3, 5^4, \cdots\}$ とする. H_5 がどの様な数で構成されるかを下の欄に書込み, H_5 の任意の 2 数 x, y の法 13 での乗積表を下に作れ.

(解) 計算は容易である:

$x\backslash y$	$1\equiv 5^4$	5	$5^2\equiv 12$	$5^3\equiv 8$	x^{-1}
$1\equiv 5^4$	1	5	12	8	1
5	5	12	8	1	8
$5^2\equiv 12$	12	8	1	5	12
$5^3\equiv 8$	8	1	5	12	5

(問題 2.23. 終り)

問題 2.24. 上の表から H_5 が群である (従って $\boldsymbol{Z}_{13}^*$ の部分群である) 事を示せ.
(証明) 群の公理の成立を乗積表から示せばよい.
[公理 0 の成立] 乗積表から, $H_5=\{1,5,8,12\}$ は法 13 の乗法で閉じている.
[公理 1 の成立] 普通の乗法で成り立つ結合法則は, 法 13 でも成り立つ.
[公理 2 の成立] $1\equiv 5^4$ が H_5 に存在する.
[公理 3 の成立] 乗積表から, 法 13 での逆元は H_5 のすべての数に存在する. ■

問題 2.25. $\boldsymbol{Z}_{13}^*$ の数 a を部分群 H_5 に掛けてできる剰余類 (集合)

$$aH_5=H_5a=\{a\cdot 5, a\cdot 5^2, a\cdot 5^3,\cdots\}$$

を考える. 例えば $a=1$ なら明らかに $aH_5=1H_5=H_5$ であり, a が H_5 の他の任意の数 $5,5^2,\cdots$ でも, aH_5 は (a) の乗積表の各行が示す通り (部分) 群 H_5 の元の並べ変えで, すべて $aH_5=H_5$ である. a として $\boldsymbol{Z}_{13}^*=\{1,2,3,\cdots,12\}$ の他の数も取り, 具体的に aH_5 がどのような元を含む集合になるかを各 aH_5 に所属する数の欄に○を記入して求めなさい.
(解) 実際に aH_5 をそれぞれ計算すれば:

aH_5	1	2	3	4	5	6	7	8	9	10	11	12
$1H_5$	○				○			○				○
$2H_5$		○	○							○	○	
$3H_5$		○	○							○	○	
$4H_5$				○		○	○		○			
$5H_5$	○				○			○				○
$6H_5$				○		○	○		○			
$7H_5$				○		○	○		○			
$8H_5$	○				○			○				○
$9H_5$				○		○	○		○			
$10H_5$		○	○							○	○	
$11H_5$		○	○							○	○	
$12H_5$	○				○			○				○

確かに剰余類は $\boldsymbol{Z}_{13}^*$ の互いに共通元のない分割を与えている. **(問題 2.25. 終り)**

問題 2.26. $2^n-1,\ n\geqq 1$ の形の素数は Mersenne 数と呼ばれた. 一方 $2^e+1,\ e=1,2,3,\cdots$ の形の素数もあり, フェルマー Fermat(素) 数と呼ばれる.
(a) 奇数の $e\geqq 3$, $e=2m+1,\ m=1,2,\cdots$ について, 次の因数分解を示しなさい:

$$x^e+1=x^{2m+1}+1=(x+1)(x^{2m}-x^{2m-1}+x^{2m-2}-x^{2m-3}+\cdots-x+1).$$

(b) フェルマー素数 2^e+1 では指数 e は 2 の冪乗, $e=2^n$ の形, に限る事を示しなさい.
(証明) (a) 素直に右辺の積を取れば,

$$\begin{aligned}&(x+1)(x^{2m}-x^{2m-1}+x^{2m-2}-x^{2m-3}+\cdots-x+1)\\&\quad=(x^{2m+1}-x^{2m}+x^{2m-1}-x^{2m-2}+\cdots+x)\\&\qquad+(x^{2m}-x^{2m-1}+x^{2m-2}-\cdots-x+1)=x^{2m+1}+1.\end{aligned}$$

(b) 整数 $e\geqq 1$ は一般に $e=2^n f$, $n\geqq 0$, $f\geqq 1$ は奇数, と表される. この表現を用いて

$$2^e+1=2^{2^n f}+1=(2^{2^n})^f+1$$

を考えると, それが素数なら $f\geqq 3$ はあり得ない; 実際 $f\geqq 3$ なら (a) で見た因数分解

$$2^e+1=(2^{2^n})^f+1=(2^{2^n}+1)\{(2^{2^n})^{f-1}-(2^{2^n})^{f-2}+(2^{2^n})^{f-3}-\cdots-2^{2^n}+1\}$$

が成り立ち, 右辺は合成数になる. 故にフェルマー素数 2^e+1 では $f=1$ で $e=2^n$ となる事が必要である; 十分ではないが. ■

始めのいくつかのフェルマー数は

$$2^{2^0}+1=3,\quad 2^{2^1}+1=5,\quad 2^{2^2}+1=17,\quad 2^{2^3}+1=257,\quad 2^{2^4}+1=65537$$

である. フェルマーは $2^{2^n}+1$ の形の数は皆素数だと予想した. しかしオイラーが

$$2^{2^5}+1=2^{32}+1=4294967297=641\times 6700417$$

を発見して予想は成り立たない, と示したという.[7)]

問題 2.27. フェルマー素数 p を法にすると $\boldsymbol{Z}_p^*$ の部分群の構造が少し特殊になる. 簡単過ぎない最小のフェルマー素数 p として $p=17=2^{2^2}+1$ を取り, 乗法群 $\boldsymbol{Z}_{17}^*$ が 3 を生成元として持つ巡回群である事を確認し, 部分群の位数構造を議論しなさい.
(解) 法 17 での 3 の冪乗計算は

$$\begin{aligned}&3^1=3,\ \ 3^2=9,\ \ 3^3\equiv 10\equiv -7,\ \ 3^4\equiv -4\equiv 13,\ \ 3^5\equiv -12\equiv 5,\ \ 3^6\equiv 15\equiv -2,\\&3^7\equiv -6\equiv 11,\ \ 3^8\equiv -1\equiv 16,\ \ 3^9=-3\equiv 14,\ \ 3^{10}=-9\equiv 8,\ \ 3^{11}\equiv 7,\\&3^{12}\equiv 4,\ \ 3^{13}\equiv 12\equiv -5,\ \ 3^{14}\equiv -15\equiv 2,\ \ 3^{15}\equiv 6,\ \ 3^{16}\equiv 18\equiv 1.\end{aligned}$$

確かに $\boldsymbol{Z}_{17}^*$ での 3 の位数は最大の 16, 3 は生成元で, $\boldsymbol{Z}_{17}^*$ は巡回群である. 17 がフェルマー数であるために $\mathrm{ord}(\boldsymbol{Z}_{17}^*)=17-1=16=2^4$ だから, ラグランジュの定理はその部分群の位数, 或いは $\boldsymbol{Z}_{17}^*$ の各元 (の作る巡回部分群) の位数を 2 の冪乗だけに限定してしまう. $\phi(2^n)=2^n\Big(1-\dfrac{1}{2}\Big)=2^{n-1}$ $(n\geq 1)$ を用いて各位数の元の個数等を見れば,

位数 $1=2^0$ の元の総数 $\phi(1)=1$, この元は 1,
位数 $2=2^1$ の元の総数 $\phi(2)=1$, この元は $16\equiv -1$,
位数 $4=2^2$ の元の総数 $\phi(4)=2$, 元は $\{4,\,13\}$,
位数 $8=2^3$ の元の総数 $\phi(8)=4$, 元は $\{2,\,8,\,9,\,15\}$,
位数 $16=2^4$ の生成元の総数 $\phi(16)=8$, 元は $\{3,\,5,\,6,\,7,\,10,\,11,\,12,\,14\}$.

法 17 のすべての元の冪乗計算での, 或いは問題 2.21. と同様の議論での, これらの結果の確認は容易である. 試みて頂きたい. **(問題 2.26. 終り)**

$\boldsymbol{Z}_{17}^*$ もこの様に巡回的である. 素数 $p = 17$ がフェルマー素数であるために $p - 1$ は素因数を 2 しか含まず, $\boldsymbol{Z}_{17}^*$ の生成元の数 $\phi(p-1) = \dfrac{p-1}{2}$ は群の全ての元の半数と多い.

3. 乱数の乗算合同法

前節では素数の法 p での乗法で整数全体から 0 を除いたものは群 $\boldsymbol{Z}_p^*$ を作る事が示され, 群 G の 1 つの元 x から生成される巡回部分群 H_x も議論された. 我々が得た知識は一様乱数生成にとっては大きい. 素数 p を法とする乗算合同法

$$x_k = ax_{k-1} \pmod p \quad 1 \leqq k \leqq p-1,$$

とその解 $x_k \equiv a^k x_0$ とは群 $\boldsymbol{Z}_p^*$ の元 a が作る巡回部分群

$$H_a := \{a, a^2, \cdots, a^T \equiv 1\}, \quad T = \mathrm{ord}(a)$$

の要素を出発値 $x_0 \in \boldsymbol{Z}_p^*$ に次々に掛けて得られる系列, 群 $\boldsymbol{Z}_p^*$ の部分群 H_a が作る剰余類 $H_a x_0$, を遍歴するものだと透視された. 部分群 H_a の剰余類はすべて H_a と同数の元を持つから, 初期値 x_0 の選択は乱数の周期 T を変えず, T は乗数 a の群 $\boldsymbol{Z}_p^*$ での位数で決まり, 群の位数, 現在の $\boldsymbol{Z}_p^*$ では $p-1$, の約数に限られ (Lagrange の定理), それを満たす位数 T の元は**もし群が巡回的なら** $\phi(T)$ 個ある $\cdots$, もわかった. 最大の周期を得るには最大位数の乗数 a, 巡回群なら生成元, を選べばよい. 我々はアーベル群が巡回的とは限らない事を見たが, 同時に $\boldsymbol{Z}_7^*$, $\boldsymbol{Z}_{13}^*$ や $\boldsymbol{Z}_{17}^*$ が巡回群である事も冪乗計算から知った.

法を素数ではなく, 例えば $m = 2^r$ とする方式もある乗算合同法乱数では, ある法 m で対象となる数体系に巡回群の構造があるかないかは本質的な問題で, その確かな見通しが欠かせない. 以下我々は任意の素数 p に対しては群 $\boldsymbol{Z}_p^*$ は巡回的である事を示し, また法 2^r での最大位数の乗数も発見する. これらは正面から解かれる最初の乱数問題である. 勿論問題は続く. 大きい素数, 例えば $p = 2^{31} - 1 = 2147483647$, に対する $\boldsymbol{Z}_p^*$ の $\phi(p-1)$ 個の生成元の中から, 乱数生成のためにはどれを選ぶべきだろうか？ これが乗算合同法を締めくくる次の章の重要な課題である.

3.1. 巡回群の条件と素数の法 p での原始根の存在

まず巡回群の少し詳しい構造から始める. 次の諸命題はそれらの間だけでも, 或いは前節までの諸命題や演習問題とも, 少しずつ重複を持つが, 理解を第 1 に目指して繰返しを避けずに述べる.

定理 3.1. G は位数 g の巡回群, a は G の生成元の任意の 1 つとする.

(a) G の一般元 $a^j (1 \leqq j \leqq g)$ の位数 h は $h = \dfrac{g}{(j,g)}$, (j,g) は j と g の最大公約数, である. 特に j が g と素で $(j,g) = 1$ である事が a^j が生成元である必要十分条件である.
(b) G の任意元の位数 h は g を割り切り, 逆にその様な任意の正整数 h, $h|g$, に対して G の元で位数が h であるものは存在して総数は $\phi(h)$ である. 特に G の生成元の数は $\phi(g)$ である.
(c_1) 巡回群 G の任意の部分群も巡回群で,
(c_2) g を割り切る任意の正整数 h, $h|g$, に対し位数 h の部分 (巡回) 群はただ 1 つ, しかも必ず存在する.

(証明) (a) a は生成元だから, $1 \leqq j \leqq g$ に対して $(a^j)^h = a^{jh} = e$ となるのは g が jh を割り切

る時でありその時に限る. $d=(j,g)$, $g=g'd$, $j=j'd$ と置くと g' と j' は素で共通因数を持たず, $h=\mathrm{ord}(a^j)$ は $\dfrac{jh}{g}=\dfrac{j'dh}{g'd}=\dfrac{j'h}{g'}=$整数, となる最小の h, $h=g'=\dfrac{g}{(j,g)}$ で与えられる. この関係によれば a^j が位数 g の生成元である事, $h=\mathrm{ord}(a^j)=g$, と $(j,g)=1$ の同値は明らか.
(b) G の任意元の位数 h が g を割り切る事は Lagrange の定理の結論である. 逆にこの様な任意の $h|g$ に対し G の中で位数 h を持つ元の数は (a) によって,

$$\text{整数 } j(1\leqq j\leqq g) \text{ で } h=\frac{g}{(j,g)} \text{ となるもの, 或いは } (j,g)=\frac{g}{h} \text{ となるもの}$$

の数である. h が g を割り切るから $g=g''h$ と置くと, 上の j は

$$j \text{ と } g''h \text{ との最大公約数 } (j,g''h) \text{ が } \frac{g}{h}=g'' \text{ であるもの,}$$

と言う事ができ, それは h と素な j'' によって $j=j''g''$ と表されるものがすべてで, しかも $1\leqq j=j''g''\leqq g=g''h$ なのだから $1\leqq j''\leqq h$ でなければならない. 故に

$$\text{求める位数 } h \text{ の元の数} = \text{この様な } j \text{ の総数} = \text{この様な } j''\text{の総数} = \phi(h)$$

である. 特に「位数 g の元の数 = 巡回群 G の生成元の数」は $\phi(g)$ で与えられる.
(c$_1$) 巡回群 G の任意の部分群 H を取る. $H=\{e\}$ なら命題の成立は自明だから $h=\mathrm{ord}(H)\geqq 2$ の場合を仮定しよう. G の生成元を a とする. $\mathrm{ord}(G)\geqq\mathrm{ord}(H)\geqq 2$ から $a\neq e$ である. $a^j\in H$ となる指数 $1\leqq j\leqq g$ の全体を J_H と記そう: $H=\{a^j|\ j\in J_H,\ a^g=e\}$. J_H の正の最小数を $i\geqq 1$ と置く; $a^i\in H$. 任意の正の整数 k について $(a^i)^k=a^{ik}$ は部分群 H の中の元 a^i の k 乗として H の元で, i のすべての倍数 ki も J_H に属している. 実はこの ki の形の整数が J_H のすべてである.[31] これを示すために任意の $j\in J_H$ を取り, j を i で割って $j=iq+r$, 余り r は $0\leqq r<i$, と置こう; H は部分群で $a^j,\ a^i,\ (a^i)^{-1}\equiv a^{g-i}$ を含むから

$$a^j\{(a^i)^{-1}\}^q=a^j(a^{g-i})^q=a^{j+gq-iq}=(a^g)^qa^r=a^r$$

も H に属し r も J_H に入る; しかし $i\in J_H$ の最小性から i より小さい $r>0$ が J_H に存在する事はできず $r=0$ である. これで任意の $j\in J_H$ は i で割り切れ, i の倍数 ki に限られ, $J_H=\{ki|\ k=1,2,\cdots\}$, $H=\{(a^i)^k|\ k=1,2,\cdots\}$ である事がわかった. 巡回群の任意の部分群 H は必ず (a^i を生成元とする) 巡回群の構造を持つ.

(c$_2$) G の生成元 a を任意に取り, g を割り切る任意の h, 即ち $h|g$ に対し $g''=\dfrac{g}{h}$, $b=a^{g''}$ とすれば $\mathrm{ord}(b)=h$, $H_b=\{b,b^2,\cdots,b^h=e\}$ が位数 h の部分巡回群として G 内に存在する. 巡回 (部分) 群 H_b には生成元 (位数 h の元) が (b) により $\phi(h)$ 個あるが, これらは同じ (b) により G 中の位数 h の元のすべてである. 故に G 中に位数 h の他の (巡回) 部分群はあり得ない. ■

1 の g 乗根の乗法群の存在からどんな正の整数 g に対しても位数 g の巡回群 G は存在する. これは明らかだが, 別の重要な具体例でこの内容を上の構造と共に反芻する.

[31] 指数の集合 J_H は実は法 g の加法に関する整数の群 $\boldsymbol{Z}/g$ の部分群であって, ここでの J_H の性質, 或いは (c$_1$) の事柄全体はそれに基づいても導かれる. 巡回 (部分) 群とこの様な整数の加法の群とは次の頁に記す重要な対応を常に持つ.

Corollary 3.2. 任意の正の整数 g に対して, $\boldsymbol{Z}/g = \{0, 1, 2, \cdots, g-1\}$ は「0 を単位元とする法 g での加法の下で」位数 g の巡回群であって,

(a) g と素, 即ち $(j, g) = 1$ の $\phi(g)$ 個の整数 j, $1 \leqq j \leqq g$, がその生成元のすべてであり,

(b) g の任意の約数 h に対し $\boldsymbol{Z}/g$ の中に法 g の加法での位数 h の元が $\phi(h)$ 個存在する.

(証明) $\boldsymbol{Z}/g = \{0, 1, 2, \cdots, g-1\}$ が加法で群である事は問題 2.4. で見られた. 数 1 はその加法 (即ち「群の乗法」) で $1^2 = 1+1 = 2$, $1^3 = 1+1+1 = 3$, $\cdots$ と群 $\boldsymbol{Z}/g$ 全体を生成する生成元であり $\boldsymbol{Z}/g$ が巡回群である事は自明である. 故に定理 3.1. の結論は有効で, (a),(b) は $\boldsymbol{Z}/g$ でも成り立つ. ■

位数 g 有限の巡回群 G では[32]その任意の元 x に生成元 a による巡回表現 $x = a^j$ が与えられる. 但し $a^{g+j} = a^g a^j = a^j$ だから指数 j としては法 g での値だけが意味を持ち, 有限巡回群 G ではその 1 つの生成元 a を定めて群全体が法 g の整数の集合 $\boldsymbol{Z}/g$ に 1 対 1 に対応する. 生成元 a はこの対応の底 base と呼ばれ, $x = a^j$ となる指数 j を $j = \log_a x$ と書いて「生成元 a を底とする $x \in G$ の対数」と呼ぶ. 名前の通り, G と $\boldsymbol{Z}/g$ とのこの対応には次の特徴的な働きがある:

> 任意の $x = a^j,\ y = a^k \in G$ に対し, 積 xy は $xy = a^j a^k = a^{j+k}$ と
> なる, 即ち $\log_a(xy) = \log_a x + \log_a y \pmod{g}$ が成り立つ.

$\log_a$ は群 G から群 $\boldsymbol{Z}/g$ へ 1 対 1 に, G での 2 元の群演算, 乗法, の結果を各元の対応物の群 $\boldsymbol{Z}/g$ 内での群演算 $+$ の結果に写し, 特に単位元 $e = a^g \in G$ を単位 (零) 元 $0 \equiv g \in \boldsymbol{Z}/g$ に, 逆元 $x^{-1} \in G$ を負元 $-j \equiv g - j \in \boldsymbol{Z}/g$ に写す. これは群の (演算を保つ) 同形対応と呼ばれる. 我々は次の構造を知った: **位数 g のすべての巡回群は巡回加法群 $(\boldsymbol{Z}/g, +)$ と同形であり, これを通して (或いはそれぞれの巡回表現の直接比較からも) 位数 g のすべての巡回群は互いに同形である**. この事実は例えば定理 3.1.(c_1) の証明を明快に統一するが,[20] 以後この知識を使う場面は余りないので我々はこれ以上は立ち入らない.

一般に位数有限の群が巡回群であるための条件を見て, 眼目の乱数問題, 素数 p に対する $\boldsymbol{Z}_p^*$ の巡回性の確認, を完全に解こう. この条件の導出[20] はある補助命題から始める.

Lemma 3.3. オイラーの関数 ϕ と任意の正の整数 g について次が成り立つ:

$$\sum_{n|g} \phi(n) = g.$$

ここで和は g を割り切るすべての整数 $1 \leqq n \leqq g$ にわたる.

(証明) 与えられた g に対して位数 g の巡回群 G, 例えば前 Corollary 3.2. の例 $\boldsymbol{Z}/g$, を取ると, 定理 3.1.(b) と Lagrange の定理の与える制限とによって

$$G \text{ の元の総数 } g = \sum_{n=1}^{g} (G \text{ の位数 } n \text{ の元の数}) = \sum_{n|g} \phi(n)$$

が成り立つ. ■

面白いが余り役に立ちそうにも見えない ϕ のこの性質が, 任意の (可換とも限らない) 有限群が巡回群である (従って結果としてアーベル群にもなる) 条件を平易強力に与える:[20]

---

[32] g が有限でなくても任意の巡回群は生成元による巡回表現を持つが, 有限の g は対応する指数を我々には親しい $(\boldsymbol{Z}/g, +)$ に限り議論を簡単にするので以下位数有限と限定する.

定理 3.4. 位数 g 有限の群 G が巡回群であるための必要十分条件は, G 上の (即ち G の元 x に対する) 方程式 $x^n = e$, $x \in G$, の異なる解の数が任意の $n = 1, 2, \cdots$ に対して n 以下である事, である.

(証明) $g = 1$ なら $G = \{e\}$ で定理は自明だから $g \geqq 2$ とする.

(必要性) G は巡回群, a をその生成元とする. 与えられた $n \geqq 1$ に対し G の一般元 $x = a^j$ $(1 \leqq j \leqq g)$ が方程式 $x^n = a^{jn} = e$ を満たすのは jn が g の倍数の場合に限る. jn の値が含まれる範囲[33] $[n,\, ng\,]$ を含む $[\,1, ng\,]$ に g の倍数は上限の ng から下向きに数えて高々 n 個しかなく, それらに対応する方程式 $x^n = e$ の G での解の個数は当然 n 以下である.

(十分性) 位数 g の群 G での方程式 $x^n = e$ の異なる解の数が任意の $n = 1, 2, \cdots$ について n 以下であると仮定する. G が巡回群かどうか, まして可換群かどうかはまだわからないから, G の位数 n の元の数を $\psi(n)$ と記そう. それでも Lagrange の定理は強力に成り立って, g を割り切らない n については $\psi(n) = 0$ を保証する. だから

$$\sum_{n=1}^{g} \psi(n) = \sum_{n|g} \psi(n) = g.$$

第 2 の和は $n|g$ である (g を割り切る)n の上だけにわたる. $\psi(n) \geqq 1$ なら n は g を割り切り, 位数 n の G の元 a があり, a は位数 n の巡回 (部分) 群 $H_a = \{a^1, a^2, \cdots, a^n = e\}$ を生成する. H_a の各元 a^j はそれぞれ方程式 $x^n = (a^j)^n = a^{jn} = (a^n)^j = e^j = e$ を満たし全体で n 個あるから, 仮定からこれらが G での方程式 $x^n = e$ の解のすべてである. 故に G の位数 n の元 $\psi(n)$ 個はみなこの巡回群 H_a 中に含まれ, H_a に存在する $\phi(n)$ 個の生成元 (定理 2.26.(b)) の全体と一致して $\psi(n) = \phi(n)$ となる. $\psi(n) = 0$ の場合も含めれば $\psi(n) \leqq \phi(n)$ が常に成り立ち, 上の式と Lemma 3.3. とから

$$g = \sum_{n|g} \psi(n) \leqq \sum_{n|g} \phi(n) = g.$$

即ちすべての $n|g$ について $\psi(n) = \phi(n)$ で, 特に $\psi(g) = \phi(g) \geqq 1$ でなければならない. こうして仮定は G が位数 g の生成元 a を持つ事, 巡回群である事, 当然アーベル群でもある事を意味すると示された. ■

今や問題 2.5. の素数 p の法での整数の乗法群

$$\boldsymbol{Z}_p^* = \{1, 2, \cdots, p-1\}$$

の巡回性, 即ち法 p での原始根の存在, の理解は容易である. 第 1.2 節で我々は文字 z の整数係数の多項式の法 m での同値をその係数の $\bmod m$ での同値で, 従ってその次数は法 m で 0 ではない係数を持つ項 z^n の最大の n で定義し, 一般の法での因数分解の一意性の不成立など奇妙な事態と共に素数の法 p での事柄の簡単化を認識した. 現在の知識からはそれは素数の法 p による整数の類別が乗法群 $\boldsymbol{Z}_p^*$ を与えるためだと概括でき, そこで得られた定理 1.13.,

「素数の法 p での n 次整数係数代数方程式 $f(z) \equiv 0$ の整数解は高々 n 個しかない」,

は乗法群 $\boldsymbol{Z}_p^*$ の巡回性の必要十分条件,

「方程式 $z^n - 1 \equiv 0 \pmod p$ が n 個以下の解しか $\boldsymbol{Z}_p^*$ で持たない」

[33] 実数 x の範囲 $a \leqq x \leqq b$ を「閉区間 closed interval」と言って $[a, b]$ と記す. 同様に範囲 $a < x < b$ は「開区間 open interval」で (a, b) と記される.

事を保証していると理解される. 故に:

定理 3.5. 任意の素数 p を法とする乗法について:
(a) 群 $\boldsymbol{Z}_p^* = \{1, 2, \cdots, p-1\}$ は巡回群であり, その位数 $p-1$ の生成元 a は必ず存在する. それを「法 p での原始根 primitive root」とも呼ぶ.
(b) $\boldsymbol{Z}_p^*$ の原始根のすべては, 任意生成元を a として

$$R := \{a^k | \ k \text{ は } p-1 \text{ と素}, \ (k, p-1) = 1, 1 \leqq k \leqq p-1\}, \quad \sharp R = \phi(p-1),$$

で与えられる. 特に a と共にその逆数 $a^{-1} \equiv a^{p-2}$ も原始根である.
(証明) (a) 既に述べた様に定理 1.13. から明らか.
(b) 前半は定理 3.1.(a) で見られた. a が原始根の時 $1 \leqq k \leqq p-2$ に対して $a^k (a^{-1})^k = e$, $a^k \neq e$ だから $(a^{-1})^k \equiv e \pmod{p}$ ではあり得ない. これは $a^{-1} \equiv a^{p-2}$ も位数 $p-1$ の原始根である事を示す. ■

原始根の総数 $\phi(p-1)$ が実際にどれくらいのものになるかを例で考えよう:

問題 3.6. 素数 $p = 2^{31} - 1 = 2147483647$ に対する乗法群 $\boldsymbol{Z}_p^*$ を考える. 位数 $p-1$ は

$$p - 1 = 2147483646 = 2 \times 3^2 \times 7 \times 11 \times 31 \times 151 \times 331$$

の素因数分解を持つ.[34] この群の生成元, 原始根の総数を求めなさい.
(解) オイラーの関数 $\phi(p-1) = \phi(2147483646)$ を計算すればよい. この場合は 10 桁以上の電卓があれば, 与えられた素因数分解から次の計算が正確にできる; 8 桁では危ういが例えば数を 2 つに分けて行う等の方法がある.[35] 手で行うのも可能である.

$$\begin{aligned}
&\phi(2147483646) \\
&= 2147483646(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{7})(1 - \frac{1}{11})(1 - \frac{1}{31})(1 - \frac{1}{151})(1 - \frac{1}{331}) \\
&= 534600000.
\end{aligned}$$

(問題 3.6. 終り)

大きい素数 p に対する $\phi(p-1)$ の傾向は上の計算から見られる. $p = 2^{31} - 1 = 2147483647$ は実際によく用いられる法の素数の 1 つで, 計算された原始根 (生成元) a の総数は $\mathrm{ord}(\boldsymbol{Z}_p{}^*) = p - 1 = 2147483646$ の 24.89% に当たり十分沢山あって, でたらめに $\boldsymbol{Z}_p^*$ の数を乗数に取っても約 $\frac{1}{4}$ の確率で原始根に当る. 一般に任意の素数 $p > 2$ では $p-1$ は必ず偶数で素因数 2 を含み, オイラーの関数の計算には因数 $1 - \frac{1}{2} = \frac{1}{2}$ が入って不等式 $\phi(p-1) \leqq \frac{p-1}{2}$ は常に成り立つ; フェルマー素数 p ならこれは等式で成り立つ. あと $p-1$ に他の素因数, 特に小さいもの, がそれほどなければ $\phi(p-1)$, 従って発見確率, は例からそう遠くはない値である. しかしこれは素数すべてについて成り立つ事ではなく, 自然或いは神は甘くはない. 乗算合同法乱数の法として性質が良いか, 或いは実用になるかは別として, 大きい素数 p の中には $p-1$ に非常に多くの素因数を持つものもあって, 上の発見確率が任意に小さい素数も (理論的には) 存在する; 例えば Koblitz[7] の Proposition II.1.3. 参照.

[34] この形の数の素因数分解は, 今の場合現用のパソコンで繰返して割り算を試みても容易にできるが, もっと桁数の大きい場合も含めて系統的に行う方法がある. 例えば Koblitz[7] p.28, 定理 1.4.3. を参照.
[35] これも例えば Koblitz[7] の p.28, 例 3 を見よ.

ある素数 p の法での原始根 a が 1 つ得られたとしよう. 定理 3.5.(b) によれば他の原始根を得るには乗法群 $\boldsymbol{Z}_p{}^*$ の位数 $p-1$ の素因数を持たない整数 j を[36]取って冪乗 a^j を作ればよい. 例えば $a=7$ はこの法 $p=2147483647$ での最小の原始根で, 上の様な j に対して 7^j を次々に作る事はこの場合の生成元すべてを掃過する手段である. これは Fishman と Moore[29] の重要な仕事で実際に行われた.

3.2. 乗算合同法: 法 2^r の場合

法が 2^r の場合の乱数乗算合同法,

$$x_k = ax_{k-1} \pmod{2^r} \quad k \geqq 1, \;\; r \geqq 4$$

も計算機上の実現の容易さからよく用いられ, 重要である. 素数の法の場合と異なり, 関係する数理は巡回群には帰着できない. それでもその周期や構造は群の圏内で最も明快に理解されるものだからこの段階で触れて進む. 但し群の言葉を使わない議論も可能で, 古くから行われ (入手しにくいが可能なら文献 [6] を是非参照せよ), 広い応用を持つ考え方を与えている. どちらも詳しい説明が我々の簡単に入手できる文献には見当たらないので, 以下本質的には文献 [2] の示唆を文献 [6] の方針に沿って実現する形で述べる.

法 $m=2^r$ だから整数は $0,1,\cdots,2^r-1$ に限って考える. 漸化式の一般解の表現 $x_k \equiv a^k x_0 \pmod{2^r}$ によれば, 偶数乗数

$$a = 2b, \quad b = 0,1,\cdots,2^{r-1}-1$$

は $a \neq 0$, しかし $s \geqq r$ に対して $a^s = 2^s b^s \equiv 0 \pmod{2^r}$ を与え, 乱数の生成式としては無意味なので除く. また偶数初期値 $x_0 = 2^s y_0$, y_0 は奇数, については, 系列

$$\{y_k := a^k y_0 \pmod{2^{r-s}} |\; k = 1,2,\cdots\}$$

を取ると $x_k = y_k \times 2^s$, つまり $y_k = a^k y_0$ を法 2^{r-s} で考えて結果を 2^s 倍する事と同じで下に見る様に周期は短くなる. 我々はこれも考察からは除く.

以下乗数と初期値の範囲を法 $m=2^r$ での奇数全体に限る. これは前節で見た法 $m=2^r$ での既約剰余群,

$$\boldsymbol{Z}_m^* = \{k|\,(k,2^r)=1\} = \{k|\,(k,2)=1\} = \{2k+1|\; k=0,1,\cdots,2^{r-1}-1\}$$

そのもので, その元の総数即ち「群 $\boldsymbol{Z}_{2^r}^*$ の位数」2^{r-1} は, オイラーの関数による計算

$$\phi(2^r) = 2^r(1-\frac{1}{2}) = 2^{r-1}$$

の示す通りである. しかしこの既約剰余群は巡回群でない; 文献 [21]pp.130–140 参照. これは群の数をさらに 8 で割った余りによって 4 つに分けると容易にわかる:

$$\boldsymbol{Z}_{2^r}^* = A_1^{(r)} \cup A_3^{(r)} \cup A_5^{(r)} \cup A_7^{(r)},$$

[36] メルセンヌ素数 $p=2^{31}-1$ についての問題 3.6 によれば, $p-1$ の素因数にメルセンヌ指数 31 そのものが入る. この事情は一般である. 任意の素数 $q \geqq 2$ と正の整数 n に対して既約剰余群 $\boldsymbol{Z}_{q^n-1}^*$ は常に位数 n の部分群を持つ; p.99, 定理 6.4.(d)(iv) 参照. このため $\boldsymbol{Z}_{q^n-1}^*$ の位数 $\phi(q^n-1)$ は必ず n で割り切れる. 特にメルセンヌ素数 $p=2^n-1$ は $\phi(p)=\phi(2^n-1)=p-1=2^n-2$ に必ず素因数としてメルセンヌ指数 (素数)n を含む.

$$A_k^{(r)} := \{8j+k|\ j=0,1,\cdots,2^{r-3}-1\},\quad \sharp A_k^{(r)} = 2^{r-3}.$$

もし $a, a' \in A_1^{(r)}$, 即ち「a, a' 共に 8 で割って余りが 1」なら,

$$a = 8j+1,\ \ a' = 8j'+1$$

と置いて $aa' = 8(8jj'+j+j')+1 \in A_1^{(r)}$ は直ちに見える. 一方 $k=3,5,7$ の場合は, 法 8 では

$$3^2 = 9 \equiv 8+1 \equiv 1,\quad 5^2 = 25 = 8\times 3+1 \equiv 1,\quad 7^2 = 49 = 8\times 6+1 \equiv 1 \pmod 8,$$

つまり $k=3,5,7$ の場合 $a \in A_k^{(r)}$ なら $a^{2i} \in A_1^{(r)}$, $a^{2i+1} \in A_k^{(r)}$ と限られてしまう. 従って群 $\boldsymbol{Z}_{2^r}^*$ の元 a の位数の上限として

$$a \in A_1^{(r)} \text{なら } \mathrm{ord}(a) \leqq \sharp A_1^{(r)} = 2^{r-3},$$
$$a \in A_k^{(r)}\ (k=3,5,7) \text{ なら } \mathrm{ord}(a) \leqq \sharp A_1^{(r)} + \sharp A_k^{(r)} = 2^{r-2},$$

が得られる. 次を示そう:

定理 3.7. $r \geqq 4$ とする. 既約剰余群 $\boldsymbol{Z}_{2^r}^*$ の元 a の位数について:
(a) $a \in A_3^{(r)}$ $(a \equiv 3 \pmod 8)$, 或いは $a \in A_5^{(r)}$ $(a \equiv 5 \pmod 8)$ なら $\mathrm{ord}(a) = 2^{r-2}$ である.
(b) $a \in A_7^{(r)}$, 又は $a \in A_1^{(r)}$ で $a \neq 1$ 即ち $a = 8j \pm 1$, $(j = 2^t k,\ k$ は正奇数, $t \leqq r-4)$ なら

$$\mathrm{ord}(a) = 2^{r-3-t}.$$

(証明) (a) 最初に次の事に注意する: 整数 $a > 0$ を $2^s, 2^{s+1}$ で割って

$$a = 2^s q + r = 2^{s+1} q' + r'$$

とすると $r =$「r'を 2^sで割った余り」$\leqq r'$ となる. 従って

$$\text{「整数 } a \text{ を } 2^{s+t}\ (t \geqq 1) \text{ で割った余り」} \geqq \text{「} a \text{ を } 2^s \text{で割った余り」}$$

である. また $A_3^{(r)},\ A_5^{(r)}$ のどちらの元であっても

$$A_3^{(r)} \text{の数なら } 8j+3 = (8j+4)-1 = 4(2j+1)-1 = 4k-1,$$
$$A_5^{(r)} \text{の数なら } 8j+5 = (8j+4)+1 = 4(2j+1)+1 = 4k+1,$$

と, 両方共「正の奇数 $k = 2j+1 \geqq 1$」で表せるから, まとめて,

$$\text{正の奇数 } k \text{ に対して} \boldsymbol{Z}_{2^r}^* \text{での } \mathrm{ord}(4k \pm 1) = 2^{r-2} \pmod{2^r}$$

となる事を示す. 証明の要点は以下の単純な計算の忍耐強い繰り返しである:

$$\begin{aligned}
a^1 &= 4k \pm 1 \equiv 3 \text{ 或は } 5 \pmod{8 = 2^3}\\
&\not\equiv 1 \pmod{2^s,\ 3 \leqq s \leqq r},\\
a^2 &= (4k \pm 1)^2 = 1 + 8k(\pm 1 + 2k) = 1 + 2^3 \times \text{正奇数 } k(2k \pm 1)\\
&\equiv 1 \pmod{2^s,\ 1 \leqq s \leqq 3 = 1+2},\\
&\not\equiv 1 \pmod{2^s,\ 1+3 = 4 \leqq s \leqq r},\\
(a^2)^2 &= a^{2\times 2} = a^{2^2} = 1 + 2^3 \times 2 \times \text{正奇数} = 1 + 2^4 \times \text{正奇数}\\
&\equiv 1 \pmod{2^s,\ 1 \leqq s \leqq 4 = 2+2},\\
&\not\equiv 1 \pmod{2^s,\ 2+3 = 5 \leqq s \leqq r},
\end{aligned}$$

$$
\begin{aligned}
\{(a^2)^2\}^2 = (a^4)^2 = a^{2^3} &= 1 + 2^5 \times \text{正奇数} \\
&\equiv 1 \,(\mathrm{mod} 2^s,\ 1 \leqq s \leqq 3+2), \\
&\not\equiv 1 \,(\mathrm{mod} 2^s,\ 3+3=6 \leqq s \leqq r), \\
&\quad \cdots\cdots\cdots\cdots\cdots\cdots \\
a^{2^{r-3}} &= 1 + 2^{r-1} \times \text{正奇数} \\
&\equiv 1 \,(\mathrm{mod} 2^s,\ 1 \leqq s \leqq (r-3)+2 = r-1), \\
&\not\equiv 1 \,(\mathrm{mod} 2^s,\ s \geqq (r-3)+3 = r), \\
a^{2^{r-2}} &= 1 + 2^r \times \text{正奇数} \\
&\equiv 1 \,(\mathrm{mod} 2^r).
\end{aligned}
$$

ここで $\boldsymbol{Z}_{2^r}^*$ の群構造の知識が役立つ. 群 $\boldsymbol{Z}_{2^r}^*$ の任意の元 a の位数 h は群の位数 2^{r-1} の約数だから (Lagrange の定理) 必ず 2 のべき乗 $h = 2^n$ の形に限り, n は $n \leqq r-1$ かつ法 2^r で $a^{2^n} \equiv 1$ が成り立つ最小の整数, 言い換えれば法 2^r で次が成り立つものである:

$$
\text{すべての } m < n \text{ について } a^{2^m} \not\equiv 1, \text{ かつ } a^{2^n} \equiv 1 \pmod{2^r}.
$$

上から $n = r-2,\ \mathrm{ord}(a) = 2^{r-2}$ と判明する.
(b) 仮定から $a = 8j \pm 1 = 2^{3+t}k \pm 1, 3 + t \leqq 3 + (r-4) = r-1, k$ は正奇数である. (a) と同様に,

$$
\begin{aligned}
a^2 &= 1 + 2^{4+t}k(\pm 1 + 2^{2+t}k) = 1 + 2^{4+t} \times \text{正奇数} \\
&\equiv 1 \,(\mathrm{mod}\ 2^s,\ 1 \leqq s \leqq 1 + (3+t) = 4+t), \\
&\not\equiv 1 \,(\mathrm{mod}\ 2^s,\ s \geqq 1 + (4+t) = 5+t), \\
a^{2^2} &= 1 + 2^{5+t} \times \text{正奇数} \\
&\equiv 1 \,(\mathrm{mod}\ 2^s,\ 1 \leqq s \leqq 2 + (3+t) = 5+t), \\
&\not\equiv 1 \,(\mathrm{mod}\ 2^s,\ s \geqq 2 + (4+t) = 6+t), \\
&\quad \cdots\cdots\cdots\cdots\cdots\cdots \\
a^{2^{r-3-t-1}} &= 1 + 2^{(r-3-t-1)+(3+t)} \times \text{正奇数} = 1 + 2^{r-1} \times \text{正奇数} \\
&\equiv 1 \,(\mathrm{mod}\ 2^s,\ 1 \leqq s \leqq (r-3-t-1) + (3+t) = r-1), \\
&\not\equiv 1 \,(\mathrm{mod}\ 2^s,\ (r-3-t-1) + (4+t) = r \leqq s), \\
a^{2^{r-3-t}} &= 1 + 2^{(r-3-t)+(3+t)} \times \text{正奇数} = 1 + 2^r \times \text{正奇数} \\
&\equiv 1 \,(\mathrm{mod}\ 2^r).
\end{aligned}
$$

故に周期は $2^{r-3-t},\ r-3-t \geqq r-3-(r-4) = 1$ である. ■

$A_3^{(r)}$ 或いは $A_5^{(r)}$ の乗数が両方共最長周期を与えると言っても, $a \in A_3^{(r)}$ は奇数乗が $8j+3$, 偶数乗が $8j+1$ の形で等間隔でないと嫌われ, 同じ点で $a \in A_5^{(r)}$ が $8j+5, 8j+1$ の等間隔を動くとして好まれる事もある [22]. 初期値の選択も含めて乱数の乗算合同法として纏めると:

定理 3.8. 法 2^r での乗算合同法系列 $x_k \equiv a x_{k-1} \,(\mathrm{mod}\ 2^r,\ r \geqq 4)$ について, その最長周期は $2^{r-2} = \dfrac{2^r}{4}$ で, これが実現される必要十分条件は初期値 x_0 が奇数である事と乗数 a が次の

条件を満たす事である:

$$a \equiv 3 \text{ 或いは } 5 \pmod 8.$$

乗数 a と初期値 x_0 の選択で実現される最長周期列 $\{x_k\}$ のすべてを mod 8 で見た値は次表の関係を満たす:

$a\backslash x_0$	1	3	5	7
3	1,3	3,1	5,7	7,5
5	1,5	3,7	5,1	7,3

(証明) 乗数 a, 初期値 x_0 の選択について, 偶数に興味がない事は既に述べた. 表の事項の証明は $x_k = a^k x_0$ の形から容易だから省略する. ■

既に述べ, (b)でも記した様に, 法 2^r での乗算合同法では系列の下位ビットほど周期が短くなる. 極端には法 2 ではすべて $\{1, 1, \cdots\}$, 法 8 では上の表の通り $\{3, 1, 3, 1, \cdots\}$, $\{5, 1, 5, 1, \cdots\}$ 等がすべてであり, 乱数としては用いる事はできない. しかし上位ビットだけが重要な問題に対してはこの事はあまり欠点とはならないだろう.

この方法では乗数の選択は素数の法での「原始根」よりさらに簡単で幾らでも選べる. しかし Park と Miller[24] が指摘する様に「選べる乗数が多すぎる」という面がある; 勝手な最長周期乗数を取る事はできても, どれでも同様なよい乱数系列が得られる訳ではない. 高性能な乗数に当たる確率は大変小さく, 選ぶ前の検定は欠かせない. 次章ではどの様に乱数系列の性能を評価し, それに基づいて最良乗数を選ぶべきか, という視点からこの事に触れる.

問題 3.9. コンピュータ上の乱数発生には漸化式 $x_k = ax_{k-1} \pmod m$, 即ち系列 $x_k = a^k x_0 \pmod m$, $k = 0, 1, 2, \cdots$, を法 $m = 2^{32} = 4294967296$, 或いは $m = 2^{31} = 2147483648$ として計算するものが実際によく用いられる. $1000 = 125 \times 8$ は 8 の倍数である事に注意して:
(a) 次の乗数の中から法 $m = 2^{32}$ で最長周期 $2^{32-2} = 2^{30} (= 1073741824)$ を与えるものを選びだせ.

$$a = 1,\ \ 3,\ \ 5,\ \ 36521,\ \ 449005,\ \ 365275.$$

(b) あるコンピュータ上では法 $m = 2^{31} (= 2147483648)$ で乗数 $a = 65539$ が用いられた. これも最長周期 $2^{31-2} = 2^{29} (= 536870912)$ を与える事を示せ.
(解) (a) 最長周期の条件は $a \equiv 3$ 又は $5 \pmod 8$ である. 1000 は 8 の倍数だから a の下 3 桁だけが問題である. 1,7 はだめ, 3,5 は良い.

$$\begin{aligned} 36521 &\equiv 521 = 65 \times 8 + 1 \equiv 1 \pmod 8, \\ 449005 &\equiv 5 \pmod 8, \\ 365275 &\equiv 275 = 34 \times 8 + 3 \equiv 3 \pmod 8. \end{aligned}$$

故に最長周期を与えるのは 3,5,449005,365275 である.
(b) $65539 \equiv 539 = 67 \times 8 + 3 \equiv 3 \pmod 8$. 故に最長周期 2^{29} が得られる. **(問題 3.9. 終り)**

上の問 (b) の乗数 a は以前に見た様に $a = 2^{16} + 3$ の関係を満たし, $a^2 - 6a + 9 \equiv 0 \pmod{2^{31}}$ が成り立つので, 系列 $x_k \equiv a^k x_0$ は漸化式

$$x_{k+2} - 6x_{k+1} + 9x_k \equiv 0 \pmod{2^{31}}$$

に従うのだった. これは乱数系列としては大変好ましくない; 最長周期の保証だけでは乱数系列の乗数として適当とは限らない.

4. スペクトル検定

4.1. 乗算合同法乱数列の格子構造

スペクトル検定は, 法が約 $2^{30}-2^{40}$ 程度の線形合同或いは乗算合同法の乗数の選択 (それは乱数ルーチンの選択そのものだが) のための, 経験的に最も信頼できる性能評価を与える. この検定内容の理解は, 線形合同法や乗算合同法の性能と限界, そして同時にこれらの乱数が関係する大変美しく魅力的な数学原理の 1 面, を構造的に把握する道でもある. スペクトル検定そのものにも勿論限界はあり, 利用では我々はそれを心得て掛からなければならない. これらの重要な展望を得るために, また次の章からの有限体や環の関係する考察の必要性を見積もるために, 以下最も記述の簡単な, 素数 p を法とする乗算合同法の場合 [23] を取上げて進もう.

素数の法 p に対する乗算合同法 $x_k = ax_{k-1} \pmod p$ で乗数 a を $\boldsymbol{Z}_p^*$ の原始根に選べば, 系列 $\{x_k|\, k=0,1,\cdots\}$ は $\boldsymbol{Z}_p^*$ のすべての数を 1 度ずつ巡り最長周期 $p-1$ が得られる事を我々は知った. この場合系列の一般項は $x_k = a^k x_0$ で, 出発値 $1 \leqq x_0 \equiv a^j \leqq p-1$ の選択は巡回する

$$a^1,\ a^2,\ \cdots,\ a^{p-1} \equiv 1,\ a^1,\ a^2,\ \cdots \pmod p$$

のどこから系列を始めるかを決めるだけだから, 得られる乱数系列は本質的に一意である. 乱数の使用目的からは容易な初期値の設定で最長周期が確実に得られる事が強く好ましいから, 法 p の乗算合同法乱数を設計する場合乗数 a の選択が原始根に限られる事は当然である. しかしそれだけでは十分ではない. 例えば法 $p = 2^{31}-1 = 2147483647$ での最小の原始根は $a=7$ だが, これを乗数とする事は系列周期が最長ではあっても乱数としては論外である. しかしそれなら, 異なる原始根の選択で乱数系列はどう変るのだろうか. 簡単な例で見よう.

法 11 の乗法群 $\boldsymbol{Z}_{11}^* = \{1,2,3,\cdots,10\}$ を考える. $\boldsymbol{Z}_{11}^*$ の元の総数 (位数) は $11-1=10$ で, その中に最大位数 10 の原始根は

$$\phi(10) = \phi(2\times 5) = 10\times(1-\frac{1}{2})(1-\frac{1}{5}) = 4$$

個存在する. 最も計算の簡単な 2 の冪乗を調べると

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 \equiv 5,\ 2^5 \equiv 10 \equiv -1 \pmod{11}$$

で $\mathrm{ord}(2) = 10$, 2 は法 11 での原始根である. だから 10 と素な (10 との最大公約数が 1 の, 或いは 10 と共通な素因数 2,5 を持たない) 数 1,3,7,9 によって作られる 2 の冪乗,

$$2^1 = 2,\ \ 2^3 = 8,\ \ 2^7 \equiv -4 \equiv 7 \equiv 2^{10-3} \equiv (2^3)^{-1},\ \ 2^9 \equiv -5 \equiv 6 \equiv 2^{10-1} \equiv (2^1)^{-1},$$

の 4 個が原始根のすべてだとわかる. ここで $2^k \times 2^{10-k} = 2^{10} \equiv 1$ を用いた. 法 11 での「乗

算合同法乱数系列」にはこうして, 乗数を a として

$$a = 2 \text{ の系列 } x_k = 2^k x_0 \text{とその逆行系列 } x_k = (2^{-1})^k x_0 = 6^k x_0,$$

$$a = 7 \text{ の系列 } x_k = 7^k x_0 \text{とその逆行系列 } x_k = (7^{-1})^k x_0 = 8^k x_0,$$

の本質的に 2 種類の系列の選択がある. これらの系列について, xy 平面に点 $P_k = (x_k, x_{k+1})$ を $k = 0, 1, \cdots, 10$ についてプロットした図, 最初にこの図の著名な利用を行った Marsaglia[25] に因んで (2 次元) マルサリア図 Marsaglia plot と呼ぼう, を作ろう.

問題 4.1. 法 11 の乗法群 $\boldsymbol{Z}_{11}^* = \{1, 2, 3, \cdots, 10\}$ の原始根 $a = 2, 7$ について:
(a) $a = 2$ の冪乗系列の 2 次元 Marsaglia 図を作れ.
(b) $a = 7$ の冪乗系列でも 2 次元 Marsaglia 図を作れ.
(解) (a) 冪乗をすべて計算すれば

$$2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 \equiv 5,\ 2^5 \equiv 10,$$

$$2^6 \equiv 9,\ 2^7 \equiv 7,\ 2^8 \equiv 3,\ 2^9 \equiv 6,\ 2^{10} \equiv 1 \pmod{11}.$$

だから点 $(1, 2)$, $(2, 4)$, $(4, 8)$, $(8, 5)$, $(5, 10)$, $(10, 9)$, $(9, 7)$, $(7, 3)$, $(3, 6)$, $(6, 1)$, を描けばよい.
(b) 同様に

$$7^0 = 1,\ 7^1 = 7,\ 7^2 \equiv 5,\ 7^3 \equiv 2,\ 7^4 \equiv 3,\ 7^5 \equiv 10,$$

$$7^6 \equiv 4,\ 7^7 \equiv 6,\ 7^8 \equiv 9,\ 7^9 \equiv 8,\ 7^{10} \equiv 1 \pmod{11}$$

となるから点 $(1, 7)$, $(7, 5)$, $(5, 2)$, $(2, 3)$, $(3, 10)$, $(10, 4)$, $(4, 6)$, $(6, 9)$, $(9, 8)$, $(8, 1)$ を●で描け

(a) 乗数 $a = 2$ の 2 次元 Marsaglia 図　　(b) 乗数 $a = 7$ の 2 次元 Marsaglia 図

ばよい. その結果は (a) と共に上の図に示す通りである. **(問題 4.1. 終り)**

上のどちらの結果でも注目すべき事の第 1 は, 点がきちんとした 2 次元格子を作っている事である. 現実的ではないが, 仮に法 11 で乱数系列を $x_k \equiv a^k x_0 \pmod{11}$ で $k = 0, 1, \cdots$ と作るとすれば, 乗数 $a = 2$ と $a = 7$ とは $\boldsymbol{Z}_{11}^*$ の数 1 から 10 までを 1 度ずつ作り, 最長周期 10 を実現する基本性能では同等で甲乙付け難い. しかしこれらの図はさらに x_k と x_{k+1} の擬似的な独立性の比較を可能にする. x_k と x_{k+1} の出方が独立 (関係ない) なら, 点 (x_k, x_{k+1}) で x_{k+1} は x_k に関係なく左右も遠近も同様に出るはずだから, その結果は「全体として」平面内にほぼ濃淡なく均等に分布する事が好ましいだろう. 現実には $a = 2$ の系列は 2 本の直線に強く密集しそのかわりそれらの線の間隔は疎で, 明らかに $a = 7$ の点の方が平面内での 2 次元分布として均等で高性能と見える. 「見える」だけでは客観的論理的ではない. スペ

クトル検定はこの性能評価を数量化体系化し, 視覚判断によらず計算機上で最良の乗数を選択する事を可能にする方法である.

一般に系列の相続く l 個を l 連 (l-string, l-tuple) と名付けよう. l 連は

$$P_k = (x_k, x_{k+1}, \cdots, x_{k+l-1}) \equiv x_k(1, a, a^2, \cdots, a^{l-1}) \pmod p, \quad 0 \leqq k \leqq p-2$$

の形である. これを l 次元ユークリッド空間 E_l の点の座標と考えると, 各 x_k を法 p で考えるのだから, 点 P_k は実際には体積が p^l である立方体

$$C_l := \{(x_0, x_1, \cdots, x_{l-1}) |\ 0 \leqq x_k < p\}$$

(これを「周期胞 periodic cell」とでも呼ぼう) の中へ各座標の法 p での値を取って引き戻さなければならない. この周期胞内の点のプロットが l 次元 Marsaglia 図である. 法が素数 p の乗算合同法では $1 \leqq x_k \leqq p-1$ で, $x_k \equiv 0$ となる座標は決して現れず, 特に 0 の l 連 $(0, 0, \cdots, 0)$ は現れない. そこで以下この Marsaglia 図とそれに関係した整数座標の点の集合 G_l を次の様に取る:

(i) l 次元ユークリッド空間 E_l 中で系列 $\{x_k\}$ の l 連の表す点全体に 1 点 $(0, 0, \cdots, 0)$
$=0 \times (1, a, a^2, \cdots, a^{l-1})$ を付け加えた点集合を考え,
(ii) それらの点のすべてを p を周期として E_l 全体へ拡張した像 (格子, 独 Gitter)
を G_l と定義する.

上の図 (a),(b) には (i) で付け加えた原点に●を記入しなければならない. G_2 はさらにその図の点のすべてを (ii) によって全軸方向 (この 2 次元の場合 x, y 方向) へ法 $p(=11)$ で次々拡張したものと同じだから, これら $l = 2$ の図の表示範囲ではそれは残る 3 つの隅にも●が付け加えられたものとして見える事になるが, 周期胞 C_2 は $0 \leqq x, y < p$ の範囲だから, その中には全体で p 個の点が配置される. この周期胞内の G_l の点の総数 p は次元 l を変えても変らない; 異なる l 連の総数は $(x_k, x_{k+1}, \cdots, x_{k+l-1})$ の $k = 1, 2, \cdots, p-1$ に対する $p-1$ 個と加えられた $(0, 0, \cdots, 0)$ の p 個しかない.

まず (i) で原点を付け加え, それらを (ii) で l 個の座標方向にそれぞれ周期 p で平行移動した (法 p で合同な座標を持つ) 点を合せた点の集合 G_l が「格子」となる事を Dieter[26] に従って一般に示そう. 念のため, l 次元空間の格子を定義しておく:

定義 4.2. l 次元ユークリッド空間 E_l の l 個の 1 次独立なベクトルの組 $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$[37] が与えられた時, これらの整数係数 1 次結合を位置ベクトルとする点の全体

$$L = L(\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l) := \{c_1\boldsymbol{e}_1 + c_2\boldsymbol{e}_2 + \cdots + c_l\boldsymbol{e}_l |\ c_j \text{は整数}\, 0, \pm1, \pm2, \cdots,\ 1 \leqq j \leqq l\}$$

を $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ を基 base ベクトルとする格子と言う. **(定義 4.2. 終り)**

Corollary 4.3. 素数 p の法での原始根 a 及び正の整数 l を任意に取ると, G_l は l 次元ユークリッド空間 E_l 中の格子を作り, 基ベクトルの 1 組は次で与えられる:

$$\boldsymbol{e}_1 := {}^t(1, a, a^2, \cdots, a^{l-1}), \ \ \boldsymbol{e}_2 := {}^t(0, p, 0, \cdots, 0), \ \ \cdots, \ \ \boldsymbol{e}_l := {}^t(0, 0, 0, \cdots, p).$$

---

[37] 行列計算での便宜から太文字 $\boldsymbol{e}$ は列ベクトル, ${}^t\boldsymbol{e}$ はその転置行ベクトルと約束する. $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ が E_l で 1 次独立とは, l 個の実数 $\{\alpha_1, \alpha_2, \cdots, \alpha_l\}$ によるこれらのベクトルの 1 次結合 $\alpha_1\boldsymbol{e}_1 + \alpha_2\boldsymbol{e}_2 + \cdots + \alpha_l\boldsymbol{e}_l$ が零ベクトル $\boldsymbol{0}$ になるのが $\alpha_1 = \alpha_2 = \cdots = \alpha_l = 0$ 以外にはない事を言う. よく知られる様にこれは l 個の l 次元ベクトル $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ を列ベクトルとする $l \times l$ 行列の行列式が 0 ではない事と同じである.

(証明) 始めに最長周期乗算合同法乱数 x_k の 1 周期に 0 を加えると, 順番は (望むらくは) でたらめに見えるが, 実現される法 p での値は全体として必ず $0,1,2,\cdots,p-1$ を 1 度ずつすべて巡回している事, そして命題で定義された $\{\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_l\}$ が実数係数で考えて明らかに空間の次元 l と同数の 1 次独立ベクトルである事に注意する. さて, ベクトル $\boldsymbol{e}_1$ の定義から

$$x_k\boldsymbol{e}_1 = x_k\,{}^t(1,a,a^2,\cdots,a^{l-1}) \equiv {}^t(x_k,x_{k+1},x_{k+2},\cdots,x_{k+l-1}) \pmod p$$

であって, x_k から始まる l 連は $x_k\boldsymbol{e}_1$ と表される. 点集合 G_l の任意の点はある k に対するこの $x_k\boldsymbol{e}_1$ を l 次元空間の各軸毎に p の整数倍の移動を行って得られる. 具体的には第 1 座標方向の p 移動 (周期移動) を表すベクトルは

$$\boldsymbol{e}'_1 := {}^t(p,0,\cdots,0) = p\boldsymbol{e}_1 - a\boldsymbol{e}_2 - a^2\boldsymbol{e}_3 - \cdots - a^{l-1}\boldsymbol{e}_l,$$

第 2 から第 l 座標軸について $\boldsymbol{e}_2 = {}^t(0,p,0,\cdots,0)$, $\cdots$, $\boldsymbol{e}_l = {}^t(0,0,0,\cdots,p)$ は明らかに p 移動だから, この G_l の任意の点の位置ベクトル $\boldsymbol{u}$ はある整数の組 $\{x_k,j_1,j_2,\cdots,j_l\}$ によって

$$\begin{aligned}\boldsymbol{u} &= x_k\boldsymbol{e}_1 + j_1\boldsymbol{e}'_1 + j_2\boldsymbol{e}_2 + \cdots + j_l\boldsymbol{e}_l\\ &= (x_k+j_1p)\boldsymbol{e}_1 + (j_2-j_1a)\boldsymbol{e}_2 + \cdots + (j_l-j_1a^{l-1})\boldsymbol{e}_l\\ &= j'_1\boldsymbol{e}_1 + j'_2\boldsymbol{e}_2 + \cdots + j'_l\boldsymbol{e}_l\end{aligned}$$

と表される. $j'_1 = x_k + j_1p$, $j'_2 = j_2 - j_1a$, $\cdots$, $j'_l = j_l - j_1a^{l-1}$ はすべて整数で, G_l の任意の点の位置を表すこのベクトルは格子 $L(\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_l)$ に属す; これで $G_l \subset L$ が示された.

逆に格子 $L(\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_l)$ の任意の点を考えよう. 定義 4.2 からこれはある整数の組 $j_1,j_2,\cdots,j_l$ による一次結合 $j_1\boldsymbol{e}_1 + j_2\boldsymbol{e}_2 + \cdots + j_l\boldsymbol{e}_l$ を位置ベクトルに持つ. j_1 を p で「整数として」割り算を行った商を q, 余りを r, 即ち $j_1 = pq + r \equiv r \pmod p$, $0 \leqq r < p$, とすれば,

$$\begin{aligned}j_1\boldsymbol{e}_1 + j_2\boldsymbol{e}_2 + \cdots + j_l\boldsymbol{e}_l &= (pq+r)\,{}^t(1,a,a^2,\cdots,a^{l-1}) + j_2\,{}^t(0,p,0,0,\cdots,0)\\ &\quad + j_3\,{}^t(0,0,p,0,\cdots,0) + \cdots + j_l\,{}^t(0,0,\cdots,0,p)\\ &= r\,{}^t(1,a,a^2,\cdots,a^{l-1}) + j'_1\,{}^t(p,0,0,0,\cdots,0) + j'_2\,{}^t(0,p,0,0,\cdots,0)\\ &\quad + j'_3\,{}^t(0,0,p,0,\cdots,0) + \cdots + j'_l\,{}^t(0,0,\cdots,0,p),\\ &\quad j'_1 = q,\quad j'_i = j_i + a^{i-1}q,\quad 2 \leqq i \leqq l,\end{aligned}$$

が成り立つ. これは l 連 $x_k\boldsymbol{e}_1 = {}^t(x_k,x_{k+1},\cdots,x_{k+l-1})$ の $x_k \equiv r$ の場合, a は法 p での原始根だからその様な場合は乱数に値 0 も含めたものには必ずある, に相当する点を各座標軸方向に周期 p の整数倍移動したもので勿論 G_l の点である. 故に格子 $L(\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_l)$ の任意点は G_l に含まれ $L(\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_l) \subset G_l$ も成り立つ事がわかり, G_l と格子 $L(\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_l)$ は同一の位置ベクトルの集合, 点の集合である. ■

4.2. スペクトル検定

l 次元格子を作ると言っても, 既述の通り周期胞に実際に配置される乗算合同法 1 周期分の点の総数は $p-1$ で一定, l 次元空間の整数格子点全体の中での占拠密度 $\dfrac{p-1}{p^l} \approx \dfrac{1}{p^{l-1}}$ は

次元 l と共に急激に小さくなる. それはしかたがないとして, 問題はその薄い点密度の前の図の様なばらつきの評価である. スペクトル検定は, 乗数 a 毎に E_l 中の平行な (超) 平面群で G_l の全格子点を含むものをすべて考え, 平面群の間隔を計算し, 平面群すべてについてのこの間隔の最大値の逆数をその乗数の性能の指標とする. つまり平面群の間隔の最大値が小さい乗数に高い評価を与える. この方法では上の法 11 の例で言えば, 明らかに乗数 $a = 7$ が $a = 2$ に勝る妥当な結論が導かれる.

E_l の中で法線ベクトル $\boldsymbol{v} = {}^t(v_1, v_2, \cdots, v_l)$ を持つ平面の点 $\boldsymbol{x} = {}^t(x_1, x_2, \cdots, x_l)$ は 1 次方程式

$$\boldsymbol{x} \cdot \boldsymbol{v} = x_1 v_1 + x_2 v_2 + \cdots + x_l v_l = s$$

に従う. 同一の法線ベクトル $\boldsymbol{v}$ を持つ平行な 2 平面

$$\boldsymbol{x} \cdot \boldsymbol{v} = x_1 v_1 + x_2 v_2 + \cdots + x_l v_l = s,$$

$$\boldsymbol{x'} \cdot \boldsymbol{v} = x'_1 v_1 + x'_2 v_2 + \cdots + x'_l v_l = t$$

の間隔 d は, ベクトル $\boldsymbol{v}$ のユークリッド長さ $|\boldsymbol{v}| := \sqrt{v_1^2 + v_2^2 + \cdots + v_l^2}$ と単位ベクトル $\boldsymbol{e} := \dfrac{\boldsymbol{v}}{|\boldsymbol{v}|}$ とを導入すると, 右上の図のように

$$d = |(\boldsymbol{x} - \boldsymbol{x'}) \cdot \boldsymbol{e}| = \frac{|\boldsymbol{x} \cdot \boldsymbol{v} - \boldsymbol{x'} \cdot \boldsymbol{v}|}{|\boldsymbol{v}|} = \frac{|s - t|}{|\boldsymbol{v}|}$$

で与えられる.[38] われわれの問題は次である: 乗数 a できまる乱数の l 連の作る l 次元格子 G_l に対して, 法線ベクトル $\boldsymbol{v}$ を持つ平面群で G_l の格子点を含むものの最大間隔はどのような $\boldsymbol{v}$ に対するものか. そしてその $\boldsymbol{v}$ と最大間隔とはどのように発見, 算出されるか?

Dieter[26] に沿って見る. 問題解決の鍵は E_l の基ベクトルを格子 G_l の基ベクトル $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$, 再記すれば

$$\boldsymbol{e}_1 := {}^t(1, a, a^2, \cdots, a^{l-1}), \quad \boldsymbol{e}_2 := {}^t(0, p, 0, \cdots, 0), \quad \cdots, \quad \boldsymbol{e}_l := {}^t(0, 0, 0, \cdots, p),$$

で表し, 法線ベクトル $\boldsymbol{v}$ については G_l のこの基底に対応する別の基ベクトルの組[39]:

$$\boldsymbol{e}_1^* := {}^t(p, 0, \cdots, 0), \quad \boldsymbol{e}_2^* := {}^t(-a, 1, 0, \cdots, 0), \quad \boldsymbol{e}_3^* := {}^t(-a^2, 0, 1, \cdots, 0),$$

$$\cdots, \quad \boldsymbol{e}_l^* := {}^t(-a^{l-1}, 0, 0, \cdots, 1); \quad \boldsymbol{e}_i \cdot \boldsymbol{e}_j^* = p\delta_{ij},$$

を導入して $\boldsymbol{v}$ を表すと同時に $\{\boldsymbol{e}_j^*\}$ が生成する (逆) 格子 G_l^* を考える所にある. もとの格子 G_l の任意のベクトル $\boldsymbol{u}$, (逆) 格子 G_l^* の任意の法線ベクトル $\boldsymbol{v}$ のそれぞれについて, デカル

[38] 点 $\boldsymbol{x'}$ から平面 $\boldsymbol{x} \cdot \boldsymbol{v} = s$ への距離が $\dfrac{|x'_1 v_1 + x'_2 v_2 + \cdots + x'_l v_l - s|}{\sqrt{{v_1}^2 + {v_2}^2 + \cdots + {v_l}^2}} = \dfrac{|\boldsymbol{x'} \cdot \boldsymbol{v} - s|}{|\boldsymbol{v}|}$ である事を既知とすればこの距離 d はさらに簡単に見通される.

[39] これはフーリエ解析の場合の波数ベクトルの基底に相当する. これらが作る格子は G_l^* と書かれ, 物性物理では「(結晶の) 逆格子」, 数学では双対 (そうつい) 格子, と呼ばれる. G_l の基ベクトルを列ベクトルとして作られる $l \times l$ 行列を A とすれば, 逆行列 A^{-1} を用いて以下に与えられる逆格子の基ベクトルは pA^{-1} の行ベクトルの転置である, と簡単に言える. * に転置の意味を含ませる事もあるが, ここではそうまではしない.

ト座標成分での表示と基底 $\{\boldsymbol{e}_i\}, \{\boldsymbol{e}_j^*\}$ での表現とを区別して次の様に記そう:

$$\boldsymbol{u} := {}^t(u_1, u_2, \cdots, u_l) = u_1'\boldsymbol{e}_1 + u_2'\boldsymbol{e}_2 + \cdots + u_l'\boldsymbol{e}_l,$$

$$\boldsymbol{v} := {}^t(v_1, v_2, \cdots, v_l) = v_1'\boldsymbol{e}_1^* + v_2'\boldsymbol{e}_2^* + \cdots + v_l'\boldsymbol{e}_l^*.$$

$\boldsymbol{e}_i$ と $\boldsymbol{e}_j^*$ の直交性 $\boldsymbol{e}_i \cdot \boldsymbol{e}_j^* = p\delta_{ij}$ から, これらのベクトルの内積は次の 2 通りに表される:

$$\boldsymbol{u} \cdot \boldsymbol{v} = u_1v_1 + u_2v_2 + \cdots + u_lv_l = p(u_1'v_1' + u_2'v_2' + \cdots + u_l'v_l').$$

眼目の「格子 G_l の点を含む平面群に最大間隔を与える法線ベクトル $\boldsymbol{v}$」の探索に向かおう. 逆格子の双対基底 $\{\boldsymbol{e}_1^*, \boldsymbol{e}_2^*, \cdots, \boldsymbol{e}_l^*\}$ は上に与えられた形からも明らかに 1 次独立だから, 任意の法線ベクトルは $\boldsymbol{v} = v_1'\boldsymbol{e}_1^* + v_2'\boldsymbol{e}_2^* + \cdots + v_l'\boldsymbol{e}_l^*$ と表せる. 直交デカルト成分であろうと双対基に関する双対座標 $\{v_1', v_2', \cdots, v_l'\}$ であろうと, $\boldsymbol{v}$ の方向は成分の比だけで決まるから問題はこれらの比である.

まず双対座標 $\{v_1', v_2', \cdots, v_l'\}$ が無理数比を持つものは考えなくてよい事を示す. 例えば $v_2' = \alpha v_1'$, α は無理数の場合, 格子 G_l の位置ベクトル $\boldsymbol{u} = u_1'\boldsymbol{e}_1 + u_2'\boldsymbol{e}_2$, u_1', u_2' は整数, を考えると $\boldsymbol{u} \cdot \boldsymbol{v} = pv_1'(u_1' + \alpha u_2')$ となるが, 任意の正の整数 N に対して必ず $|u_1' + \alpha u_2'| < \dfrac{1}{N}$ となる整数 u_1', u_2' がある.[40] 故に無理数比の双対座標を持つ法線ベクトル $\boldsymbol{v}$ では超平面の方程式 $\boldsymbol{u} \cdot \boldsymbol{v} = s$ で格子 G_l の点 $\boldsymbol{u}$ がその上にあるように与えるべき s の値にもその間隔 (従って元の格子の空間での平面間隔) にも最小の正の値がなく, そのような $\boldsymbol{v}$ はこれを法線ベクトルに持つ「平面の間隔の最大値」を求める問題では考える必要がない. 一方有理数比の双対座標を持つ $\boldsymbol{v}$ は, 全座標を比の分母の (最小) 公倍数倍し必要なら共通の無理数因子で割って, 向きを変えずに整数成分に直せる. だから平面群の法線ベクトル $\boldsymbol{v}$ としては $\boldsymbol{v} = v_1'\boldsymbol{e}_1^* + v_2'\boldsymbol{e}_2^* + \cdots + v_l'\boldsymbol{e}_l^*$ で $v_1', v_2', \cdots, v_l'$ がすべて整数のもの, 即ち逆格子ベクトル $\boldsymbol{v} \in G_l^*$ だけで考えればよい.

$\boldsymbol{u}$ を格子 G_l の任意ベクトル, $\boldsymbol{v}$ を逆格子 G_l^* のあるベクトルとすると,

$$\boldsymbol{u} \cdot \boldsymbol{v} = p(u_1'v_1' + u_2'v_2' + \cdots + u_l'v_l')$$

で座標 $\{u_1', u_2', \cdots, u_l'\}$ はすべての整数値の組を動き, $\{v_1', v_2', \cdots, v_l'\}$ はある固定された整数値の組である. 上の式の右辺が p の倍数である事は明らかだが, もっと精密に次の重要な関係が成り立つ:

定理 4.4. 整数の組 $v_1', v_2', \cdots, v_l'$ の最大公約数を $z = \mathrm{GCD}(v_1', v_2', \cdots, v_l')$ と記す $(z \geqq 1)$. $\{u_1', u_2', \cdots, u_l'\}$ がすべての整数値を動く時,

---

[40] 無理数 α の有理数 $-\dfrac{u_1'}{u_2'}$ による近似を考えればこの事は直感的に明らかだが次のような証明もある. $\alpha, 2\alpha, \cdots$ は皆無理数で, それぞれ適当な整数を差し引いて $\alpha - m$, $2\alpha - n$, $\cdots$ がすべて区間 $(0, 1)$ に入るようにできる. 我々の親しんだ用語では「$\alpha, 2\alpha, \cdots$ を法 1 で考える」と言ってもよい. これらは互いに法 1 で合同 (差が整数) になる事もなく, また区間 $[0, 1]$ を N 等分した $\dfrac{1}{N}$ の幅の N 個の小区間, $\{[\dfrac{j}{N}, \dfrac{j+1}{N}], 0 \leqq j \leqq N-1\}$, のどの境界 (有理数点である) とも一致しない無限個の点となる. だから少なくともどれか 1 つの小区間には必ず 2 つ以上の点が入り (「Dirichlet の引出し / 部屋割り論法」と言われる),

$$|(j\alpha - m) - (k\alpha - n)| = |(-m + n) + (j - k)\alpha| = |u_1' + u_2'\alpha| < \frac{1}{N}$$

となる整数 $u_1' := n - m$, $u_2' := j - k$ がある. ■

$$f(u'_1, u'_2, \cdots, u'_l) := u'_1v'_1 + u'_2v'_2 + \cdots + u'_lv'_l$$

は $z = \mathrm{GCD}(v'_1, v'_2, \cdots, v'_l)$ の倍数全体を動き, それ以外の値は取らない.
(証明) f の取る値の全体の集合を S と置く. S の任意の要素 a, ある整数の組 $u'_1, u'_2, \cdots, u'_l$ に対する $a = f(u'_1, u'_2, \cdots, u'_l)$, の値は自明に整数である. a は $v'_1, v'_2, \cdots, v'_l$ の整数係数 1 次結合だから $v'_1, v'_2, \cdots, v'_l$ の公約数の任意の 1 つ (特にそれらの最大公約数 $z = \mathrm{GCD}(v'_1, v'_2, \cdots, v'_l)$) によって割り切られ, 0 ではない $a \in S$ の絶対値は z より大きいか等しい. また任意の整数 s, t と別の任意の整数の組 $u''_1, u''_2, \cdots, u''_l$ に対しては

$$sf(u'_1, u'_2, \cdots, u'_l) \pm tf(u''_1, u''_2, \cdots, u''_l) = f(su'_1 \pm tu''_1, su'_2 \pm tu''_2, \cdots, su'_l \pm tu''_l) \text{ (複号同順)}$$

も成り立つ. だから $a, b \in S$ なら $sa \pm tb \in S$ である. 特に $t = 0$ として S の任意の数 a の任意の整数 s 倍も S に属している. S の正の最小値を h と置こう. 上の事から必ず $h \geqq z = \mathrm{GCD}(v'_1, v'_2, \cdots, v'_l)$ である. $h \in S$ なのだから

$$h = f(u''_1, u''_2, \cdots, u''_l)$$

と与える整数の組 $\{u''_1, u''_2, \cdots, u''_l\}$ が存在する. 今 S の任意の数

$$a := f(u'_1, u'_2, \cdots, u'_l)$$

を h で割って $a = hq + r, 0 \leqq r < h$ と置くと,

$$0 \leqq r = a - qh = f(u'_1, u'_2, \cdots, u'_l) - qf(u''_1, u''_2, \cdots, u''_l)$$
$$= f(u'_1 - qu''_1, u'_2 - qu''_2, \cdots, u'_l - qu''_l) \in S$$

が成り立つ. 故に $r \geqq 0$ も S の元で h より小さく, h が S の中で正で最小なのだから $r = 0$ で a は h で割り切れる. こうして S の数は h の倍数だけから成り立つ事がわかり, h のすべての倍数は S に属すから, S は h の倍数の全体と一致する. しかも上で見た様に, $v'_1, v'_2, \cdots, v'_l$ の整数係数 1 次結合として S のすべての数は $v'_1, v'_2, \cdots, v'_l$ の最大公約数 $z = \mathrm{GCD}(v'_1, v'_2, \cdots, v'_l)$ で割り切れ, 特に h は z で割り切れて $h \geq z$ である. 逆に例えば $f(1, 0, \cdots, 0) = v'_1 \in S$ だから $\pm v'_1$ は h で割り切れ, 同様に $v'_2, \cdots, v'_l$ もすべて h で割り切れる; h は $v'_1, v'_2, \cdots, v'_l$ の公約数である. 当然 h は最大公約数 z の約数で $h \leqq z$ が上の $h \geqq z$ とあわせて成り立つ. これは $h = z$ である事, そして S は $v'_1, v'_2, \cdots, v'_l$ の最大公約数の倍数全体と一致する事, を証明する. ■

こうして法線ベクトル $\boldsymbol{v}$ を止め, $\boldsymbol{u}$ が格子 G_l のすべての点を動く時の $\boldsymbol{u} \cdot \boldsymbol{v} = p(u'_1v'_1 + u'_2v'_2 + \cdots + u'_lv'_l)$ の取る値の集合は「$\{v'_j\}$ の最大公約数 $z = \mathrm{GCD}(v'_1, v'_2, \cdots, v'_l)$」を用いて

$$\{kzp |\ k = 0, \pm 1, \pm 2, \cdots\}$$

と表されるとわかった. 法線ベクトルは方向だけが問題だから, 整数の双対座標 $\{v'_j\}$ を公約数で割り, $\{v'_j\}$ の最大公約数 $\mathrm{GCD}(\{v'_j\}) = 1$ であるものだけを考えて十分である. 即ち

$$\boldsymbol{v} = v'_1\boldsymbol{e}^*_1 + v'_2\boldsymbol{e}^*_2 + \cdots + v'_l\boldsymbol{e}^*_l \in G^*_l, \quad \mathrm{GCD}(v'_1, v'_2, \cdots, v'_l) = 1,$$

の形の逆格子ベクトルだけで考えてよい. この様な $\boldsymbol{v}$ を G^*_l の既約なベクトルと呼び, その全体を暫くの間 $G^\sharp_l$ と記す事にしよう. 上の結果も含めた展望は次である:

Lemma 4.5. (a) 任意の $\boldsymbol{v} \in G_l^\sharp$ に対して, G_l の任意ベクトル $\boldsymbol{u}$ の与える内積

$$\boldsymbol{u} \cdot \boldsymbol{v} = p(u'_1 v'_1 + u'_2 v'_2 + \cdots + u'_l v'_l)$$

の値は p の整数倍であり, その全体を巡る.
(b) l 次元ユークリッド空間 E_l の中で任意の $\boldsymbol{v} \in G_l^\sharp$ を共通法線ベクトルとする間隔 $d := \dfrac{p}{|\boldsymbol{v}|}$ の平行平面群

$$\boldsymbol{u} \cdot \boldsymbol{v} = p(u'_1 v'_1 + \cdots + u'_l v'_l) = 0, \pm p, \pm 2p, \cdots$$

は, 右辺のどの値に対しても格子 G_l の点 $\boldsymbol{u}$ を必ず含み, 且つこれら平行平面群の上に格子 G_l のすべての点 $\boldsymbol{u}$ は含まれる.
(証明) (a) は定理 4.4. で見られた事に $\mathrm{GCD}(v'_1, v'_2, \cdots, v'_l) = 1$ を入れて得られる事, (b) はその言い換えと上の式の表す平行平面群間隔についての言及の追加である. ■

スペクトル検定は, 与えられた乗数 a について, それで決まる l 次元逆格子 G_l^* を取り, すべての既約な逆格子ベクトル $\boldsymbol{v} \in G_l^\sharp$ を法線ベクトルとする平行平面群の間隔 $\dfrac{p}{|\boldsymbol{v}|}$ の最大値を求めて乗数 a の評価とするものだとわかった. そのためには既約な逆格子 $G_l^\sharp$ の 0 ベクトルではない $\boldsymbol{v}$ の全体についてそのユークリッド長さ $|\boldsymbol{v}|$ の最小値を求めればよい. 逆格子 G_l^* の任意ベクトル $\boldsymbol{v}$ は必ずある既約な逆格子ベクトルの整数倍であり, 従って長さも整数倍だから, 最小長さのベクトルの探索を行う上では $\boldsymbol{v}$ を既約な逆格子に限る必要はない; 双対座標が最大公約数 1 になっているかどうかに煩わされる事なく, 逆格子 G_l^* の全ベクトルから探索すればよいのである!

これを行う事に考えを進めよう. 逆格子ベクトル $\boldsymbol{v} \in G_l^*$ の長さ $|\boldsymbol{v}|$ の計算ではデカルト座標ベクトル $\boldsymbol{v} = {}^t(v_1, v_2, \cdots, v_l)$ が活躍する. 整数デカルト座標の $\boldsymbol{v}$ がすべて G_l^* の逆格子ベクトルを与える訳ではないが判定条件は簡明である:

Corollary 4.6. デカルト座標ベクトル $\boldsymbol{v} = {}^t(v_1, v_2, \cdots, v_l)$ が逆格子 G_l^* の元であるためには, $v_1, v_2, \cdots, v_l$ が整数で次が成立つ事が必要十分である:

$$v_1 + v_2 a + v_3 a^2 + \cdots + v_l a^{l-1} \equiv 0 \pmod{p}.$$

(証明) 「$\boldsymbol{v}$ が逆格子ベクトルである, $\boldsymbol{v} \in G_l^*$」事は整数の $v'_1, v'_2, \cdots, v'_l$ 対して

$$\boldsymbol{v} = v'_1 \boldsymbol{e}_1^* + v'_2 \boldsymbol{e}_2^* + \cdots + v'_l \boldsymbol{e}_l^*$$

が成り立つ事と同値だから, $\boldsymbol{e}_1^*$,$\boldsymbol{e}_2^*$,$\cdots$,$\boldsymbol{e}_l^*$ の形 (p.53) を入れると, デカルト座標として

$$v_1 = pv'_1 - v'_2 a - v'_3 a^2 - \cdots - v'_l a^{l-1}; \;\; v_j = v'_j \; (2 \leqq j \leqq l)$$

が成り立ち, すべて整数である. これから直ちに

$$v_1 + v_2 a + v_3 a^2 + \cdots + v_l a^{l-1} = pv'_1 \equiv 0 \pmod{p},$$

即ち命題中の式が得られる; 故にこの式は整数デカルト座標 $v_1, v_2, \cdots, v_l$ のベクトルが逆格子ベクトルである必要条件である. 逆にこの式が 右辺 $= pq$, q も整数, で成立する整数デカルト座標のベクトル $\boldsymbol{v} = {}^t(v_1, v_2, \cdots, v_l)$ については

$$\boldsymbol{v} = {}^t(pq - v_2a - v_3a^2 - \cdots - v_la^{l-1}, v_2, \cdots, v_l)$$

$$= q\boldsymbol{e}_1^* + v_2\boldsymbol{e}_2^* + \cdots + v_l\boldsymbol{e}_l^* \in G_l^*$$

である. だからこの式は整数デカルト座標 $v_1, v_2, \cdots, v_l$ を持つベクトル $\boldsymbol{v}$ が逆格子ベクトルである十分条件でもある. ■

再記になるが, これらの結果を次の定理にまとめよう:

定理 4.7. (a) 素数 p の乗法群 $\boldsymbol{Z}_p^*$ の生成元 a を乗数とする乗算合同法乱数の l 連が定める l 次元格子 G_l のすべての格子点を含む平面群の最大間隔 $d_{\max}(l)$ は, 逆格子 G_l^* のベクトル $\boldsymbol{v} \neq \boldsymbol{0}$ の長さ $|\boldsymbol{v}|$ の最小値 $|\boldsymbol{v}|_{\min}$ から $d_{\max}(l) = \dfrac{p}{|\boldsymbol{v}|_{\min}}$ で与えられる.
(b) $|\boldsymbol{v}|_{\min}$ を与える $\boldsymbol{v}$ の探索は 0 ばかりではない整数デカルト座標 $v_1, v_2, \cdots, v_l$ で条件

$$v_1 + v_2a + v_3a^2 + \cdots + v_la^{l-1} \equiv 0 \pmod{p}.$$

を満たすものを持つ $\boldsymbol{v}$ の上だけで行えばよい. **(定理 4.7. 終り)**

G_l^* の逆格子ベクトル $\boldsymbol{v}$, 即ち上の条件を満たす整数デカルト座標 $v_1, v_2 \cdots, v_l$ を持つもの, は無限個あるが, その具体的な基 $\{\boldsymbol{e}_j^*\}$ の 1 組が既知だから, すべての $1 \leqq j \leqq l$ に対して $|\boldsymbol{v}|_{\min} \leqq |\boldsymbol{e}_j^*|$ は明らかで, 最短ベクトルは大きさ $|\boldsymbol{v}|$ が $\{|\boldsymbol{e}_j^*| \mid 1 \leqq j \leqq l\}$ の最小値, 高々 p 程度, 以下の整数座標を持つ $\boldsymbol{v} \in G_l^*$ の中で探せばよい. これは始めから有限探索問題である. 勿論乱数では p は 2^{31} 程度以上と大きいから, 有限探索と言っても実用には工夫がいる.

この探索アルゴリズムは Dieter[26] に与えられ, Knuth[2], 伏見 [4] にもプログラムとして示されている. 法 2^r での乗算合同法その他でのスペクトル検定に関しては関連文献 [27),28),26)] を, 特に線形合同法を主眼としては Knuth[52] を引用する.

Fishman と Moore[29] は素数の法 $2^{31} - 1 = 2147483647$ の乗算合同法について, $l = 2$ から $l = 6$ までの $d_{\max}(l)$ が理論的に取り得る最小の値[41]の 125%以内に収まる乗数 a をすべての原始根 $\phi(2147483646) = 534600000$ 個の中から探した. Park と Miller[24] が「ヘラクレス (の力技) 的 herculean」と形容したこの精査では約 400 の乗数が $7.5 \times 10^{-5}\%$ の確率で検定基準に合格したという. 第 1 位の乗数 $a = 950706376$ 等は IMSL の乱数ルーチン等にも組込まれていた.

同様の基準で Fishman[30] は法 2^{32} の場合のすべての乗数についても検定を行った. 合格したのは 132 個で, 合格率はやはり $4.9 \times 10^{-5}\%$ の程度である. これらの結果は原始根や $a \equiv 5 \pmod 8$ の乗数をでたらめに取っても, とても高性能なものには当たらない事を示す. まさに Park と Miller[24] の表題, "Good random number generators are hard to find"の通りで, この様な選択実装の問題についてはこの報告が再びよい情報源として勧められる.

スペクトル検定の内容, 乱数系列の l 連の E_l での美しい格子構造は, そんなに大きくない l までの分布しか必要としない問題については, Lehmer 以来追及された乗算合同法の見事

[41] これら可能な最小値についてはすぐ後のこの章の付録で $l = 2, 3$ の場合について触れる.

な適合を明らかにし, 徹底した検定からの最良結果の安全な利用を可能にする. 勿論我々は, 乗算合同法 l 連の分布密度の上限 $\approx p^{-l+1}$ から生じる本質的な短所と, それを克服するための (Tausworthe 他の) 方法等の必然も同時に見出した訳であるが.

問題 4.8.(a) ベクトル $\boldsymbol{e}^* \neq 0$ と $\boldsymbol{f}^*$, 例えば $\boldsymbol{e}^* = {}^t(x_1, x_2, \cdots, x_l),\ \boldsymbol{f}^* = {}^t(y_1, y_2, \cdots, y_l),\ l \geqq 2$ が与えられた時, 実数 t に対するベクトル $\boldsymbol{f}^* - t\boldsymbol{e}^*$ の長さの 2 乗

$$|\boldsymbol{f}^* - t\boldsymbol{e}^*|^2 = t^2\boldsymbol{e}^* \cdot \boldsymbol{e}^* - 2t\boldsymbol{e}^* \cdot \boldsymbol{f}^* + \boldsymbol{f}^* \cdot \boldsymbol{f}^*, \quad |\boldsymbol{e}^*| > 0$$

の最小値は $t = \dfrac{\boldsymbol{e}^* \cdot \boldsymbol{f}^*}{|\boldsymbol{e}^*|^2}$ の時の値 $|\boldsymbol{f}^*|^2 - \dfrac{(\boldsymbol{e}^* \cdot \boldsymbol{f}^*)^2}{|\boldsymbol{e}^*|^2}$ で与えられる事, また $\boldsymbol{f}^* - t\boldsymbol{e}^* \neq \boldsymbol{0}$ ならこの t が $(\boldsymbol{f}^* - t\boldsymbol{e}^*) \perp \boldsymbol{e}^*$ を意味する (シュミット Schmidt の直交化である) 事を示せ.

(証明)
$$|\boldsymbol{f}^* - t\boldsymbol{e}^*|^2 = |\boldsymbol{e}^*|^2 \left\{ t^2 - 2t\frac{\boldsymbol{e}^* \cdot \boldsymbol{f}^*}{|\boldsymbol{e}^*|^2} + \left(\frac{\boldsymbol{e}^* \cdot \boldsymbol{f}^*}{|\boldsymbol{e}^*|^2} \right)^2 \right\} + |\boldsymbol{f}^*|^2 - \frac{(\boldsymbol{e}^* \cdot \boldsymbol{f}^*)^2}{|\boldsymbol{e}^*|^2}$$
$$= |\boldsymbol{e}^*|^2 \left(t - \frac{\boldsymbol{e}^* \cdot \boldsymbol{f}^*}{|\boldsymbol{e}^*|^2} \right)^2 + |\boldsymbol{f}^*|^2 - \frac{(\boldsymbol{e}^* \cdot \boldsymbol{f}^*)^2}{|\boldsymbol{e}^*|^2}.$$

この最小値は $t = \dfrac{\boldsymbol{e}^* \cdot \boldsymbol{f}^*}{|\boldsymbol{e}^*|^2}$ の時の $|\boldsymbol{f}^*|^2 - \dfrac{(\boldsymbol{e}^* \cdot \boldsymbol{f}^*)^2}{|\boldsymbol{e}^*|^2}$ である. $\boldsymbol{e}^*$ と $\boldsymbol{f}^* - t'\boldsymbol{e}^*$ との直交条件は

$$\boldsymbol{e}^* \cdot (\boldsymbol{f}^* - t'\boldsymbol{e}^*) = \boldsymbol{e}^* \cdot \boldsymbol{f}^* - t'\boldsymbol{e}^* \cdot \boldsymbol{e}^* = 0, \quad t' = \frac{\boldsymbol{e}^* \cdot \boldsymbol{f}^*}{|\boldsymbol{e}^*|^2},$$

だから上の最短の $\boldsymbol{f}^* - t\boldsymbol{e}^*$ は $\boldsymbol{e}^*$ と直交する. ■

問題 4.8.(b) 問題 4.1. では法 11 の乗算合同法乱数として乗数に法 11 の原始根 a を取った系列 $x_k = a^k \pmod{11}$ の 2 連の作る 2 次元 Marsaglia 図を作った. $a = 2$ の場合の p.50 の (a) 図での $d_{\max}(2) = d_{\max}$ を考えよう. 我々の考察によると, それは 2 次元逆格子基ベクトル[42]

$$\boldsymbol{e}^* = \begin{pmatrix} -a \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ 1 \end{pmatrix}, \quad \boldsymbol{f}^* = \begin{pmatrix} p \\ 0 \end{pmatrix} = \begin{pmatrix} 11 \\ 0 \end{pmatrix}$$

の**整数係数** 1 次結合ベクトル

$$\boldsymbol{v} = j'\boldsymbol{e}^* + k'\boldsymbol{f}^*, \ \ j', k' \text{は共に } 0 \text{ になる事はない整数},$$

の長さ $|\boldsymbol{v}|$ の最小値 $|\boldsymbol{v}|_{\min}$ によって $d_{\max} = \dfrac{p}{|\boldsymbol{v}|_{\min}} = \dfrac{11}{|\boldsymbol{v}|_{\min}}$ で与えられる. デカルト座標

$$\boldsymbol{v} = \begin{pmatrix} j \\ k \end{pmatrix}$$

で言えば, 条件

$$j + ak = j + 2k \equiv 0 \pmod{11}$$

を満たす整数の組 $\{j, k\}$ に対して $|\boldsymbol{v}| = \sqrt{j^2 + k^2}$ の (0 ではない) 最小値を求めればよい. 既に $\boldsymbol{e}^*$ が長さ $|\boldsymbol{e}^*| = \sqrt{2^2 + 1^2} = \sqrt{5}$ を満たす逆格子ベクトルとして存在するから, 整数 j, k

[42] 一般に逆格子基ベクトルの中で $\boldsymbol{e}_1^*$ が一番長いので以下これを $\boldsymbol{f}^*$ と書き, 2 次元で残る逆格子ベクトル $\boldsymbol{e}_2^*$ を $\boldsymbol{e}^*$ と記す.

としては $j^2+k^2 \leqq 5$, 即ち $|j|, |k| \leqq 2$ となるものだけを考えれば十分である. 人間計算機になってこれらをしらみ潰しに調べ, 下表を完成して $|\boldsymbol{v}|_{\min}$ と $d_{\max}$ を求めなさい.

(解) $\{j,k\}$ と $\{-j,-k\}$ は同じ $|\boldsymbol{v}|$ を与えるから $j \geqq 0$ だけでよい. 法 11 で表は次の通り:

j	0		1					2				
k	±1	±2	-2	-1	0	1	2	-2	-1	0	1	2
$j+2k$	±2	±4	-3	-1	1	3	5	2	0	2	4	6
$j+2k \equiv 0$								○				
$\lvert\boldsymbol{v}\rvert = \sqrt{j^2+k^2}$								$\sqrt{5}$				

上の表から j,k としてはただ 1 組 $\pm\boldsymbol{e}^*$ に相当するものだけが発見されて

$$|\boldsymbol{v}|_{\min} = \sqrt{5}, \quad d_{\max} = \frac{11}{|\boldsymbol{v}|_{\min}} = \frac{11}{\sqrt{5}}. \qquad \textbf{(問題 4.8.(b) 終り)}$$

問題 4.8.(c) 法 $p=11$ で原始根 $a=7$ を乗数に取る場合には逆格子の基ベクトルは

$$\boldsymbol{e}^* = \begin{pmatrix} -a \\ 1 \end{pmatrix} = \begin{pmatrix} -7 \\ 1 \end{pmatrix}, \ |\boldsymbol{e}^*| = \sqrt{50}, \qquad \boldsymbol{f}^* = \begin{pmatrix} p \\ 0 \end{pmatrix} = \begin{pmatrix} 11 \\ 0 \end{pmatrix}, \ |\boldsymbol{f}^*| = 11,$$

である. これらのベクトルはかなり長いので, 逆格子基ベクトルが t を任意の整数として $\{\boldsymbol{e}^*, \boldsymbol{f}_1^* := \boldsymbol{f}^* - t\boldsymbol{e}^*\}$ でもよい事[43]を利用して $|\boldsymbol{f}_1^*| = \min$ となる $\boldsymbol{f}_1^*$ で $\boldsymbol{f}^*$ を置き換える. $|\boldsymbol{f}_1^*| = |\boldsymbol{f}^* - t\boldsymbol{e}^*|$ が最小になるのは, 問題 4.8.(a) によれば

$$t = \frac{\boldsymbol{e}^* \cdot \boldsymbol{f}^*}{|\boldsymbol{e}^*|^2} = \frac{-77}{50} = -1.54$$

の場合だが, これは整数ではないので最も近い整数の場合, $\boldsymbol{f}' := \boldsymbol{f}^* + \boldsymbol{e}^*$, $\boldsymbol{f}'' := \boldsymbol{f}^* + 2\boldsymbol{e}^*$ の 2 つを考え, 長さの短い方を $\boldsymbol{f}_1^*$ としよう. $\boldsymbol{f}_1^*$ を決定しなさい.

(解)

$$\boldsymbol{f}' = \begin{pmatrix} 11-7 \\ 0+1 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \end{pmatrix}, \quad |\boldsymbol{f}'| = \sqrt{17},$$

$$\boldsymbol{f}'' = \begin{pmatrix} 11-14 \\ 0+2 \end{pmatrix} = \begin{pmatrix} -3 \\ 2 \end{pmatrix}, \quad |\boldsymbol{f}''| = \sqrt{13}.$$

故に $\boldsymbol{f}_1^* = \boldsymbol{f}'' = \begin{pmatrix} -3 \\ 2 \end{pmatrix}$, $|\boldsymbol{f}_1^*| = \sqrt{13}$. **(問題 4.8.(c) 終り)**

問題 4.8.(d) $|\boldsymbol{f}_1^*| < 4$ なので, もう $\boldsymbol{v} = {}^t(j,k)$ でそのデカルト座標が条件

$$j + ak = j + 7k \equiv 0 \pmod{11}, \quad |j| \leqq 3, \quad |k| \leqq 3$$

を満たすものをしらみ潰しに調べ上げてその長さ $\sqrt{j^2+k^2}$ の最小値を直接求めよう. 下の表を完成し, $|\boldsymbol{v}|_{\min}$ と $d_{\max} = \dfrac{11}{|\boldsymbol{v}|_{\min}}$ を決定しなさい.

(解)

[43] 確かに, $m\boldsymbol{e}^* + n\boldsymbol{f}_1^* = (m-nt)\boldsymbol{e}^* + n\boldsymbol{f}^*$ は, m,n がすべての整数を動く時, $m'\boldsymbol{e}^* + n\boldsymbol{f}^*$ の形のすべての整数の組 $m' = m-nt, n$ に対するベクトル全体, 即ち全逆格子ベクトルを動く.

j	0			1						
k	±1	±2	±3	-3	-2	-1	0	1	2	3
$j+7k$	±7	±14	±21	-20	-13	-6	1	8	15	22
$j+7k\equiv0$										○
$\lvert\boldsymbol{v}\rvert=\sqrt{j^2+k^2}$										$\sqrt{10}$

j	2							3						
k	-3	-2	-1	0	1	2	3	-3	-2	-1	0	1	2	3
$j+7k$	-19	-12	-5	2	9	16	23	-18	-11	-4	3	10	17	24
$j+7k\equiv0$									○					
$\lvert\boldsymbol{v}\rvert=\sqrt{j^2+k^2}$									$\sqrt{13}$					

故に $|\boldsymbol{v}|_{\min}=\sqrt{10}$, $d_{\max}=\dfrac{11}{|\boldsymbol{v}|_{\min}}=\dfrac{11}{\sqrt{10}}$. なお最短逆格子ベクトルは

$$\boldsymbol{v}=\begin{pmatrix}1\\3\end{pmatrix}=\boldsymbol{f}'+\boldsymbol{f}''=2\boldsymbol{f}^*+3\boldsymbol{e}^*. \qquad \textbf{(問題 4.8.(d) 終り)}$$

問題 4.8.(e) 乗数 $a=2$ に対する p.50 の Marsaglia 図は次の座標の点からなる:

$$(1,2),\ (2,4),\ (4,8),\ (8,5),\ (5,10),\ \cdots.$$

視察では $y=2x,\ \ y=2x\pm11,\ \cdots$ の平行直線の間隔が最も大きい. この間隔 d_2 を求め, 問題 4.8.(b) の結果と比較しなさい. また乗数 $a=7$ に対する Marsaglia 図は次の点からなる:

$$(1,7),\ (7,5),\ (5,2),\ (2,3),\ (3,10),\ \cdots.$$

最も間隔の大きいのは $(2,3),\ (5,2)$ を通る直線に平行なものの様に見える. この間隔 d_7 を求めて, 問題 4.8.(d) の結果と比較しなさい.

(解) 平面の直線 $ax+by+c=0$ と点 (x_0,y_0) の距離 d は $d=\dfrac{|ax_0+by_0+c|}{\sqrt{a^2+b^2}}$ である. d_2 は原点 $(0,0)$ と直線 $y=2x+11,\ 2x-y+11=0$ との距離で, 問題 4.8.(b) の通り

$$d_2=\frac{11}{\sqrt{2^2+1^2}}=\frac{11}{\sqrt{5}}.$$

$(2,3),\ (5,2)$ を通る直線の方程式は $y-3=\dfrac{2-3}{5-2}(x-2)=-\dfrac{x-2}{3},\quad x+3y-11=0$ であるから, これと原点 $(0,0)$ との距離は問題 4.8.(c) の結果に合致して

$$d_7=\frac{11}{\sqrt{1^2+3^2}}=\frac{11}{\sqrt{10}}<d_2.$$

故に p.50 の図 (a), (b) の視察による我々の直感通り乗数 $a=7$ の方が乗数 $a=2$ よりは優れている. なお $(5,2),\ (7,5)$ を通る直線の方程式は

$$y-2=\frac{5-2}{7-5}(x-5),\quad 3x-2y-11=0$$

で, 原点からの距離は $d = \dfrac{11}{\sqrt{13}}$, これが問題 4.8.(d) の表の通り法線ベクトル $\pm(3,-2)$ に対応する 2 番目に大きい格子間隔である. **(問題 4.8.(e) 終り)**

付録. $d_{\max}(l)$ の $l = 2, 3$ での理論的最小値

$l = 2$ 次元の平面内にデカルト座標を整数とは限定しない 1 次独立な基ベクトル $\boldsymbol{e}_1^*,\ \boldsymbol{e}_2^*$ があるとし, これらで作られる格子,

$$\boldsymbol{v} = v_1\boldsymbol{e}_1^* + v_2\boldsymbol{e}_2^*,\ \ v_1,\ v_2 = 0, \pm1, \pm2, \cdots$$

を考える. 基準を統一するために基ベクトル $\boldsymbol{e}_1^*,\ \boldsymbol{e}_2^*$ の張る平行四辺形の面積は 1,[44] 即ち第 3 成分 0 を補って 3 次元空間の中のベクトルと考えて作られる外積 $\boldsymbol{e}_1^* \times \boldsymbol{e}_2^*$ を用いて記すと

$$|\boldsymbol{e}_1^* \times \boldsymbol{e}_2^*| = 1, \tag{4.1}$$

が成り立つと常に仮定する. ベクトルの加法が示す様にベクトル $\boldsymbol{e}_1^*, \boldsymbol{e}_2^*, \boldsymbol{e}_1^* - \boldsymbol{e}_2^*$ は 3 角形を作る. どの様な基ベクトル $\boldsymbol{e}_1^*, \boldsymbol{e}_2^*$ を選べば, この 3 角形の 3 辺の長さ $|\boldsymbol{e}_1^*|, |\boldsymbol{e}_2^*|, |\boldsymbol{e}_1^* - \boldsymbol{e}_2^*|$ の最大値 $d_{\max}(2)$ が条件 (4.1) の下で, 即ち 3 角形の面積が $\dfrac{1}{2}$ 一定で最小になるだろうか.

まず次が成り立つ:

Corollary 4.9. 一定の面積の 3 角形で 1 つの辺を固定する時, 他の 2 辺の最大のものが最小になるのはこの固定辺の上の 2 等辺 3 角形の場合である.
(証明) 面積一定の条件で 3 角形の頂点は固定された底辺に平行に自由に移動できる. 底辺

以外の 2 辺の大きい方が最小になるのは明らかに 2 等辺の場合である. ■

だから問題は底辺の長さ a を変える時, 2 つの等辺の長さ b との大きい方が最小になるのはどんな場合かで, どれを底辺に取っても事情は同じだから直感的には正 3 角形の場合だろうと答えは示唆される. もう少し精密には, 底辺 a の両側の等角を θ として条件 (4.1) が

$$\text{条件}\ \frac{1}{2} = \frac{1}{2}a \cdot \frac{a}{2}\tan\theta, \quad \tan\theta = \frac{2}{a^2}$$

を与える事, 従って 2 等辺の長さ $b = \dfrac{a}{2\cos\theta}$ で

[44] 逆格子の基ベクトル $\boldsymbol{e}_1^*, \boldsymbol{e}_2^*, \cdots, \boldsymbol{e}_l^*$ の行列式が示す様に, 本当は 1 ではなく p をこれらが張る体積とすべきだが, これは次元 l に関係ない一定の数だから以下 1 と簡単化する.

$$b^2 = \frac{a^2}{4}(1+\tan^2\theta) = \frac{a^2}{4}\left(1+\frac{4}{a^4}\right)$$

の最小が (a での微分で)a が増大して $a^2 = 2$ となる, つまり $\tan\theta = 1, \theta = \dfrac{\pi}{4}$ になる時生じるが, しかしその前に $\theta = \dfrac{\pi}{3}$ の正 3 角形の時 $a^2 = \dfrac{2}{\sqrt{3}} < 2$ が実現している事, からも知られる.

このように, 2 次元での $d_{\max}(2)$ の最小値は $\boldsymbol{e}_1^*$ と $\boldsymbol{e}_2^*$ が長さ $\dfrac{\sqrt{2}}{\sqrt[4]{3}}$ の正 3 角形を張る逆格子, 3 角格子 trigonal lattice, を作る場合である. 乱数の 2 連の作る元の格子はこの逆格子の逆格子で, それも同じ 3 角格子の形である事は 2 次元行ベクトルと見た $\boldsymbol{e}_1^*$, $\boldsymbol{e}_2^*$ の作る逆行列を計算してみれば容易にわかる. 勿論, この格子の基ベクトルは整数成分にはならないから法が素数 p の乗算合同法乱数の 2 連では実現しない. ただ乱数のスペクトル検定ではその 2 連の作る最大格子間隔が (4.1) と同じ条件の下で $p\dfrac{\sqrt[4]{3}}{\sqrt{2}}$ よりどれくらい大きいか, と乗数 a の選択の基準にして比較する事ができる. 文献 [29] ならこれが 125%以内, という訳である.

3 次元では, 逆格子の基である 3 つのベクトルが作る 4 面体を同様に考えると, 一定の体積の 4 面体 (同じベクトルの作る平行 6 面体と比べて 4 面体は底面の面積が $\dfrac{1}{2}$, 高さは同じで, 錐体だから体積は $\dfrac{1}{6}$) のうち正 4 面体で辺の最大値が最小になる. 証明はそう難しくはない. 実際 1 つの面の 3 角形 ABC を底面として固定すると, 体積一定の条件のもとで残る

ただ 1 つの頂点 P はこの底面に平行に動く事ができるが, 底 3 角形の 3 頂点 A, B, C から P

までの 3 辺 PA, PB, PC の長さの最大値が最小になるのは, これらの 3 辺が等しい時である事はすぐわかる. この時点 P から底 3 角形へ下ろした垂線の脚 H は 3 角形 ABC で 3 頂点から等距離にある; $\mathrm{HA} = \mathrm{HB} = \mathrm{HC}$. 点 H は 3 角形 ABC の外接円の中心, 外心である. だから問題の一端は面積一定の 3 角形の外接円の半径が最小になるのはどんな場合か, であり, 解は問題を逆転して一定の半径の円が外接する 3 角形の面積が最大になる形を考えて正 3 角形と得られる. こうして正 3 角形の上の一定の体積の正 3 角錐でその辺の最大のものが最小になるのは正 4 面体である事の証明が残る. これは最も正確には解析で微分を用いて行われるが, 結論が常識通りだから実行する価値はあまりない. ここでは受け入れてしまおう. あとは体積 $\dfrac{1}{6}$ の正 4 面体の辺の長さ $d_{\max}(3) = \sqrt[6]{2}$ の算出と, この正 4 面体の 3 稜, 方向だけで言えば

面心立方格子　　体心立方格子

例えば $(0,1,1),\ (1,0,1),\ (1,1,0)$ の 3 ベクトル, が作る「面心立方」と呼ばれる格子である事, 実空間で乱数の 3 連の作る格子としてはこれら 3 ベクトルを行とする行列の逆行列の列ベクトルに相当する「体心立方」になる事, の証明になる. これらの事柄もそれぞれ面白いが, 結論はみな常識から外れるものではないから, 証明の詳細に立ち入る事は興味ある読者に任せる. 4 次元以上については「数の幾何学」の文献 [31] を参照して頂きたい.

5. 有限体と原始多項式

5.1. まえおき: $Z/p = Z_p$ の上の線形漸化式

乱数の乗算合同法 $x_k \equiv ax_{k-1} \pmod p$, p は素数, は整数係数の n 次線形漸化式

$$x_k \equiv b_1x_{k-1} + b_2x_{k-2} + \cdots + b_nx_{k-n} \pmod p, \quad b_n \neq 0 \tag{5.1}$$

の最も簡単な場合である. 乱数生成方式は, 自然にと言ってよいだろうが, 乗算合同法から (5.1) の利用へと発展した. この一般の (5.1) の場合を見越して乗算合同法 $x_k - ax_{k-1} \equiv 0$ の解の形を $x_k = c\lambda^k$ と仮定して代入しよう. 得るのは方程式 $c\lambda^k - ac\lambda^{k-1} \equiv 0$ である. $c = 0$ 或いは $\lambda = 0$ なら「すべての k で $x_k = 0$」のつまらない解になるから $c\lambda \neq 0$ と仮定して $c\lambda^{k-1}$ で両辺を割ると, λ を決定する方程式 $\lambda - a = 0$ とその解 $\lambda = a$, そしてそれによる既知の漸化式解 $x_k = ca^k,\ c = x_0$ が得られる. 今の簡単な $x_k \equiv ax_{k-1}$ ではこの回りくどい解法はあまり有難くはない. しかしもっと一般の, 特に我々に興味ある整数の $\{b_1, b_2, \cdots, b_n\}$ を係数に持つ上の線形 n 次漸化式 (5.1) についてはこれは重要な考え方である. 暫くの間「法 p」や「整数係数」の限定を忘れて係数 $\{b_1, b_2, \cdots, b_n\}$ は任意の複素数であり, (5.1) は法 p ではなく複素数としての等式とし, 目標を**出発値** $\{x_0, x_1, \cdots, x_{n-1}\}$ **から系列全体** $\{x_k\}$ **を決定する初期値問題**と明確にしよう. この様な再帰的 recursive な関係, 漸化式 recursion equation, 階差或いは差分方程式 difference equation について, 次の Lemma の (a)–(c) は容易に見られる:

Lemma 5.1. (a) (5.1) を満たす任意の 2 つの解 $\{x_k\},\ \{y_k\}$ の 1 次結合 $Ax_k + By_k$, A, B は定数, も再び (5.1) の解である (漸化式 (5.1) の線形性).
(b) 初期条件 $\{x_0, x_1, \cdots, x_{n-1}\}$ を与えれば, (5.1) の解 $\{x_k\}$ は $k \geqq n$ に対して一意に定まる.
(c) (5.1) に付随する決定方程式或いは特性 (固有) 方程式

$$\lambda^n = b_1\lambda^{n-1} + b_2\lambda^{n-2} + \cdots + b_{n-1}\lambda^1 + b_n \tag{5.2}$$

が単根 $\{a_1, a_2, \cdots, a_n\}$ だけを持てば,[45] すべての $k = 0, 1, 2, \cdots$ に対して

$$\{x_k^{(i)} := (a_i)^k |\ \ i = 1, 2, \cdots, n\}$$

は漸化式を満たし, 初期値問題の解が次の表現を持つ:

$$x_k = c_1x_k^{(1)} + c_2x_k^{(2)} + \cdots + c_kx_k^{(n)} = c_1(a_1)^k + c_2(a_2)^k + \cdots + c_n(a_n)^k. \tag{5.3}$$

ここで定数 $c_1, c_2, \cdots, c_n$ は初期条件 $\{x_0, x_1, \cdots, x_{n-1}\}$ で決定され, 逆に任意の初期条件 $\{x_0, x_1, \cdots, x_{n-1}\}$ は定数 $\{c_1, c_2, \cdots, c_n\}$ を適当に定めて実現される.
(証明) (a) $\{x_k\},\ \{y_k\}$ が共に (5.1) を満たせば,

$$x_k = b_1x_{k-1} + b_2x_{k-2} + \cdots + b_nx_{k-n},$$

[45] 乱数問題の線形漸化式では既約多項式だけが興味の対象となる; 特性多項式が既約でない線形漸化式の解の周期は短くなり, しかもその周期は初期条件の取り方で複雑に変るので乱数としての実用に耐えない. だからここでは特性方程式が重解を持つ場合は考えない. 但し任意の法 m での線形漸化式全般を対象にするなら避け難く重解を持つ特性方程式も考慮すべきで, 状況の記述には以下の「有限体」とそれを係数とする「既約多項式」の範囲を越えて「環」への視野が求められる. 興味ある読者は第 7 章通読後に付録 B を参照して頂きたい. なお実数や複素数の上での線形漸化式の特性重根は行列の一般化固有値や対応する一般固有空間の発祥の問題で, これらについては杉山 [32], 笠原 [33], 松阪 [34] 等がよい参考書である.

$$y_k = b_1 y_{k-1} + b_2 y_{k-2} + \cdots + b_n y_{k-n}$$

が成り立つ. これらに係数 A, B を掛けた和は,

$$Ax_k + By_k = b_1(Ax_{k-1} + By_{k-1}) + b_2(Ax_{k-2} + By_{k-2}) + \cdots + b_n(Ax_{k-n} + By_{k-n}),$$

であり, $z_k = Ax_k + By_k$ と書き直せば確かに (5.1) が成り立つ:

$$z_k = b_1 z_{k-1} + b_2 z_{k-2} + \cdots + b_n z_{k-n}.$$

(b) 一般に x_k はそれに先立つ n 個のもの, $\{x_{k-1}, x_{k-2}, \cdots, x_{k-n}\}$, から漸化式 (5.1) によって $x_k = b_1 x_{k-1} + b_2 x_{k-2} + \cdots + b_n x_{k-n}$ とただ一通りに決定される. $k = n, n+1, \cdots$ として命題は自明である.

(c) i が $1, 2, \cdots, n$ のどれであっても, $x_k = (a_i)^k$ で定義される系列 $\{x_k\}$ が (5.1) の解である事は, 実際 $\lambda = a_i$ を代入して (5.2) を用いれば,

$$\begin{aligned} b_1 x_{k-1} + b_2 x_{k-2} + \cdots + b_n x_{k-n} &= b_1\lambda^{k-1} + b_2\lambda^{k-2} + \cdots + b_n\lambda^{k-n} \\ &= (b_1\lambda^{n-1} + b_2\lambda^{n-2} + \cdots + b_n\lambda^{n-n})\lambda^{k-n} = \lambda^n\lambda^{k-n} = \lambda^k = x_k \end{aligned}$$

となることから見られる. 故に (a) の線形性から (5.3) も (5.1) の解である. この (5.3) の形の 1 次結合で任意の初期値問題の解が作れる事を見よう. 表現 (5.3) が出発値 $\{x_0, x_1, \cdots, x_{n-1}\}$ を持つ条件は, 係数 $\{c_1, c_2, \cdots, c_n\}$ の n 元連立 1 次方程式

$$\begin{aligned} x_0 &= c_1(a_1)^0 + c_2(a_2)^0 + \cdots + c_n(a_n)^0, \\ x_1 &= c_1(a_1)^1 + c_2(a_2)^1 + \cdots + c_n(a_n)^1, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_{n-1} &= c_1(a_1)^{n-1} + c_2(a_2)^{n-1} + \cdots + c_n(a_n)^{n-1}, \end{aligned} \tag{5.4}$$

である. (5.4) の係数行列式は良く知られた Vandermonde 行列式:[46]

$$D = D(a_1, a_2, \cdots, a_n) := \begin{vmatrix} (a_1)^0 & (a_2)^0 & \cdots & (a_n)^0 \\ (a_1)^1 & (a_2)^1 & \cdots & (a_n)^1 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ (a_1)^{n-1} & (a_2)^{n-1} & \cdots & (a_n)^{n-1} \end{vmatrix}$$

$$\begin{aligned} &= (a_2 - a_1)(a_3 - a_1)(a_4 - a_1)\cdots(a_n - a_1) \\ &\quad \times (a_3 - a_2)(a_4 - a_2)\cdots(a_n - a_2) \\ &\quad \times (a_4 - a_3)\cdots(a_n - a_3) \end{aligned}$$

[46]実際, 下の行列式 D は $\{a_1, a_2, \cdots, a_n\}$ の整式 (多項式) であり, 列の交換で符号を変えるから, 例えば a_j の整式と見て $a_j = a_k$ の時 $D = 0$ となる; $a_j = a_k$ なら D で a_j と a_k を交換しても同じだが, 行列式としては符号が変るから $D = -D$, $2D = 0$, $D = 0$ である. だから因数定理によって因数 $(a_j - a_k)$ がある. 即ち D は因数 $(a_j - a_k)$ をすべての番号の対 (j, k) に対して含み, (5.5) の右辺の積は左辺の行列式に因数として含まれる. $a_1, a_2, \cdots, a_n$ についての次数を考えると, (5.5) の左辺の行列式 D も右辺の積も, $0 + 1 + \cdots + (n-1) = n(n-1)/2$ で同じである. 故に (5.5) 左辺の行列式は右辺の積の定数倍である; D の対角成分の積 $(a_1)^0(a_2)^1(a_3)^2(a_4)^3\cdots(a_n)^{n-1}$ と右辺での同じ項の係数が 1 である事とを考えるとこの定数は 1 で, 下の (5.5) の等式の成立がわかる.

$$\times \quad \cdots\cdots\cdots$$

$$\times(a_n - a_{n-1}) \tag{5.5}$$

である. $\{a_k\}$ は方程式 (5.2) の単根ばかりで皆異なるから (5.5) から $D \neq 0$. これで (5.3) は任意の $\{x_0, x_1, \cdots, x_{n-1}\}$ に対して一意な解 $\{c_1, c_2, \cdots, c_n\}$ を持つと判明する. ■

(c) で定数 $c_1, c_2, \cdots, c_n$ が初期条件 $\{x_0, x_1, \cdots, x_{n-1}\}$ からきまるとはわかっても, 解 $\{x_k\}$ がどんな性質を持つのかはまだ明らかではないが, これは後に正確に議論される.

我々は「法 p で」の制限を外して漸化式の解系列を実数や複素数として考えて来た. その結果 n 次決定方程式 (5.2) を複素数の範囲で考えたが, 得られた結果は法 p でも正しい事を強調する. 実際, (5.2) を普通の複素数で考えて解いて, たとえ虚根等が出て来たとしても, それを用いた (5.3) の $\{x_k\}$ はたしかに漸化式 (5.1) の解である. 我々に興味のある整数係数の漸化式 (5.1) の場合, その解は初期値 $\{x_0, x_1, \cdots, x_{n-1}\}$ で一意に決定され, 初期値さえ整数なら以後の解系列 $\{x_k\}$ が (5.3) の形であっても必ず全体は整数列である事を保証されるので, 整数の合同算法で見た様にこの整数系列を最後に法 p で考えても最初から法 p の簡約を取っても (5.1) は成り立つ. しかし問題は $\{x_k\}$ に最長周期を与える構造の理解である. 乗算合同法の一般解 $x_k = a^k x_0$ は a が複素数等ではなく整数そのものの易しい場合だが, それでも合同算法から作られる $\boldsymbol{Z}_p^*$ の巡回群構造を考えずに原始根の存在等を見る事は困難だったろう. 一般の n 次線形漸化式についても, 考察の鍵は**決定方程式 (5.2) を素数の法 p での数体系 $\boldsymbol{Z}_p = \boldsymbol{Z}/p = \{0, 1, \cdots, p-1\}$ で解く**,[47] 或いは**整数係数の多項式を法 p の四則算法で因数分解する**という, 今の所途方もなく見える考えが与える.

一体どのようにして古い時代にこのような飛躍に達したのか畏敬を禁じ得ないが, 現在では我々にも容易に辿れる道が開かれている. 例から始めてこれを目指そう.

5.2. 簡単な例

代数方程式を解く事は多項式の因数分解と同じである. 上に述べた素数の法 p の計算での因数分解では, 法 p の選択毎に普通の実数, 複素数の場合とはかけ離れた様相が現れる事もあるが, 全体的には 2 次方程式での虚数の導入と大変よく似た統一的構造がある. てんでばらばらな様相としては, 例えば 2 を法とする $\boldsymbol{Z}_2 = \{0, 1\}$ の数体系では「因数分解 $z^2 + 1 \equiv z^2 + 2z + 1 \equiv (z+1)^2 \pmod 2$」が $2z \equiv 0$ によって成り立ち, 方程式 $z^2 + 1 \equiv 0$ は $\boldsymbol{Z}_2$ の中で解けて $z = 1 \equiv -1$ が 2 重解になる事を挙げておこう. 多項式 $f(z) = z^2 + 1$ は法 2 の約束の数体系では**既約 irreducible=因数分解不可能**, でなく**可約 reducible=因数分解可能**なのである. このような結果は奇妙で面白いがあまり本質的ではない. 真の難しさ, そして統一的な美しい姿, は方程式 $f(z) = z^2 + z + 1 \equiv 0$ の様に $\boldsymbol{Z}_2 = \{0, 1\}$ で解を持たない ($f(z)$ で $z = 0, 1$ とおいて見よう) 場合, 即ち「$\boldsymbol{Z}_2$ 係数で因数分解できない, $\boldsymbol{Z}_2$ 上既約な多項式 $f(z)$」で生じる. この場合が乱数にとっては主な興味の対象なのである.

多項式やその因数分解は数や文字の加減乗除 (4 則算法) で行われる. だから問題への直感

[47] 既に第 2 章, p.24 で触れた通り, 素数 p の場合, 整数の集合としての $\boldsymbol{Z}/p = \{0, 1, \cdots, p-1\}$ から 0 を除いたものが集合としての乗法群 $\boldsymbol{Z}_p^*$ なので, この近縁を強調して素数の p に限って $\boldsymbol{Z}/p$ を $\boldsymbol{Z}_p$ と書く. これから導入する加法と乗法の定義された集合, 「体 field」, としての見方からは $\boldsymbol{Z}_p$ はよく $\boldsymbol{F}_p$ とも記される.

を獲得するためには法 p での四則算法や式の因数分解の例を考えるべきである. ただし法 2 での $z^2+z+1\equiv 0$ は少しややこしい. $p=3$ を法として簡単な $f(z)=z^2+1=0$ を取ろう. $\boldsymbol{Z}_3=\{0,1,2\equiv -1\}$ を数の全体, 加減乗法はすべて法 3 で定義する, として以下 mod 3 は略す. $\boldsymbol{Z}_3$ の上でのこの簡単な 2 次方程式は $f(0)=1,\ f(\pm 1)=2\equiv -1,$ によって $\boldsymbol{Z}_3$ 内に解を持たず, 因数定理 Corollary 1.12.(p.12) から $\boldsymbol{Z}_3$ 係数の (モニックな)1 次因数を含む事ができない ($\boldsymbol{Z}_3$ で既約である). といっても, $\boldsymbol{Z}_3$ 係数のモニックな 1 次因数は $z-0=z,\ z-1,$ $z-2\equiv z+1$ の 3 個だけだけであるが. そこで文字 z の取り得る数の全体 $\boldsymbol{Z}_3$ を拡張して, $f(z)=0$ の解 $z=i$ があるとし, この i も数の仲間にいれよう. $f(i)=i^2+1=0$ である. これは我々がかつて学校で 2 次方程式を解くために $i^2+1=0$ となる純虚数を想像し付け加えて実数から複素数への拡張を行ったのと姿も精神も全く同じである.

複素数と同様に $\boldsymbol{Z}_3$ に i を加えて四則算法が行える数の体系 K を作って見よう. このためには K は $\boldsymbol{Z}_3$ の元と新しい数 i とから加法で作られる「数 = 文字 i の式」はすべて含まなければならない. 数を代わりに (「代数」的に) 表す文字は $\boldsymbol{Z}_3$ の数の計算規則のすべてに従うべきだから, i と $\boldsymbol{Z}_3$ の数との計算規則もすべて $\boldsymbol{Z}_3$ の通りと仮定する.[48] i の 0 倍とは「なにもない」事で, $0i=0$ としよう. $1i$ は i, i が 2 つある事は $i+i=2i$ と書く. $i+i+i=3i$ になると, 我々の数 $\boldsymbol{Z}_3$ では 3 はなにもない 0 と同じなのだから, $3i\equiv 0i=0$ とすべきだし, $2i+i\equiv 0$ から $2i\equiv -i$ と書くのも自然である, こうして, 拡張された数の全体で加減法を不自由なく行うためには下の 9 個の元が必要だと見られる:

$$K\equiv\{0,\ 1,\ 2,\ i,\ 2i,\ 1+i,\ 2+i,\ 1+2i,\ 2+2i\}.$$

交換, 結合法則を用いたこれらのものの加法表の作成は容易で, 次の様にまとめられる:

$+$	0	1	2	i	$2i$	$1+i$	$2+i$	$1+2i$	$2+2i$	負数
0	0	1	2	i	$2i$	$1+i$	$2+i$	$1+2i$	$2+2i$	0
1	1	2	0	$1+i$	$1+2i$	$2+i$	i	$2+2i$	$2i$	2
2	2	0	1	$2+i$	$2+2i$	i	$1+i$	$2i$	$1+2i$	1
i	i	$1+i$	$2+i$	$2i$	0	$1+2i$	$2+2i$	1	2	$2i$
$2i$	$2i$	$1+2i$	$2+2i$	0	i	1	2	$1+i$	$2+i$	i
$1+i$	$1+i$	$2+i$	i	$1+2i$	1	$2+2i$	$2i$	2	0	$2+2i$
$2+i$	$2+i$	i	$1+2i$	$2+2i$	2	$2i$	$1+2i$	0	1	$1+2i$
$1+2i$	$1+2i$	$2+2i$	$2i$	1	$1+i$	2	0	$2+i$	i	$2+i$
$2+2i$	$2+2i$	$2i$	$1+2i$	2	$2+i$	0	1	i	$1+i$	$1+i$

乗法については, 文字 i が $z^2+1=0$ の解と想定され, $i^2=-1\equiv 2$ を満たすべき事から,

> 「文字 i を含む整式として, 係数は mod 3 で値を定め, その様な整式 a,b,c について交換法則 $a+b=b+a,\ ab=ba$, 結合法則 $a+(b+c)=(a+b)+c$, $a(bc)=(ab)c$, そして分配法則 $a(b+c)=ab+ac$ は成り立つとし, i^2 は常に $-1\equiv 2$ で置き換える」

と, 複素数と同じ規則で計算する. 下の問題で実際に見よう.

---

[48] 少し難しいが正確な考え方では「$m(i)=0$ となる数 i が云々の性質で存在する」とは言わずに, 係数 $\boldsymbol{Z}_3$ と同じ計算規則に従う文字 i (別に i ではなく x でも z でも構わない) が作る多項式の全体という「実在集合 K」に下で触れる「$m(i)$ を法とする等しさ」を定めて「数体系 K」を構成し, その上で $m(i)$ が因数分解され方程式 $m(i)=0$ が解を持つ, と議論する. 秋月-鈴木 16) の p.15 の端的な記述や Wärden[35] の p.129 以降を参照.

問題 5.2. $K^* := K - \{0\} = \{1,\ 2,\ i,\ 2i,\ 1+i,\ 2+i,\ 1+2i,\ 2+2i\}$ について, その乗積表を算出し, 逆元 (逆数) も求めなさい.
(解) 乗積表は下の通り:

$\times$	1	2	i	$2i$	$1+i$	$2+i$	$1+2i$	$2+2i$	逆数
1	1	2	i	$2i$	$1+i$	$2+i$	$1+2i$	$2+2i$	1
2	2	1	$2i$	i	$2+2i$	$1+2i$	$2+i$	$1+i$	2
i	i	$2i$	2	1	$2+i$	$2+2i$	$1+i$	$1+2i$	$2i$
$2i$	$2i$	i	1	2	$1+2i$	$1+i$	$2+2i$	$2+i$	i
$1+i$	$1+i$	$2+2i$	$2+i$	$1+2i$	$2i$	1	2	i	$2+i$
$2+i$	$2+i$	$1+2i$	$2+2i$	$1+i$	1	i	$2i$	2	$1+i$
$1+2i$	$1+2i$	$2+i$	$1+i$	$2+2i$	2	$2i$	i	1	$2+2i$
$2+2i$	$2+2i$	$1+i$	$1+2i$	$2+i$	i	2	1	$2i$	$1+2i$

(問題 5.2. 終り)

我々が複素数の計算に倣って行った事を振り返ろう. 文字 i の多項式の加減乗法で作り出されるのは文字 i の様々な $\boldsymbol{Z}_3$ 係数多項式 $f(i)$ である. i^2 が出る度にそれを -1 と置く事は $m(i) = i^2 + 1$ が出現する度にそれを 0 とする規則である. $\boldsymbol{Z}_3$ 係数の任意の多項式 $f(i)$ は monic な多項式 $m(i)$ によって $\boldsymbol{Z}_3$ の係数だけを用いて割る事ができて,[49] その結果を $f(i) \equiv q(i)m(i) + r(i) \pmod 3$, $q(i)$ は商, $r(i)$ は高々 1 次の余り とすれば, $m(i) \equiv 0$ とする計算は $f(i)$ をこの余り $r(i)$ と同等視して $m(i)$ の倍数を無視する事に等しい. だから文字 i の $\boldsymbol{Z}_3$ 係数の任意多項式の集合に係数の法 3 での同一視と共に多項式間の同等の法として $m(i)$ も入れて, 各多項式を余りの 1 次式 $r(i)$ で代表させ, 法 $(3, m(i))$ で定義した加減法の体系が K であり, 0 となるものを除いた乗法の体系が K^* である.

法 $(3, m(i))$ での加法 $+$ の表は, $(K, +)$ が群である事を示す. 実際この算法 $+$ で K は表のとおり閉じているし (公理 0), 他の元を変えない「単位元」に相当する $0 := 0 + 0i$ があり (公理 2; 以下 0 は単位元でなく「0 元, 零元」と呼ぶ), 各行各列には必ず 1 つだけ 0 があって, 「加えて 0 になる逆 元 $\equiv$ 負 元」の存在もわかる (公理 3) からである.

なぜ $(K, +)$ は閉じて群を作るのだろう? 1 つの理解は K の元が, 法 $m(i)$ を入れた事によって, 文字 i の $\boldsymbol{Z}_3$ 係数 1 次式の全体と同じ事, $K = \{a + bi |\ a, b \in \boldsymbol{Z}_3\}$, になった構造と我々の用いた計算

$$(a + bi) \pm (a' + b'i) = (a \pm a') + (b \pm b')i \quad \text{(複号同順)}$$

から得られる. 加減法の結果はやはり文字 i の 1 次式の形になり, $\boldsymbol{Z}_3$ の元を成分とする 2 成分ベクトル (a, b) の計算 $(a, b) \pm (a', b') = (a \pm a', b \pm b')$ (複号同順) と同じである. だから K は, 丁度複素数が複素平面上の点として 2 個の実数成分で表された様に, $\boldsymbol{Z}_3$ の 2 成分を持つベクトル全体と同等, 「$\boldsymbol{Z}_3$ 係数 2 次元ベクトル空間」そのものと言える. この様な 2 成分を持つ群は群 $(\boldsymbol{Z}_3, +)$ の 2 個から作られた直積群と呼ばれ, $\boldsymbol{Z}_3 \times \boldsymbol{Z}_3$ と記される. もっと一般に法多項式 $m(i)$ が n 次なら, 得られるベクトル空間は $1, i, i^2, \cdots, i^{n-1}$ の係数に対応して n 次元になるだろう. 文字 i を含む式の計算について法 $m(i)$ と共に我々が仮定したのは,

[49] 「最高次の係数が 1」の多項式を「monic」と言った. $\boldsymbol{Z}_p = 0, 1, \cdots, p-1$, p は素数, 今の場合 $p = 3$, とすると, $\boldsymbol{Z}_p$ 係数の任意多項式 $m(i)$ が monic なら勿論, monic でなくても 0 ではない最高次の係数の逆数は $\boldsymbol{Z}_p^*$ が乗法群であり存在するので, $m(i)$ による $\boldsymbol{Z}_p$ 係数多項式の $\boldsymbol{Z}_p$ 係数での割り算は可能である.

$\boldsymbol{Z}_3$ 係数での加法に関しては要するに, i の多項式の全体をこの様なベクトル空間と見做す, という事であった.

乗積表は, 集合 $K^* := K - \{0\} =$「K から 0 を 除いたもの」が $\bmod 3$ での乗法 $\times$ に関して群 (アーベル群) であることを示している. 実際 K^* は $\times$ で閉じている (公理 0). 乗法で他の元を変えない単位元 1 は K^* に存在し (公理 2), 乗積表の各行各列には必ず 1 つ 1 があり, 掛け合わせて 1 になる逆元も存在する (公理 3).

なぜ K^* は乗法群を作るのか? それは, $m(i) = 0$ の仮定が文字 i の式の積を $\boldsymbol{Z}_3$ 上既約な $m(i)$ を法として定義するからである. $m(i)$ の既約性は, $\boldsymbol{Z}_3$ 係数の 0 ではない $m(i)$ より低次の 2 式 (K^* の任意の 2 元) の積が $m(i)$ の倍数 ($\equiv 0 \mod m(i)$) にはならない事, 積 (又はそれを $m(i)$ で割った余り) が再び K^* に属し, 「K^* が乗法で閉じる」構造を保証する. $\boldsymbol{Z}_3$ の単位元, 0 次の整式 $e(i) = 1 := 1 + 0i$, は K^* の単位元を準備している. また法 3 で 1 次以下で 3 と $m(i)$ を法として 0 に合同ではない式 $f(i), g(i), h(i)$ について, $g(i) - h(i) \not\equiv 0$ なら積 $f(i) \times \{g(i) - h(i)\}$ が $\boldsymbol{Z}_3$ 既約な $m(i)$ の倍数を作る (3 と $m(i)$ を法として 0 に合同になる) 事はなく $f(i)g(i) \not\equiv f(i)h(i)$, 故に K^* の乗積表の各行, 各列はすべて K^* の元の並べ換えになり, 必ず 1 が 1 つだけ入って $f(i)$ の逆元が確定する. K^* の乗法群構造は $\boldsymbol{Z}_3^*$ という礎材を **法多項式** $m(i)$ **の** $\boldsymbol{Z}_3$ **既約性**をほぞ, 鍵として組み合わせて構築されている事が見える.

我々は扱われた $m(i)$ の特定の形を超えて一般的な視野を得た:

> 四則算法可能な数体系 $\boldsymbol{Z}_3$ に同じ計算規則に従う文字 i の冪乗を添加して加減法で作った数 (整式) の体系 K は自然にベクトル空間 (加法に関する直積群) を構成する. もとの数体系で既約な多項式 $m(i)$ に基づく $m(i) = i^2 + 1 \equiv 0$ の規則, 即ち $m(i)$ で割った余りを取る, $m(i)$ を法とする約束は系 K(より適切には $m(i)$ を法とする K) から $\{0\}$ を除外した元の全体 K^* を乗法に関して群とし, 除法, 即ち任意の $f(i) \in K$ と $g(i) \in K^*$ に対する
>
> $$\text{商 } \frac{f(i)}{g(i)} := f(i)g(i)^{-1} \in K$$
>
> と定義される算法, も定義可能として, もとの数体系 $\boldsymbol{Z}_3$ と同じ四則演算の可能性を拡張された K の上で保証する.

今ではもう小さく見える事柄になったが, 得られた複素数 K の上では $\boldsymbol{Z}_3$ 上既約な多項式 $m(z) = z^2 + 1$ は可約となり, 方程式 $m(z) = 0$ は解ける. 実際 K^* の乗積表の 2 乗を与える部分, 対角線で $-1 \equiv 2$ を探して, 方程式 $m(z) \equiv 0$ の解が $z = i$ と $z = -i \equiv 2i$ で与えられ因数分解

$$z^2 + 1 \equiv (z - i)(z + i) \equiv (z - i)(z - 2i)$$

が成り立つ事が見られる.

$\boldsymbol{Z}_3$ から $m(i)$ を因数分解する数体系 K を作るこの手続きは, 上に示唆された通り $\boldsymbol{Z}_3$ 既約な任意の多項式 $m(i)$ を基にして可能である. 我々はガロア Galois に導かれて驚くべき認識に達した. 少なくともある種の数体系で既約な任意の多項式があれば, それを因数分解し代数方程式の解を与える様に数体系を拡大して「複素数を作る」方法があり, この「複素数」の体系そのものが上に見た様に既約多項式毎に存在し得て, 我々が学んだ実数の複素数への拡大はその一例に過ぎない!

5.3. 有限体

最長周期列, 慣用で M 系列, と呼ぶある特別な種類の線形漸化式の解の周期構造の詳しい解析は Zierler[36] によって行われた. 少し後に法 2 の場合の $\{0,1\}$ の M 系列を組み上げて例えば実際的 32 ビットの一様乱数とする基本アイデアが Tausworthe[10] そして Lewis-Payne[11] によって与えられ, 生成される一様乱数系列の統計的性質が論じられた. 方法を実際化する努力は伏見と手塚 [12] の高次均等分布を保証する最も一般の出発値設定条件に完成され, 乱数生成の実際的で最強力な方法として確立された. この成果と文献への approach や M 系列乱数設計方針の原理, 具体的には

(a) 有限体, 原始多項式と最大周期列 (M 系列) とは何か, どうしてその様なものが存在するのか,
(b) M 系列の基本性質, 実際乱数への応用に必要な $\boldsymbol{Z}_2 = \{0,1\}$ 上の M 系列の実数一様乱数への組み上げ問題とその解決,[12] 特に「高次均等分布」というもの実現方法,

についての構造の透視と理解とを我々は手にしたいと思う.

M 系列は符号理論 [37),38),39)] 等多くの工学応用に現れる. M 系列問題では「多項式の作る環 ring」という言葉がしばしば最も端的な証明を与えるが, 反面解析は抽象計算的で難解になる (第 7 章参照). 我々は M 系列乱数についても乗算合同法の様な視覚的で易しい理解を望むので, 以下では「有限体 finite field」の必要最小限の言葉で議論を統一しよう. それは有限体の膨大な応用への展望を得る道でもある.

有限体を考える根底には前節で問題として見られた「ある体系で因数分解できない既約な方程式を解く手続き」がある. 結果は実数の複素数への拡大と同じだった. 思いを統一するために虚数 imaginary number を振返ろう. 実数係数方程式 $x^2+1=0$ を解くため我々は「$i^2=-1$ を満たす数 i を想像 imagine し」, i と実数との加減乗法で作られる数, 即ち「文字 i の多項式 $F(i)$」, は $i^2=-1$ 或いは $i^2+1=0$ を用いて, 即ち

多項式 $F(i)$ の式 $m(i)=i^2+1$ による実数係数割り算

$$F(i) = q(i)(i^2+1) + r(i)$$

の余り $r(i)$ を取って $F(i)$ を i の 1 次式 $r(i)$ に置き換え, 表現

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2}$$

から a,b 共に 0 ではない複素数 $a+bi$ による割り算が i の 1 次式の枠の中で可能な事を見て,

「複素数とは $a+bi$(a,b は実数) の形のものの全体」

と認識し記憶した. 複素数 = 虚数 は実数にただ 1 つの「虚数単位 i」を付け加えただけのものだが, 考えて見れば不思議な事に, これによって例えばすべての複素数係数の n 次代数方程式 $f(z)=0$ は (重解の多重度も入れて) 丁度 n 個の解を必ず複素数の中に持つ (代数学の基本定理) 事になる. この見事な構造はさらに複素解析, 関数論などの美しい沢山の結果に裏打ちされて, 我々の理解の中で全く揺がない存在になっている.

複素解析もまだ建設中の時代に例えば $\boldsymbol{Z}_p$ に注目し, 実数係数で既約な法多項式 $m(i)=i^2+1$ の代りに 1 世紀以上も後に工学応用で幅広い応用を得る事になった

「$\boldsymbol{Z}_p$ 係数で既約な n 次法多項式 $m(i)$」

を取って全く同じ手続きを考え, 「それが四則計算可能な構造 (有限体) をすべての素数 p とすべての整数 $n \geqq 1$ に対して与える」事, 矛盾なく行え美しい諸結果に至るばかりでなく翻って複素数の存在様式の基本理解までも与える事はガロアの 1 つの仕事として見通されてしまった. 歴史は Lidl-Niederreiter[56] の preface や notes(p.73) にも詳しい. しかし発見には古代以来 2000 年と天才が必要だったとしても, 彼と続く人々が築いてくれたリフト, 体の公理体系, は我々にももう遠くはない. 是非ともそれに乗ろう.

「体 field」の概念は有理数, 実数や複素数の様に「加法と乗法」2 種類の演算が定義された集合から抽象される:

定義 5.3. 集合 K の任意の 2 元 x, y の間に加法 $x + y \in K$ と, (通常 $x{\cdot}y$, xy と略記する) 乗法 $x \times y \in K$ とが定義され, 次の公理を満たす時, K を体 field と呼ぶ:

公理 1 K は加法 $+$ に関してある元 $0 \in K$ を単位元 (以下「0 元, 零元」と呼ぶ) とするアーベル群である. 任意の $x \in K$ に対し加法の (右) 逆元を $-x \in K$ と記す:

$$x + (-x) = 0, \quad x - y := x + (-y).$$

公理 2 $K^* := K - \{0\}$ は空集合ではなく, 乗法演算についてある元 $e \in K$ を単位元とするアーベル群である.

公理 3 任意の $x, y, z \in K$ について, 左右の分配法則

$$x(y + z) = xy + xz, \quad (x + y)z = xz + yz$$

が成り立つ. **(定義 5.3. 終り)**

定義から体は必ず加法の単位元 0 と乗法の単位元 e とを含む. 群で我々はその単位元が一意 (存在してただ 1 つ) である事を見た. 故に体の 0 と e とは一意である. 体の元の総数を再び体の「位数 order」, 位数有限の体を有限体 finite field とそれぞれ言う. 公理 1–3 は体の零元 0 に乗法での特別な役割を与える:

Corollary 5.4. (a) 体 K の任意元 x に対して $0x = x0 = 0$.
(b) 次が成り立つ: $-(x + y) = (-x) + (-y)$, $-(xy) = (-x)y = x(-y)$, $(-x)(-y) = xy$.
(c) 任意の $x, y \in K$ について, $xy = 0$ なら $x = 0$ 又は $y = 0$ である. 対偶として x も y もどちらも 0 でなければ $xy \neq 0$.

(証明) (a) 0 は加法 $+$ の単位元だから自分自身に作用して $0 = 0 + 0$, 分配法則は $x0 + x0 = x(0 + 0) = x0$ を与える. $x0 \in K$ の逆元 $-(x0)$ を両辺に加えて $x0 = 0$ がわかる.
(b) 加法の可換性と結合法則から

$$(x + y) + \{(-x) + (-y)\} = \{x + (-x)\} + \{y + (-y)\} = 0 + 0 = 0,$$

即ち $-(x + y) = (-x) + (-y)$ が見られる. また

$$0 = 0y = \{x + (-x)\}y = xy + (-x)y,$$

$-(xy)$ を加えて $-(xy) = (-x)y$. x と y を交換して $-(xy) = x(-y)$.
$0 = (-x)0 = (-x)\{y + (-y)\}$ から

$$0 = (-x)y + (-x)(-y) = -(xy) + (-x)(-y).$$

xy を加え $xy = (-x)(-y)$.

(c) $xy=0$ と仮定する. このとき $x=0$ か $x\neq 0$ かのどちらかだが, もし $x\neq 0$ なら乗法に関する x の逆元 x^{-1} があり, (a) と結合法則によって $0=x^{-1}0=x^{-1}(xy)=(x^{-1}x)y=ey=y$ である. 故に $xy=0$ なら $x=0$ か $y=0$ かの少なくとも 1 方は必ず成り立つ. ■

実は素数 p に対する $\boldsymbol{Z}_p$ はすべての有限体の中に必ず存在する基礎構造である. この大切な事柄を見るのに暫く任意の体 K を想定しよう. 体 K の部分集合 F が同じ算法について再び体である時, F を K の「部分体 subfield」, K を F の「拡大体 overfield」と, それぞれ呼ぶ. 特に体の部分体が必ず自分自身である時「素体 elementary field」と呼ぶ. ここに有限体の単位元 e と $\boldsymbol{Z}_p$ とが特別な役割で登場する. K の任意元 x と任意自然数 m について

$$mx := x+x+\cdots+x \quad (m\text{ 個の和}) \tag{5.12}$$

と定義する. この定義からは K の他の任意元 y, 任意自然数 n について

$$\begin{aligned} mx+nx &= (x+\cdots+x)+(x+\cdots+x)=(m+n)x, \\ (mx)(ny) &= (x+\cdots+x)(y+\cdots+y)=(mn)(xy) \end{aligned} \tag{5.13}$$

は明らか. 体 K の単位元 e に対して, $pe=0$ となる最小の正の整数 p ($p\geqq 2$) があれば「体 K の標数 characteristic は p」と言い, その様な有限の p がない時「K の標数は 0」とする. 次が成り立つ:

Lemma 5.5. 位数有限の任意の体 (任意の有限体)F について:
(a) 標数 p は素数で, 任意の元 $x\in F$ について $px=0$.
(b) F の部分集合 $\Pi_p := \{je|\ j\in \boldsymbol{Z}_p$は整数$\}$ は $0,\ e\in F$ から (四則算法で) 生成され, F の最小の部分体, 素体で, $\boldsymbol{Z}_p$ に「同形 isomorphic[50]」である.
(c) K が体 F の任意の拡大体なら K は F 係数線形空間であり,[51] 従って $\mathrm{ord}(F)=q$ に対して $\mathrm{ord}(K)=q^n=\mathrm{ord}(F)^n$ となる正整数 n がある. n は F 係数線形空間 K の次元で, この事を「K の F に関する相対次数 $[K:F]=n$ である」とも「K は F の n 次拡大体である」とも言う.
(d) 特に標数 p の任意の有限体 K は Π_p を係数とする線形空間であり, その位数は (素数である) 標数 p のべき乗 p^n に限る.

(証明) (a) F の元は有限個だから, $1e, 2e, \cdots$ のすべてが異なる事はなく, $1\leqq m<n$ で $me=ne$ となる整数 m,n が必ずあり, $(n-m)e=0$ が成り立つ. この様な $n-m>0$ の最小値として標数 p は正である. $1e=e=0$ はあり得ず $p\geqq 2$. 仮に数 p が合成数で $j,k\geqq 2$ によって $p=jk$ と分解されれば (20) から $(je)(ke)=(jk)e=pe=0$, 故に Corollary 5.4.(c) により

---

[50] 2 つの体 K と K' とが同形であるとは, K と K' の元を 1 つずつ (1 対 1 に) 対応させて, しかも体の演算 $+$ と $\times$ を保つ事ができる, という事を言う. 即ち上の 1 対 1 対応が $\varphi: x\in K\to\varphi(x)\in K'$ なら

$$\varphi(x+y)=\varphi(x)+\varphi(y), \text{且つ}\varphi(xy)=\varphi(x)\varphi(y)$$

が成り立つ事, である.

[51] 正確には「K が F 係数線形 (或いはベクトル) 空間である」とは次の公理 (a),(b) が成り立つ事である:

(a) ベクトルと呼ぶものの集合 K に加法 $+$ が定義されて $(K,+)$ は可換群であり,
(b) 係数 (スカラー) と呼ぶものの体 F があって, 任意の $a\in F$ と $x\in K$ には積 (「スカラー倍」) $ax\in K$ が定義され, $a,b\in F$, $x,y\in K$ に対し次の性質 1-4 を持つ:

1. $a(bx)=(ab)x$ (結合法則),
2. $1x=x$,
3. $a(x+y)=ax+ay$ (ベクトルに関する分配法則),
4. $(a+b)x=ax+bx$ (スカラーに関する分配法則).

je 又は ke が 0 で, 標数は p より小さい j か k となり p の最小性に矛盾する. 故に仮定は誤りで p は素数. $pe = 0$ と結合法則から, 任意の $x \in F$ に対し

$$px = (e + e + \cdots + e)x = (pe)x = 0x = 0.$$

(b) $\Pi_p,\ \Pi_p^*$ が $+, \times$ について群の公理 0–2 を満たす事は明らかである. Π_p の任意の元 ke に対し ke の F での $+$ に関する逆元は $-ke = (p-k)e$ として存在する; 実際

$$ke + (p-k)e = (k + p - k)e = pe \equiv 0$$

だからである. $ke \in \Pi_p^*$ の時 ke の乗法 $\times$ での逆元は, k^{-1} を $\boldsymbol{Z}_p^*$ での k の逆数として $k^{-1}e$ と存在する; $(ke)(k^{-1}e) = (kk^{-1})e = \{1 + (p \text{ の倍数})\}e = e$. 故に公理 3 も成り立ち Π_p は体である. Π_p は $\{0, e\}$ だけから加減乗法で生成される. だから F のすべての部分体は $\{0, e\}$ と共に Π_p を含む. 特に Π_p の部分体は必ず Π_p を含み Π_p 自身であり, 定義によって Π_p は素体, F の最小の部分体である. 同形性については, $\boldsymbol{Z}_p$ の数 j と Π_p の元 je の対応 $\varphi(j) := je$ を考えればよい. 集合 $\boldsymbol{Z}_p$ と Π_p は同数 p 個の元を持つから φ は $\boldsymbol{Z}_p$ の全ての数 j と Π_p のすべての元 je との 1 対 1 対応であり, $\boldsymbol{Z}_p$ での加減乗法を Π_p のそれらに (5.13) によって対応付けている:

$$\begin{aligned}
(\boldsymbol{Z}_p\text{での演算} \pm \text{の対応物})\ \varphi(j \pm k) &= (j \pm k)e = je \pm ke \\
&= (\Pi_p\text{での} \pm \text{演算})\ \varphi(j) \pm \varphi(k), \\
(\boldsymbol{Z}_p\text{での演算}\times\text{の対応物})\ \varphi(jk) &= (jk)e = (je)\times(ke) \\
&= (\Pi_p\text{での}\times\text{演算})\ \varphi(j)\times\varphi(k).
\end{aligned}$$

この事を「φ は $\boldsymbol{Z}_p$ と Π_p の加法と乗法群の同形 (対応)」, 「体の同形 (対応)」, と言うのである.

(c) ベクトルの集合として体 K を, 係数体としてその部分体 F を, $+$ として体の加法を, 「ベクトル」$x \in K$ の $a \in F$ による「スカラー倍 ax」としては K での積を, それぞれ取って線形空間の公理が満たされている事は明らかである.[52] この線形空間の次元とは, F 係数での 1 次独立[53]「ベクトル」の最大数 n で, その存在は有限体 K では容易に見出される. 実際, $a_1 = e \in K$ と部分体 F には属さない K の任意元 a_2(があればそれ) を取り, K の部分集合

$$W_2 := \{c_1a_1 + c_2a_2 |\ \ c_1, c_2 \in F\}$$

を作る. この中のある元が 0 に等しい, $c_1a_1 + c_2a_2 = 0$, と仮定しよう. もし $c_2 \neq 0$ なら c_2 の F での逆元を掛けて $a_2 = -{c_2}^{-1}c_1e \in F$ となり, a_2 の取り方に矛盾する. だから $c_2 = 0$ であるべきで, 伴われて $c_1a_1 = c_1 = 0$ も成り立つ. 言い換えれば K のベクトル $\{a_1 = e,\ a_2\}$ は F 係数で 1 次独立である. これは W_2 の 2 元が等しい, 即ち $c_1a_1 + c_2a_2 = {c_1}'a_1 + {c_2}'a_2$, なら $c_1 = {c_1}'$, かつ $c_2 = {c_2}'$ となる事も意味し,[54] $W_2 \subset K$ は F 係数の 2 次元空間である. 故に位数 $\mathrm{ord}(F) = F$ の元の総数 $= q$ なら, W_2 の元の総数 $\sharp W_2$ は (c_1, c_2) の形の F 係数の組の総

[52]有限個の元しかない係数体 F を持つ線形空間 (ベクトル空間)K は我々には珍らしいし成書での記述も殆どないから以下少し丁寧に述べる. 実 (複素) 数係数線形代数の構成を学んだ教科書があれば, それに沿って下の様に見返せば, 部分空間, ベクトルの 1 次独立性, 基底, 次元, 1 次変換, 行列 (式), 連立 1 次方程式 $\cdots$ の証明論理が (「長さ」に関連する事は除いて) 成り立つと容易に分るだろう.

[53]ベクトル $\{a_1, a_2, \cdots, a_k\}$ が F 係数で 1 次独立とは, F の数 $c_1, c_2, \cdots, c_k$ に対して $c_1a_1 + c_2a_2 + \cdots + c_ka_k = 0$ となるのが $c_1 = c_2 = \cdots = c_k = 0$ に限る事を言う.

[54]実際 $(c_1 - {c_1}')a_1 + (c_2 - {c_2}')a_2 = 0$, 即ち $c_1 - {c_1}' = 0, c_2 - {c_2}' = 0$ なのだから $c_1 = {c_1}'$, かつ $c_2 = {c_2}'$.

数で $\sharp W_2 = q^2$ である. もし $W_2 = K$ ならこれで命題 (c) は証明された事になる. そうでなければ, K には W_2 には属さない元 a_3 があるからそれを取り,

$$W_3 := \{c_1a_1 + c_2a_2 + c_3a_3 |\ \ c_1, c_2, c_3 \in F\}$$

を作る. 再び $c_1a_1 + c_2a_2 + c_3a_3 = 0$ なら $c_1 = c_2 = c_3 = 0$ である事は $c_3 \neq 0$ を仮定して生じる矛盾から示される. こうして F 係数 3 次元空間 $W_3 \subset K$ が得られ, $\sharp W_3 = q^3$ である. K は有限個の元しか持たないからこの手続きは必ず有限回で終了し, ある正の整数 n があって

$$K = W_n = \{c_1a_1 + c_2a_2 + \cdots + c_na_n |\ \ c_j \in F,\ \ 1 \leqq j \leqq n\},$$

$$K \text{ の元の総数} = \mathrm{ord}(K) = \text{係数の組 } (c_1,\, c_2,\, \cdots,\, c_n) \text{ の総数} = q^n = \mathrm{ord}(F)^n,$$

が成り立つ. n は部分体 (係数体)F 上の K の次元である.
(d) 上の (c) の部分体 F を $\Pi_p,\ \mathrm{ord}\,\Pi_p = p$ に取れば明らか. ■

以下では Π_p は $\boldsymbol{Z}_p$ と同一視し, もはや証明等で概念の混乱を招く恐れは少ないので乗法の単位元 e は 1 と記す. 我々は殆ど $\boldsymbol{Z}_p$ 係数多項式だけを必要とするが, その限定は議論の一般性を隠すので, 以下暫くの間係数体を標数 p, 位数 $q = p^m$ の一般の体 F と置き, F の拡大体を K と記す.

5.4. 有限体上の既約多項式, 特に原始多項式

体 F の元を係数に持ち, F の数と同じ計算規則に従う文字 z の多項式の全体を $F[z]$ と記す. $F[z]$ の一般元は次の形である:

$$f(z) = b_0z^n + b_1z^{n-1} + \cdots + b_{n-1}z^1 + b_nz^0,\ \ b_j \in F,\ \ 0 \leqq j \leqq n.$$

体 F 係数の任意の n 次多項式は $b_0 \in F^* := F - \{0\}$ の逆元 ${b_0}^{-1}$ を掛けて monic にする事が常に可能で, monic な多項式だけを考えても一般性を失わない.

元 $a \in F$ が F 係数多項式 $f(z)$ に対して $f(a) = 0$ を与える事を, 「a は方程式 $f(z) = 0$ の解」とも「a は多項式 $f(z) \in F[z]$ の根」とも言う. 念のため, $f(z) \in F[z]$ が 2 つ以上, それぞれ 1 次以上の F 係数多項式の積の時「F 係数で可約 reducible, 或いは F 可約」と, そう分解できない時「F 係数で既約 irreducible, 或いは F 既約」と呼ぶ約束も確認する. F 係数多項式の F 内の根に対する次の事柄 (a),(b) は $\boldsymbol{Z}/m$ 上の Corollary 1.12., $\boldsymbol{Z}/p = \boldsymbol{Z}_p$ 上の定理 1.13., 共に p.12, とそれぞれ同様に証明される:

Corollary 5.6. (a) (因数定理) 体 F を係数に持つ文字 z の多項式 $f(z) \in F[z]$ について, もし $a \in F$ が $f(z)$ の根, 即ち $f(a) = 0$ なら, $f(z)$ は因数 $z - a$ で F 係数で割り切れる.
(b) 任意の体 F において F 係数 n 次多項式の根は n 個以下しかない.
(証明) (a) $f(z) = b_0z^n + b_1z^{n-1} + \cdots + b_{n-1}z^1 + b_n$, $b_j \in F$, $0 \leqq j \leqq n$, $b_0 \neq 0$ の形とする. 体 F が許す加減乗法から $f(z)$ の monic な $z - a$ による F 係数での割り算は勿論可能で

$$f(z) = (z - a)g(z) + r,\ \ \text{商 } g(z) \in F[z] \text{ は } n - 1 \text{ 次},$$

の形になる. r は 0 次式 (定数 $\in F$), $f(a) = 0$ から $r = 0$, 故に $f(z) = (z - a)g(z)$ である.
(b) F 内の任意の根 a に対して, (a) によって $f(z)$ は因数 $z - a$ を持ち, F 係数因数分解 $f(z) = (z - a)g(z)$ が成り立つ. $g(z)$ の任意の根 $b \in F$ についても再び因数定理から $g(z)$ が因数 $z - b$ を持つ. この議論を続けて

$$f(z) = (z-a)(z-b)\cdots(z-e)h(z)$$

の形に到達する; $h(z) \in F[z]$ は定数, 1 つの F 既約な 2 次以上の多項式又は 2 個以上のそれらの積で, $h(z) = 0$ とする $z \in F$ は存在しない. $f(z)$ の次数から $\{a, b, \cdots, e\}$ は全部でも n 個以下である. 上に現れた $a, b, \cdots, e \in F$ 以外に $f(z)$ の F 内の根はない; 前の $\boldsymbol{Z}_p$ での議論を再現して記憶を再生しよう. 仮に別の $a' \in F$ があって $f(a') = 0$ を与えると仮定すると

$$0 = (a'-a)(a'-b)\cdots(a'-e)h(a')$$

となるが, この右辺はすべて F の 0 ではない元の積で, 体 F ではこの等式はあり得ず[55]矛盾である. 故に n 次の $f(z) \in F[z]$ の体 F 内の根は必ず n 個以下である. ■

直ちに次が得られる:

定理 5.7. 任意の有限体 K の乗法群 K^* は巡回群である. K の標数が p, K が $\boldsymbol{Z}_p$ の n 次拡大なら, 原始元 primitive element とも呼ばれる生成元 generator $a \in K^*$ が $\phi(p^n-1)$ 個存在し, これによる K^* の巡回表現

$$K^* = \{a^1,\, a^2,\, \cdots,\, a^{p^n-1} = 1\},$$

が成り立つ.

(証明) 群 K^* の元 z に対する方程式 $z^k = 1$ は K 係数 k 次方程式だから Corollary 5.6.(b) によってその根 $(\neq 0)$ は K 即ち乗法群 K^* 中で k 個以下である. 故に群 K^* が巡回群である条件 (p.42, 定理 3.4.) は満たされ, K^* を巡回的に生成する生成元 $a \in K^*$ が存在し, すべて異なる $\{a^1,\, a^2,\, \cdots,\, a^{p^n-1} = 1\}$ が K^* のすべてである. K^* の任意の元を a で表し (「巡回表現」し) て a^j とするとその位数は $\mathrm{ord}(a^j) = \dfrac{p^n-1}{(p^n-1, j)}$ であり,[56] これが $\mathrm{ord}(a^j) = p^n - 1$ になるのは分母が 1, j が p^n-1 と素な場合である. 故に

$$\text{原始元の数} = \text{その様な } j \text{ の数} = (p^n-1 \text{ と素な正整数の総数}) =: \phi(p^n-1). \qquad ■$$

有限体のあり方はこの定理で大きく規定されてしまう. まず任意の有限体 K は $\boldsymbol{Z}_p$ にただ一つの元 (生成元)a を添加して四則算法で作られる事がわかる. この事実を「有限体 K はある素数 p に対する $\boldsymbol{Z}_p$ の単純拡大である」と言う. また次の構造も明白になる:

Lemma 5.8. 素体 $\boldsymbol{Z}_p$ の n 次拡大である任意の有限体 K の元 x はすべて ($\boldsymbol{Z}_p$ 係数) 方程式

$$G(z) := z^{p^n} - z = 0 \tag{5.14}$$

を満たし, K はこの方程式の根すべての集合である. 特に K の任意の生成元を a とすれば, $G(z)$ の K 係数での 1 次因数への分解 splitting が次の形で成り立つ:

$$G(z) = z(z-a^1)(z-a^2)\cdots(z-a^{p^n-1}). \tag{5.15}$$

(証明) 位数 p^n-1 の乗法群 K^* の一般元 a はラグランジュの定理によって $a^{p^n-1} = 1$ を満たし, $z^{p^n} - z = 0$ の根である. $a = 0$ もこの方程式は満たすから, K の p^n 個の元全体が高々同

[55] Corollary 5.4.(c), p.72.

[56] これはわかりにくい事柄だからもう 1 度確認する. $1 \leqq j \leqq p^n-1$ に対して $(a^j)^h = a^{jh} = e$ となるのは jh が (巡回) 群の位数 $g := p^n-1$ の倍数になる時である. $d = (j, g) =$「j と g の最大公約数」, $g = g'd$, $j = j'd$ と置くと g' と j' は素で, $g = g'd$ が $jh = j'hd$ を割り切る最小の h は $h = g' = g/d = g/(j, g)$ である. 即ち $h = \mathrm{ord}(a^j) = g/(j, g) = (p^n-1)/(p^n-1, j)$.

数しか存在しないはずの (5.14) の異なる解, $G(z)$ の根, のすべてである. (5.15) は体係数での因数定理 Corollary 5.6.(a) で $F = K, f(z) = G(z)$ として明らか. ■

F(係数) 既約多項式は F 係数では因数分解できないが, 体 F の拡大体 K の数の使用も許すとどうなるかを考えよう. まず p.73 の Lemma 5.5.(c) が与える次の展望に注意する:

Lemma 5.9. 体 F の n 次拡大体 K の任意元 $a \in K$ は高々 n 次の F 係数多項式の根である.
(証明) 体 K は部分体 F を係数とする n 次元ベクトル空間を作る. F 係数で 1 次独立なベクトル (K の元) の最大数は次元と同じ n だから, $n+1$ 個の K の元 $a^0, a^1, a^2, \cdots, a^n$ は F 係数で必ず 1 次従属である. 故にすべてが 0 ではない係数 $c_0, c_1, \cdots, c_n \in F$ があって $f(a) = c_0a^n + c_1a^{n-1} + \cdots + c_n = 0$ が成り立つ; a は高々 n 次の F 係数多項式 $f(z) = c_0z^n + c_1z^{n-1} + \cdots + c_n \in F[z]$ の根である. $a \in F$ なら $f(z) = z - a$ としてよい. $a \in K - F$ では $f(z)$ は 2 次以上の F 係数多項式でなければならない. ■

さらに次が成り立つ:

Lemma 5.10. 位数 q の体 F, F の n 次拡大体 K と K の任意元 a について:
(a) a を根とする F 係数の既約多項式 $f(z) \in F[z]$ は F の定数倍の任意性を除いて一意であり, 「元 $a \in K$ の F 上の (即ち F 係数の) 最小多項式 minimal polynomial」と呼ばれる. a を根とするすべての F 係数多項式は, a の最小多項式 $f(z)$ によって F 係数で整除される.
(b) 特に $G(z) := z^{q^n} - z$ は F 係数で $f(z)$ によって整除される.
(証明) (a) 前 lemma から $a \in K$ には 1 次以上高々 n 次の F 係数の多項式が必ずあってその根になる. それら多項式中の最小次数で monic なもの[57]を $f(z)$ とする. a を根とする任意の F 係数多項式 $g(z)$ を取ると, それは次数が $f(z)$ 以上だから $f(z)$ で F 係数で割る事ができる. 結果の $g(z) = f(z)q(z) + r(z)$ で $z = a$ として $0 = g(a) = f(a)q(a) + r(a) = r(a)$ であり, $r(z)$ が 1 次以上なら a は $f(z)$ より低次の F 係数多項式 $r(z)$ の根となる. これはあり得ないから $r(z)$ は 0 次の定数 0, F 係数因数分解 $g(z) = f(z)q(z)$ が成り立つ. 特に $g(z)$ が既約なら商 $q(z)$ は 0 次でなければならず $g(z) =$ 定数$\times f(z)$. 即ち a を根とする F 既約多項式は定数倍を除いて一意に定まる.
(b) 位数 q の体 F の n 次拡大として K は位数 q^n で, 0 を除く乗法群 K^* の全ての元 a はラグランジュの定理 a^{q^n-1}=1 を満たす. 或いは 0 も含めれば, K の全ての元は方程式 $G(z) = z^{q^n} - z = 0$ の解である. 故に (a) によって a の最小多項式 $f(z)$ はこの多項式 $G(z)$ を割り切る因数である. ■

上の事実と後の議論の便宜のために, 以下では一般性を失う事なく最小多項式をモニックなものに限る.

次の Corollary 5.11. から Lemma 5.15. までは乱数問題で中心的な役割を担う「原始多項式」への最後の準備である.

Corollary 5.11. (a) 標数 p の任意の体 K とその任意元 x, y に対して次が成り立つ:

$$(x+y)^{p^m} = x^{p^m} + y^{p^m}, m = 1, 2, \cdots.$$

(b) 位数 q の有限体 F, 任意の $u, v \in F$, F の任意拡大体 K とその任意元 $x, y \in K$ について

[57] これは実は 1 つしかないがまだそれはわからない. 故に 2 つ以上あればその任意の 1 つを取るとする. monic にする必要はないが, そうする事は 0 でない最高次の係数の逆数を掛けて常に可能である.

次が成り立つ:

$$(ux+vy)^q = ux^q + vy^q.$$

(証明) (a) まず, 素数 p 乗に関する 2 項展開を考える:

$$(x+y)^p = x^p + {}_p\mathrm{C}_1 x^{p-1}y + \cdots + {}_p\mathrm{C}_{p-1}xy^{p-1} + y^p.$$

$1 \leqq j \leqq p-1$ の場合, 2 項係数 ${}_p\mathrm{C}_j = \dfrac{p!}{j!(p-j)!}$ の分母の $j!$ と $(p-j)!$ の中に (p が素数なので) p を割り切る因数はなく, ${}_p\mathrm{C}_j$ は全体として p の倍数, 即ち ${}_p\mathrm{C}_j \equiv 0 \pmod p$. 故に

$$(x+y)^p = x^p + y^p.$$

p 乗を m 回繰り返したものが p^m 乗だから, 上から次が得られる:

$$(x+y)^{p^m} = \{\cdots[(x^p+y^p)^p]^p\cdots\}^p = \{\cdots[x^{p^2}+y^{p^2}]^p\cdots\}^p = \cdots = x^{p^m} + y^{p^m}.$$

(b) F の標数を p とし, $q = p^m$ と置く. p は当然 K の標数でもある. (a) の結果で x, y を ux, vy で置き換える. 任意の $u, v \in F$ に対し $u, v = 0$ なら自明に, $u, v \in F^*$ なら Lagrange の定理の $u^{q-1} = 1$ と $v^{q-1} = 1$ を経て, $u^q = u,\ v^q = v$ が成り立つから,

$$(ux+vy)^q = u^q x^q + v^q y^q = ux^q + vy^q. \qquad \blacksquare$$

簡単な問題で上の内容を確認しよう:

問題 5.12. 2 項係数 ${}_n\mathrm{C}_j,\ 0 \leqq j \leqq n$, をパスカルの三角形で $n = 11$ まで構成して, 素数の $n = p$ に対しては両端の $j = 0, n$ に対する 1 を除いて $\bmod p$ で 0 に合同である事を示せ.
(解) 次の通り:

${}_1\mathrm{C}_j$	1	1									
${}_2\mathrm{C}_j$	1	2	1								
${}_3\mathrm{C}_j$	1	3	3	1							
${}_4\mathrm{C}_j$	1	4	6	4	1						
${}_5\mathrm{C}_j$	1	5	10	10	5	1					
${}_6\mathrm{C}_j$	1	6	15	20	15	6	1				
${}_7\mathrm{C}_j$	1	7	21	35	35	21	7	1			
${}_8\mathrm{C}_j$	1	8	28	56	70	56	28	8	1		
${}_9\mathrm{C}_j$	1	9	36	84	126	126	84	36	9	1	
${}_{10}\mathrm{C}_j$	1	10	45	120	210	252	210	120	45	10	1
${}_{11}\mathrm{C}_j$	1	11	55	165	330	462	462	330	165	55	11	1

確かに, 素数 p に対する ${}_p\mathrm{C}_j$ では両端以外は法 p で 0 である. **(問題 5.12. 終り)**

Corollary 5.13. 位数 q の有限体 F の元を係数とする任意多項式 $f(z)$ については

$$\{f(z)\}^q = f(z^q)$$

が成り立つ.
(証明) 一般性を失う事なく $f(z) = b_0 z^r + b_1 z^{r-1} + \cdots + b_r,\ b_k \in F$ の形として Corollary 5.11. を繰り返し適用すると,

$$\{f(z)\}^q = \{b_0 z^r + (b_1 z^{r-1} + \cdots + b_{r-1}z + b_r)\}^q$$

$$= (b_0 z^r)^q + (b_1 z^{r-1} + \cdots + b_{r-1} z + b_r)^q$$
$$= {b_0}^q z^{rq} + (b_1 z^{r-1})^q + (b_2 z^{r-2} + \cdots + b_{r-1} z + b_r)^q$$
$$= \cdots\cdots\cdots$$
$$= b_0 (z^q)^r + b_1 (z^q)^{r-1} + \cdots + b_{r-1} z^q + b_r = f(z^q). \qquad \blacksquare$$

Lemma 5.14. 標数 p の有限体 K の乗法群 K^* の任意元 $a \neq 0$ に対して

$$a,\ \ a^p,\ \ a^{p^2} = (a^p)^p,\ \ a^{p^3} = [(a^p)^p]^p,\ \ \cdots,\ \ a^{p^k},\ \ ;$$
$$a^{-1},\ \ (a^{-1})^p,\ \ (a^{-1})^{p^2} = [(a^{-1})^p]^p,\ \ \cdots,\ \ (a^{-1})^{p^k},\ \ \cdots$$

の形の元はすべて K^* で同位数である.

(証明) $[K : \boldsymbol{Z}_p] = n$, 即ち体 K は $\boldsymbol{Z}_p$ の n 次拡大体だとし, K^* の生成元 b による巡回表現 $a = b^j$ を取れば, 定理 5.7. の証明で再確認した様に次が成り立つ:

$$\mathrm{ord}(a) = \mathrm{ord}(b^j) = \frac{p^n - 1}{(p^n - 1, j)}, \quad \mathrm{ord}(a^p) = \mathrm{ord}(b^{jp}) = \frac{p^n - 1}{(p^n - 1, jp)}.$$

素数 p に対し p と $p^n - 1$ とは共通素因数を持たず互いに素で $(p^n - 1, jp) = (p^n - 1, j)$ だから $\mathrm{ord}(a) = \mathrm{ord}(a^p)$. これを繰り返して

$$\mathrm{ord}(a) = \mathrm{ord}(a^p) = \mathrm{ord}\{(a^p)^p\} = \mathrm{ord}(a^{p^2}) = \cdots = \mathrm{ord}(a^{p^k}) = \cdots.$$

また $1 \leqq k < \mathrm{ord}(a)$ のとき $1 = (aa^{-1})^k = a^k (a^{-1})^k$ なら, $a^k \neq 1$ だから $(a^{-1})^k = 1$ ではあり得ず, $k = \mathrm{ord}(a)$ のとき始めて $a^k = 1$ と共に $(a^{-1})^k = 1$ となる. 故に $\mathrm{ord}(a^{-1}) = \mathrm{ord}(a)$ である. $(a^{-1})^p = (a^p)^{-1}$ だから, 残る結論は前半から従う. $\blacksquare$

Lemma 5.15. K が F の拡大体, $a \in K$ が F 係数の (必ずしも既約ではない) 任意多項式 $f(z)$ の 1 根, $\mathrm{ord}(F) = q$ なら, 次の K の元はすべて $f(z)$ の同位数の根である:

$$a,\ a^q,\ a^{q^2} = (a^q)^q,\ a^{q^3} = ((a^q)^q)^q,\ \cdots. \tag{5.16}$$

これらは $f(z)$ の互いに共役 conjugate な根と呼ばれる.

(証明) $f(a) = 0$ なら, Corollary 5.13. は任意の正の整数 s に対し $f(a^{q^s}) = \{[f(a)^q]^q \cdots\}^q = 0$ を保証する. 故に (5.16) の元は皆 $f(z) = 0$ の解である. F の標数, 即ち K の標数を p とすれば $\mathrm{ord}(F) = q = p^m$ となる正の整数 m があるから任意の正の整数 j に対して $a^{q^j} = a^{p^{mj}}$ であり, Lemma 5.14. によって (5.16) の元の位数はすべて等しい. $\blacksquare$

上の Lemma 5.15. で $a \in F$ なら $a^q = a$ となって命題は自明で, ここでは F に根を持たない $f(z)$, F 既約であるか或いはその様な因数の積か, の場合しか興味はない. F 既約多項式の場合には $f(z)$ の根は実は (5.16) の形のものがすべてだが, これは次の章で触れる.

さあ, 特別な既約多項式, 原始多項式について知識を収束しよう. 原始多項式は普通素体 $\boldsymbol{Z}_p$ を係数として考えるが, 少し一般化して述べる:

定理 5.16. 位数 q の有限体 F とその n 次拡大体 K, $n \geqq 2$ について,
(a) 乗法群 K^* の任意の生成元 a の F 係数の最小多項式 (モニックな F 既約多項式) は n 次であり, すべて K^* の生成元である n 個の共役な単根

$$a,\ a^q,\ a^{q^2} = (a^q)^q,\ \cdots,\ a^{q^{n-1}} \tag{5.17}$$

を持つ. これを「F 上の n 次原始多項式 primitive polynomial」と呼ぶ.
(b) F 係数 n 次多項式 $f(z)$ が原始多項式である必要十分条件は次の (i),(ii) である:
(i) $f(z)$ が F 既約で,
(ii) $f(z)$ が $z^r - z$ を F 係数で割り切る様な r の最小値は $r_{\min} = q^n$ である.
(証明) Lemma 5.9. から K^* の生成元 a は高々 n 次の F 係数多項式の根, 従って a の F 係数最小多項式 $f(z)$ も高々 n 次である. $f(z)$ は Lemma 5.15. によって K^* の同位数の元, 即ちすべて K^* の生成元である (5.17) の全体も根とするが, $q, n \geqq 2$ から

$$q^{n-1} < (q-1)(q^{n-1} + q^{n-2} + \cdots + 1) = q^n - 1,$$

a は位数 $q^n - 1$ の生成元だから (5.17) の n 個は皆 K の異なる元である. 故にそれらすべてを根に持つ $f(z)$ は n 次と確定し, (5.17) の単根がその根の全体で, $f(z)$ は K で 1 次因数に分解される. 位数から a は $\boldsymbol{Z}_p$ 係数 (当然 F 係数) の方程式 $H(z) = z^{q^n-1} - 1 = 0$ を, 従って $G(z) = z^{q^n} - z = 0$ も満たし, Lemma 5.10.(b) によって a の F 係数最小多項式 $f(z)$ は $G(z)$ を F 係数で割り切る. $f(z)$ が $z^r - z$ を F 係数で割り切るなら $a^r - a =$「$f(a)$ の倍数」$= 0$ で, $a \neq 0$ だから $a^{r-1} - 1 = 0$, 即ち $a^{r-1} = 1$ で, $r-1$ は生成元 a の位数 $\mathrm{ord}(a) = q^n - 1$ の倍数である. 即ち $f(z)$ が $z^{r-1} - 1$ を F 係数で割り切る最小の $r-1$ は $r_{\min} - 1 = q^n - 1$ であり $r_{\min} = q^n$ であって, (i) と (ii) は $f(z)$ が原始多項式である必要条件である.

逆に n 次の $f(z) \in F[z]$ について (i), (ii) の成立を仮定する. (i) の F 既約性は F のある n 次拡大体 K, $\mathrm{ord}(K) = q^n$, が存在し, そこで $f(z)$ が根を持つ事を保証する.[58] $\mathrm{ord}(K) = q^n$ でこの K での $f(z)$ の任意の根を $a \in K^*$, $\mathrm{ord}(K^*) = q^n - 1$, と置く. a の位数を $r-1$ としよう; 当然 $r - 1 \leqq q^n - 1$ である. a は F 係数方程式 $z^{r-1} - 1 = 0$, $z^r - z = 0$ の根だから, F 既約な $f(z)$ は Lemma 5.10. により F 係数で $z^r - z$ を割り切る. (ii) によってこの r の最小値が q^n だから, $r - 1 \geqq q^n - 1$. 故に前の不等式と併せて a の位数 $r - 1 = q^n - 1$, 即ち a は K の生成元であり, a の最小多項式 $f(z)$ が原始多項式だと確定する. ■

5.5. 有限体の存在

「有限体」の舞台の上で我々は素数を中心に演じられる大変精妙な構造を見た. 目を返すと, しかし, 我々が今迄に存在を確認したのは素数 p に対する素体 $\boldsymbol{Z}_p$, そして $\boldsymbol{Z}_3$ に 2 次既約多項式 $z^2 + 1$ の根を添加した位数 $3^2 = 9$ の拡大体だけだった. だから厳格には得られた理解すべてに「もし位数有限の体 F, 或いはその拡大体 K が存在すれば」という但し書きが必要で, 結論として我々が今持つのは,

もし有限体 F とその n 次拡大体 K が存在すれば
それらは素数の標数 p を持ち,
K は F 係数の有限 n 次元ベクトル空間を作り,
位数は $\mathrm{ord}(F) = p^m$, $\mathrm{ord}(K) = (p^m)^n = p^{mn}$ に限られ,

[58] 下で詳しく述べるが, 既に §5.2 で行った様に実際には $f(z)$ の 1 根 i(があるとしてそれ) を F に添加し, 加減乗法で拡大体 K を作ればよい. $f(i) = 0$ の関係によって i^n は i^{n-1} 以下で表され, K は実体としては

$$K = \{c_0 + c_1 i + c_2 i^2 + \cdots + c_{n-1} i^{n-1} |\ c_j \in F,\ 0 \leqq j \leqq n-1\}$$

の形で F 係数 n 次元線型空間であり, 文字 i の F 係数多項式の全体 $F[i]$ という「もの」に多項式 $f(i)$ を法として, 即ち $f(i)$ の倍数はすべて 0 とみなして, 合同を定義した剰余類集合 $F[i]/f(i)$ として確かに存在する. 文字の名称 i は何でもよい, z でもよいので, 実際にはよく $K = F[z]/f(z)$ と記される.

K の乗法群 K^* は巡回群で生成元を持ち,
K^* の生成元の最小多項式として F 上の n 次既約 (原始) 多項式が存在し, $\cdots$

という事になる. この前提 (従ってすべて) を正当化し, 有限体について必要な知識を完成させよう.

劇の進行はすこしこみ入るが粗筋は簡単である. 任意の素数 p を固定し素体 $\boldsymbol{Z}_p$ の存在に基づいて, 我々は任意の自然数 m に対する位数 $q = p^m$ の有限体 F, その任意の次数の拡大体 K と F 上の n 次既約多項式の存在とを示す. それには次を得れば十分である:

補助 lemma 位数 q の有限体 A が存在すれば, 任意の自然数 n に対して A の n 次拡大体 B と A 係数の n 次既約多項式とは存在する.

実際, これが示されれば, $A = \boldsymbol{Z}_p$ とし, 任意の自然数 m を取って $\boldsymbol{Z}_p$ の m 次拡大体である位数 $q = p^m$ の体 $B = F$ の存在が保証される. そこで再びこの F を A に取り直せば, 任意の自然数 n に対して F の n 次拡大である位数 q^n の体 $B = K$ の存在と F 係数 n 次既約多項式の存在とが得られて目的は達せられる.

以下暫く, 標数 p, 位数 $q = p^m$ $(m = 1, 2, \cdots)$ の有限体 A の存在を仮定する. A の乗法群 A^* の位数が $q-1$ だから任意の $a \in A^*$ はフェルマーの小定理 $a^{q-1} = 1$ を満たし, $a = a^q$ となる. この両辺を q 乗すれば $a = a^q = (a^q)^q = a^{q^2}$ が得られ, 続けて

$$a = (a^{q^2})^q = a^{q^2 \cdot q} = a^{q^3} = \cdots = a^{q^n},$$

即ち $G(a) = a^{q^n} - a = 0$ に至る. $G(0) = 0$ も含めて, $A = \{0, a, b, \cdots, l\}$ の全ての元は多項式 $G(z) = z^{q^n} - z$ の根であり, 因数分解 $G(z) = z(z-a)(z-b)\cdots(z-l)I(z)$ が成り立つ. ここで $I(z)$ は $q^n - q$ 次 A 係数多項式である.

任意の体 K 係数多項式 $f(z) \in K[z]$ について 1 つの有名なトリック, 微分 $f'(z)$ を用いる. 多項式だからそれは次の代数的規則だけですべて計算される:

$$(z^j)' := jz^{j-1}, \quad j \geqq 0, \quad \{f(z) + g(z)\}' := f' + g', \quad (fg)' := f'g + fg'.$$

結果は勿論通常の実数や複素数上で極限操作が与えるものと変りはなく, $f'(z)$ も K 係数多項式である. 次が得られる:

Lemma 5.17. (a) 任意の体 K を係数とする多項式 $f(z) \in K[z]$ の K 内の重根は必ず $f'(z)$ の根でもある.
(b) 標数 p の任意の有限体 K の上で, 任意の正の整数 r に対する多項式 $g(z) = z^{p^r} - z$ は (それが K 内に根を持つとしても) 単根しか持てない.
(証明) (a) $z = a \in K$ が $f(z) \in K[z]$ の $j(\geqq 2)$ 重根なら, 因数定理から K 上の因数分解は $f(z) = (z-a)^j g(z)$ の形である. このとき $f'(z) = j(z-a)^{j-1}g(z) + (z-a)^j g'(z)$ となる事は通常の積の微分から明らかで, $j - 1 \geqq 1$ によって $f'(a) = 0$ も成り立つ.
(b) $g'(z) = p^r z^{p^r - 1} - 1 \equiv -1 \pmod{p}$ だから, 標数 p の体 K 内で $g'(z)$ は決して根を持てない. 故に (a) によって $g(z)$ は K 内で重根は持てない. ■

Lemma 5.17.(b) によって, 我々が存在を仮定した標数 p, 位数 $q = p^m$ の体 A 上で $G(z) = z^{q^n} - z = z^{p^{nm}} - z$ は重根を持てない. 故に $q^n - q$ 次 A 係数多項式 $I(z)$ は A には根を持てず, $I(z)$ そのものは必ずしも A 既約ではないが 2 次以上の「A 既約因数」しか含めない. その様な A 既約因数 $f(z)$ を 1 つ, 次数 $j \geqq 2$ を取り, 複素数や 5.2. 節の例に倣って「感覚的」

に言えば $f(z)=0$ の根 $z=i$ があるとしてそれを A に添加し, A の j 次拡大体 A' を作る. 実際にはこの手続きは A 係数の i の多項式の全体 $A[i]$ に法 $f(i)$ を入れたもの, $j-1$ 次以下の文字 i の A 係数多項式の全体に $f(i)$ の倍数は 0 とする規則で (法 $f(i)$ で) 四則算法を行うもの $A[i]/f(i)$ を与え, これが A' の実体である. 新しく作られた標数 p, 位数 $q^j=p^{jm}$ の体 A' で $G(z)$ を見る. 再び Lemma 5.17.(b) で $K=A'$ とすると, この標数 p の体 A' の上でも $G(z)$ は重根を持てない. だから $j<n$ なら $G(z)$ には必ず A' 既約な 2 次以上の因数が残る. この因数を 1 つ任意に取ってその根を A' に付加し, A' をさらに拡大した体を作る. この手続きは $G(z)$ が完全に 1 次因数に分解されるまで続けられる. 出来上がった標数 p の体を B' と記し, 体 B' 中の $G(z)$ の根の全体を B と置く; 位数から考えて $B'=B$ だろうが, その事は以下の議論には関係しない. B は始めに与えた体 A を含み, 次の性質を示す:

Lemma 5.18. 任意の素数 p, 自然数 m,n, $q=p^m$ に対し, 多項式 $G(z)=z^{q^n}-z$ を 1 次因数に分解する標数 p の任意有限体 B' 中で $G(z)$ の根 (単根) の全体 B は位数 q^n の有限体を作る.

(証明) Lemma 5.17.(b) によって $K=B\subset K'=B'$ でも $G(z)$ は単根しか持てない. B の任意の元 a,b を取る; $G(a)=G(b)=0$. 素数 p, 自然数 m,n に対して常に

$$(-1)^{q^n}=(-1)^{p^{mn}}\equiv -1 \pmod{p}$$

である事に注意して次を得る:

$$G(a-b)=(a-b)^{q^n}-(a-b)=a^{q^n}+(-b)^{q^n}-(a-b)=G(a)-G(b)=0.$$

即ち加法 $+$ に関する群 B' の部分集合 B は部分群の条件, $a,b\in B$ なら $a-b\in B$, を満たし群であり (Lemma 2.14.(a)), 特に $0\in B$ が成り立つ. 次に $b\in B^*:=B-\{0\}$ として次の計算をする:

$$G(ab^{-1})=(ab^{-1})^{q^n}-ab^{-1}=-a(b^{-1})^{q^n+1}(b^{q^n}-b)=-a(b^{-1})^{q^n+1}G(b)=0;$$

ここで $G(a)=0$ による $a^{q^n}=a$ を用いた. だから $a,b\in B^*$ なら $ab^{-1}\in B^*$ でもあり, B^* は乗法に関する群 $B'-\{0\}$ の部分群である. 故に B は (部分) 体で, 次数 q^n の $G(z)$ の単根の全体として位数 q^n である. ■

この様に標数 p, 位数 $q=p^m$ の体 A があれば, 任意の自然数 $n=1,2,\cdots$ に対して A を拡大して構築された $G(z)=z^{q^n}-z=0$ の根の全体である位数 q^n の有限体 B が存在する. 乗法群 B^* の既知の巡回性はその生成元の A 係数の最小多項式, A 上の n 次原始多項式, 即ち n 次 A 既約多項式, の存在も保証する. **(補助 Lemma 証明終り)**

定理 5.19. 任意の素数 p と自然数 m,n に対して, 位数 $q=p^m$ の有限体 F, その n 次拡大体 K, F 係数 n 次既約多項式, 特に F 係数 n 次原始多項式は存在する.

(証明) 再記する. 任意素数 p に対する素体 $A=\boldsymbol{Z}_p$ の存在は既知である. だから任意の自然数 m について $\boldsymbol{Z}_p$ の m 次拡大体である位数 $q=p^m$ の有限体 $B=F$ の存在が補助 lemma からわかる. その F を A として再び補助 lemma を用いると, 任意の標数 p, 位数 $q=p^m$ の有限体 F の n 次拡大である位数 q^n の体 $B=K$ と $F=A$ 係数で既約な n 次多項式, 特に乗法群 K^* の生成元の最小多項式としての F 係数 n 次原始多項式とは存在が確定する. ■

存在を上で示された標数 p, 位数 $p^m=q$ の体 F 上で, これも存在の確認された n 次既約多項式 $f(z)$ を $G(z)=z^{q^n}-z$ を 1 次因数に分解する体 K の構成に用いれば, K は実は 1 度の

拡大操作, $f(z)$ の根の添付, で得られた事がわかる. 拡大方法に関係なく, 得られた有限体は $G(z)=z^{q^n}-z$ の単根の全体だから, 位数だけで特徴付けられるものとして「位数 q^n のガロア体 $\mathrm{GF}(q^n)$」と記される. 多項式 $G(z)=z^{q^n}-z$ は Lagrange の定理を満たすものを方程式 $G(z)=0$ で選び出す篩である. $G(z)$ と F 上の n 次既約多項式, 原始多項式と限らないもの, が有限体の中で演じているさらに精妙な姿で終幕としよう. 以後, 議論の明確のために $G_r(z):=z^r-z$, $G_{p^m}(z):=z^{p^m}-z$ と書く. $\mathrm{GF}(p^m)$ の任意元 a を取ると, $G_{p^m}(a)=a^{p^m}-a=0$, 即ち $a=a^{p^m}$ であり次が成り立つ:

$$a=a^{p^m}=(a^{p^m})^{p^m}=a^{p^m\cdot p^m}=a^{p^{2m}}=(a^{p^m})^{p^{2m}}=a^{p^{3m}}=\cdots=a^{p^{nm}}.$$

即ち任意の $n=1,2,\cdots$ に対して $G_{p^m}(z)$ の根 a は $G_{p^{mn}}(z)=0$ も満たす. 故に:

Corollary 5.20. 任意の素数 p と自然数 m,n, $q=p^m$ とに対して,
(a) 多項式 $G_{q^n}(z):=z^{q^n}-z$ は多項式 $G_q(z):=z^q-z$ で $\boldsymbol{Z}_p$ 係数で整除される.
(b) $G_{q^n}(z)=z^{q^n}-z$ に含まれる $F=\mathrm{GF}(q)$ 係数既約因数の次数 d は n の約数に限る.

(証明) (a) ガロア体 $K=\mathrm{GF}(p^{mn})$ は $G_{p^{mn}}(z)$ を 1 次因数に分解する. これらの 1 次因数には上の事から多項式 $G_{p^m}(z)$ のすべての根が含まれ, $G_{p^m}(z)$ は K 係数で $G_{p^{mn}}(z)$ を割り切るが, これらは共に $\boldsymbol{Z}_p$ 係数だから整除は $\boldsymbol{Z}_p$ 係数だけで行われる.
(b) $G_{q^n}(z)=z^{q^n}-z=z^{p^{mn}}-z$ は $K=\mathrm{GF}(p^{mn})$ で 1 次因数に分解される. 当然 $G_{q^n}(z)$ の任意の $F=\mathrm{GF}(q)$ 既約因数 $f(z)$, 次数 $d\leqq n$, も同様である. この $f(z)$ の 1 つの根 $a\in K$ を $F=\mathrm{GF}(q)$ に添加すれば F の d 次拡大体 $K'=\mathrm{GF}(q^d)$ ができるが, これは $K=\mathrm{GF}(q^n)$ の部分体で K は K' のある拡大次数 $h=n/d$ の拡大体であり, h は整数である. 故に d は n の約数でなければならない. ■

定理 5.21. F は位数 q の任意の有限体とする.
(a) 多項式 $G_{q^n}(z)=z^{q^n}-z$ は n を割り切るすべての自然数 d $(1\leqq d\leqq n)$ を次数とするすべてのモニックで F 既約な多項式因数の重複を持たない (square-free な) 積に等しい.
(b) 任意の F 既約 n 次多項式 $g(z)$ は $K=\mathrm{GF}(q^n)$ で 1 次因数に分解され, その任意の 1 根を $a\in K$ として n 個の

$$a=a^{q^0},\ \ a^q=a^{q^1},\ \ a^{q^2}=(a^q)^q,\ \ \cdots,\ \ a^{q^{n-1}} \tag{5.17}$$

を根のすべて, 同位数の共役な単根, として持つ. これら $g(z)$ の共役根の単一の位数を「F 既約多項式 $g(z)$ の指数 exponent」と呼ぶ. 指数は q^n-1 の約数である.
(c) ガロア体 $K=\mathrm{GF}(q^n)$, $K'=\mathrm{GF}(q^{n'})$, $n>n'$ について K' が K の部分体であるのは n' が n を割り切る $(n'|n)$ ときでありその場合に限る.
(証明) (a) 任意の正の整数 d に対して d 次 F 既約 (でモニック) な任意の多項式 $f(z)$ はその 1 根 a を F に添加すれば F の d 次拡大体 $K'=F[z]/f(z)$ が得られ, K' は $z^{q^d}-z\in F[z]$ の根の全体で a を含む. 故に a の F 係数最小多項式である $f(z)$ は F 係数で $z^{q^d}-z$ を割り切り, 特に $d|n$ の場合 $n=dn'$ として Corollary 5.20.(a) から $f(z)$ は重根を持てない $G_{q^n}(z)=z^{q^n}-z=z^{q^{dn'}}-z$ の F 既約 1 重因数である. この整除は F 上の任意の d' 次既約多項式, 但し d' は n を割り切る, $d'|n$ である任意のもの, についても成り立ち, 体 F 係数で既約因数分解は一意だから (第 8 章定理 8.8.(b)) 命題 (a) のすべての F 既約因数の 1 重積 P は $G_{q^n}(z)$ に含まれる. 逆に Corollary 5.20.(b) によって P は $G_{q^n}(z)$ を含むから命題が従う.
(b) 任意の F 既約 n 次多項式 $g(z)$ は (a) によって根を $K=\mathrm{GF}(q^n)$ 内に持つ. その根の 1 つ

$a \in K$ に対して (5.17) の形の元が皆 $g(z)$ の同位数の (共役 conjugate な) 根である事は既に見られた. (5.17) の異なる元は多くとも $\{a = a^{q^0}, a^q = a^{q^1}, a^{q^2}, \cdots, a^{q^{n-1}}\}$ の n 個である; $a^{q^n-1} = 1$, $a^{q^n} = a$, $\cdots$ で以後の q 乗は同じ系列の繰り返しに過ぎない. $a^{q^s} = a^{q^t}$ となる整数 $0 \leqq s < t \leqq n$ を考える. 集合としては $K = F[z]/g(z)$ なのだから, K の任意元 b は F の係数 $\{d_j |\ 1 \leqq j \leqq n, (d_j)^q = d_j\}$ によって $b = d_1 a^{n-1} + d_2 a^{n-2} + \cdots + d_{n-1} a^1 + d_n a^0$ と表される. Corollary 5.11. から

$$b^q = (d_1 a^{n-1} + d_2 a^{n-2} + \cdots + d_n)^q = d_1 (a^q)^{n-1} + d_2 (a^q)^{n-2} + \cdots + d_n$$

である. だから仮定 $a^{q^s} = a^{q^t}$ は

$$b^{q^t} = d_1 (a^{q^t})^{n-1} + d_2 (a^{q^t})^{n-2} + \cdots + d_n = d_1 (a^{q^s})^{n-1} + d_2 (a^{q^s})^{n-2} + \cdots + d_n = b^{q^s}$$

を意味する; K の**すべての**元 b は $b^{q^t - q^s} = 1$ を満たし, その位数は $q^t - q^s > 0$ かその約数以下か, である. ここで $q^t - q^s \leqq q^n - 1$ だが, b を位数 $q^n - 1$ の K^* の生成元に取れば $t = n$, $s = 0$ 以外にはあり得ないと結論される. 故に (5.17) の n 個はすべて異なり, n 次で F 上既約な $g(z)$ の単根のすべてである. 指数の性質は定理 2.18.(c) による.
(c) $\mathrm{GF}(q^n)$ は $G_{q^n}(z)$ の, そして $\mathrm{GF}(q^{n'})$ は $G_{q^{n'}}(z)$ の根の全体だから (a) によって明らか.■

少し準備を要する「体係数の多項式の既約因数分解一意性」の証明は最終章に示す. 体 F, 例えば $F = \boldsymbol{Z}_p = \mathrm{GF}(p)$ の $\mathrm{GF}(p^n)$ への拡大を異なる F 既約多項式の異なる根を選んで 2 様に行い, 体 K, K' を得たとしよう. 定理 5.21.(a) で見る $G_{p^n}(z) = z^{p^n} - z$ の構造は, 任意の n 次 F 既約多項式 $f(z)$ の根がそれぞれに例えば $i \in K$ と $i' \in K'$ として含まれる事を保証する. F 係数のすべての多項式 $h(z)$ に対して対応 $\varphi(h(i)) = h(i')$ を定義すれば, φ は K と K' とを $f(i^{(\prime)})$ が定める加法, 乗法表を保って対応させる. 故に F の拡大に選ばれた既約多項式やその 1 根の選択に関係なく体 K と K' は同形で, 同形を同一視して位数 p^n の有限体, ガロア体 $\mathrm{GF}(p^n)$ は一意だと定理 5.21.(a) は端的に示している.

5.6. 演習問題

$\boldsymbol{Z}_2 = \{0, 1\}$ 上の 3 次多項式は

$$f(z) = z^3 + Az^2 + Bz + C \ \ (A, B, C \text{ は } 0 \text{ または } 1)$$

の形である. この中で $\boldsymbol{Z}_2 = \{0, 1\}$ で既約なものを考える. $f(0) = C = 0$ なら因数 z があるから既約でないと除いてよく, $\boldsymbol{Z}_2$ 既約 3 次多項式の候補は下の表の $C = 1$ のものだけになる. この中で $\boldsymbol{Z}_2$ 可約な 3 次多項式は必ず残る $\boldsymbol{Z}_2$1 次因数 $z - 1 \equiv z + 1$ を含み $f(1) \equiv 0 \pmod 2$ となる. だから $f(1) \not\equiv 0 \pmod 2$ なら $\boldsymbol{Z}_2$ 係数 1 次因数はなく既約である. 表の多項式の $z = 1$ での値を求め, 既約性○を×で記入し, 可約の場合には因数分解すれば次の様になる:

	$z = 1$ での値	既約性	因数分解
$z^3 + z^2 + z + 1$	$4 \equiv 0 \pmod 2$	×	$\equiv z^3 + 3z^2 + 3z + 1 = (z + 1)^3$
$z^3 + z^2 + 1$	$3 \not\equiv 0 \pmod 2$	○	
$z^3 + z + 1$	$3 \not\equiv 0 \pmod 2$	○	
$z^3 + 1$	$2 \equiv 0 \pmod 2$	×	$\equiv (z + 1)(z^2 \pm z + 1)$

z^2+z+1 は 2 次既約多項式である事に注意する.

$\boldsymbol{Z}_2$ の 3 次拡大体 $K=\mathrm{GF}(8)$ は存在する. その乗法群 K^* は $8-1=7$ の素数個の元からなるから,[59] 1 以外の K^* の元 6 個はすべて生成元で位数 7, これらの最小 (既約) 多項式は原始多項式で 3 次でなければならない. だから上の 2 つの $\boldsymbol{Z}_2$ 既約 3 次多項式は共に原始多項式である.

問題 5.22. (a) 3 次の $\boldsymbol{Z}_2$ 既約 (原始) 多項式 $f(z)=z^3+z+1$ の根 i と $\boldsymbol{Z}_2$ の数の四則演算 $+-\times\div$ で作られる数は, i の 3 次以上の式は全部 $i^0=1,\ i^1=i,\ i^2$ だけで作られる 2 次以下の式に置きなおせる. だから $\boldsymbol{Z}_2$ と i の四則算法でつくられる数 (「複素数」) は

$$(a,b,c):=ai^0+bi^1+ci^2;\ \ a,b,c \text{ は } 0 \text{ または } 1,$$

の形のものがすべてで, 次の $2^3=8$ 個である:

$$(0,0,0):=0+0i+0i^2=0, \qquad (1,0,0):=1+0i+0i^2=1,$$
$$(0,1,0):=0+1i+0i^2=i, \qquad (0,0,1):=0+0i+1i^2=i^2,$$
$$(1,1,0):=1+1i+0i^2=1+i, \qquad (1,0,1):=1+0i+1i^2=1+i^2,$$
$$(0,1,1):=0+1i+1i^2=i+i^2, \qquad (1,1,1):=1+1i+1i^2=1+i+i^2.$$

この全体を K, K から 0 を除いたものを $K^*:=K-\{0\}$ と書く. i の冪乗を計算し, K^* の数の i の冪での表現 (巡回表現) を下の表の第 2 行に記入し, これを用いて K^* の乗積表を完成しなさい.

(b) また, 同じ表から各元の冪乗表をつくり, 1 以外が生成元である事を確認しなさい.

(c) $\boldsymbol{Z}_2$ 既約 3 次多項式 $f(z)=z^3+z+1$ の K での因数分解を求めなさい. またもう 1 つの $\boldsymbol{Z}_2$ 既約 3 次多項式 $g(z)=z^3+z^2+1$ の因数分解も求めなさい.

(解) (a) $f(i)=0$ より

$$i^3=1+i,\quad i^4=i+i^2,\quad i^5=i^2+i^3=1+i+i^2,$$
$$i^6=i+i^2+i^3=1+i^2,\quad i^7=i+i^3=i+1+i\equiv 1.$$

積 ab の表は, 巡回表現から指数法則 $i^s\cdot i^t=i^{s+t}$ で簡単に計算できる.

$a\backslash b$	1	i	i^2	$1+i$	$1+i^2$	$i+i^2$	$1+i+i^2$
	i^7	i^1	i^2	i^3	i^6	i^4	i^5
1	1	i	i^2	$1+i$	$1+i^2$	$i+i^2$	$1+i+i^2$
i	i	i^2	$i^3=1+i$	$i+i^2$	1	$1+i+i^2$	$1+i^2$
i^2	i^2	$1+i$	$i+i^2$	$1+i+i^2$	i	$1+i^2$	1
$1+i$	$1+i$	$i+i^2$	$1+i+i^2$	$1+i^2$	i^2	1	i
$1+i^2$	$1+i^2$	1	i	i^2	$1+i+i^2$	$1+i$	$i+i^2$
$i+i^2$	$i+i^2$	$1+i+i^2$	$1+i^2$	1	$1+i$	i	i^2
$1+i+i^2$	$1+i+i^2$	$1+i^2$	1	i	$i+i^2$	i^2	$1+i$
逆数	1	$1+i^2$	$1+i+i^2$	$i+i^2$	i	$1+i$	i^2

(b) 指数法則 $(i^s)^t=i^{st}$, ラグランジュの定理 $i^7=1$, $i^{s+7}=i^s$ を繰返して使えば簡単である. 結果は次の通り:

[59] 素数 $7=2^3-1$ はメルセンヌ Mersenne 数, 3 はメルセンヌ指数 Mersenne exponent である.

a^1	a^2	a^3	a^4	a^5	a^6	a^7	生成元
1	1	1	1	1	1	1	$\times$
i	i^2	$i^3=1+i$	$i+i^2$	$1+i+i^2$	$1+i^2$	1	○
i^2	$i+i^2$	$1+i^2$	i	$1+i$	$1+i+i^2$	1	○
$1+i$	$1+i^2$	i^2	$1+i+i^2$	i	$i+i^2$	1	○
$1+i^2$	$1+i+i^2$	$i+i^2$	$1+i$	i^2	i	1	○
$i+i^2$	i	$1+i+i^2$	i^2	$1+i^2$	$1+i$	1	○
$1+i+i^2$	$1+i$	i	$1+i^2$	$i+i^2$	i^2	1	○

確かに, 1 以外のすべての数は生成元である.

(c) $\boldsymbol{Z}_2=\mathrm{GF}(2)$ 上の 3 次既約多項式 $f(z)=z^3+z+1$ の根 i に対して, i^2, $i^{2^2}=i^4$ も共役な根で, $K=\mathrm{GF}(8)$ 係数の因数分解

$$f(z)=z^3+z+1=(z-i)(z-i^2)(z-i^4)=(z-i)(z-i^2)(z-i+i^2)$$

が成り立つ. 残るもう 1 つの $\boldsymbol{Z}_2$ 上の 3 次既約多項式 $g(z)$ は $\mathrm{GF}(8)^*$ の残る i^3 とその 2 乗の繰り返し

$$i^3=1+i,\ \ (i^3)^2=i^6=1+i^2,\ \ (i^3)^{2^2}=i^{12}=i^5=1+i+i^2$$

を根に持つから,

$$\begin{aligned}g(z)&=z^3+z^2+1=(z-1-i)(z-1-i^2)(z-i-i^2)\\&=(z+1+i)(z+1+i^2)(z+i+i^2).\end{aligned}$$

これが K での因数分解である. **(問題 5.22. 終り)**

問題 5.23. 問題 5.22. で得た $\boldsymbol{Z}_2$ の 3 次拡大体 $K=\mathrm{GF}(8)$ の中では, 3 次 $\boldsymbol{Z}_2$ 既約多項式 $f(z)=$
z^3+z+1 の根 $i\neq 0$ はまた多項式,

$$G(z)=z^8-z=z(z-1)H(z)=0,$$

$$H(z):=z^6+z^5+z^4+z^3+z^2+z+1$$

の根でもある. 故に $H(z)$ は i の最小多項式である $f(z)=z^3+z+1$ で $\boldsymbol{Z}_2$ 係数で整除される. この割り算を行い, $G(z)$ の $\boldsymbol{Z}_2$ 既約因数への完全な分解を完成せよ.

(解) 割り算は次の様になる:

$$\begin{array}{rl}
 & z^3+z^2\qquad +1\\
\hline
z^3+z+1 & \big)\ z^6+z^5+z^4+z^3+z^2+z+1\\
 & \underline{z^6\qquad +z^4+z^3\qquad\qquad}\\
 & \quad z^5\qquad\qquad +z^2+z+1\\
 & \quad \underline{z^5\qquad +z^3+z^2\qquad}\\
 & \qquad\qquad z^3\qquad +z+1\\
 & \qquad\qquad \underline{z^3\qquad +z+1}\\
 & \qquad\qquad\qquad 0
\end{array}$$

故に $\boldsymbol{Z}_2$ での $G(z)$ の既約因数分解は

$$G(z) = z(z+1)(z^3+z+1)(z^3+z^2+1).$$

この様に, 拡大次数 3 を割り切る次数, 3 次と 1 次, のすべての $\boldsymbol{Z}_2$ 既約な多項式

$$z^3+z^2+1,\ \ z^3+z+1,\ \ z-1,\ \ z$$

は $G(z)$ の中に含まれ, z^3+z^2+1, 或いは z^3+z+1 を 0 とする根はこの $K=\mathrm{GF}(8)$ の中で求められる. しかし $\boldsymbol{Z}_2$ 上の 3 次可約なものうち $z^3+1=(z+1)(z^2+z+1)=0$ は K でなくガロア体 $\mathrm{GF}(2^2)$ 等をその完全な分解に必要とする. **(問題 5.23. 終り)**

5.7. BCH(Bose-Chaudhuri-Hocquenghem) 符号

有名な Bose-Chaudhuri-Hocquenghem 符号の基本事項は有限体の知識のストレートな応用である. 是非この段階で触れておこう. コンピュータ内やコンピュータ間等のデータの送受は普通 $\boldsymbol{Z}_2$ の元 $0,1$, 一般には $\boldsymbol{Z}_p$ や有限体 $\mathrm{GF}(p^n)$ の元でも構わないので以下そうする, の j 連 $x_0x_1x_2\cdots x_{j-1}$ を 1 区切り, 「語」とし, それを送受での誤りが入った場合のその検出や訂正や, を目指した余剰情報を添えた k 連, $k>j$, の符号 (code)$y_0y_1y_2\cdots y_{k-1}$ に変換 (符号化 encode) して送る. 受信側は変換の規則に従い, 得られた符号からもとの語を復元 (復号 decode) する.

よく行われるのは語も符号もある文字 z の $\boldsymbol{Z}_p$ 係数多項式と考え直す多項式符号 polynomial code の場合で,

(1) 語 $x_0x_1x_2\cdots x_{j-1}$ を $\boldsymbol{Z}_p$ 係数で $j-1$ 次以下の次の多項式に対応させる:

$$f(z) = x_0z^0 + x_1z^1 + x_2z^2 + \cdots + x_{j-1}z^{j-1}$$

(2) ある r 次符号化多項式 encoding polynomial

$$e(z) = c_0z^0 + c_1z^1 + c_2z^2 + \cdots + c_rz^r,\ \ c_i \in \boldsymbol{Z}_p,\ \ 1 \leqq i \leqq r,$$

を取り,

(3) その符号は $k=j+r$ と置いて $\boldsymbol{Z}_p$ 係数多項式としての積

$$F(z) = e(z)f(z) = y_0z^0 + y_1z^1 + y_2z^2 + \cdots + y_{k-1}z^{k-1}$$

に対応する $y_0y_1y_2\cdots y_{k-1}$ に取る. $F(z)$ の係数が送信される符号である.

もとの語の全体は

$$\{x_0x_1x_2\cdots x_{j-1} |\ x_i \in \boldsymbol{Z}_p, 0 \leqq i \leqq j-1\}$$

だが, これらに対応する多項式語は $\boldsymbol{Z}_p$ 係数の高々 $j-1$ 次多項式の全体

$$W = \{f(z) = x_0z^0 + x_1z^1 + \cdots + x_{j-1}z^{j-1} |\ x_0, x_1, \cdots, x_{j-1} \in \boldsymbol{Z}_p\}$$

を作る; 語は実用では $x_0 \neq 0,\ x_{j-1} \neq 0$ と制限する (多項式語 $f(z)$ が必ず $j-1$ 次になり, 定数項を持つ様にする) が, ここではそれを考えない. 多項式符号 $F(z)$ の全体は高々 $k-1$ 次の z の多項式, 但しその全部ではなくて因数 $e(z)$ を含むもの, $e(z)$ で割り切れるものの全体,

$$C_e = \{F(z) = f(z)e(z) |\ f(z) \in W\}$$

に限定され特徴付けられる. もとの多項式語の全体 W は $\boldsymbol{Z}_p$ 係数線形空間である:

$$f(z), g(z) \in W \text{ なら任意定数 } \alpha, \beta \in \boldsymbol{Z}_p \text{ に対して } h(z) = \alpha f(z) + \beta g(z) \in W.$$

即ち $h(z) = \alpha f(z) + \beta g(z)$ も高々 $j-1$ 次である. 勿論 $\alpha f(z) + \beta g(z)$ の係数の計算は $\boldsymbol{Z}_p$ での加法で行う.

Lemma 5.24. $\boldsymbol{Z}_p$ 係数線形空間であるという性質は多項式符号の全体 C_e でも保たれる.

(証明) $F(z) = f(z)e(z) \in C_e,\ G(z) = g(z)e(z) \in C_e$ であれば, $h(z) := \alpha f(z) + \beta g(z) \in W$ だから,

$$aF(z) + bG(z) = \{\alpha f(z) + \beta g(z)\}e(z) = h(z)e(z) \in C_e, \quad \forall \alpha, \beta \in \boldsymbol{Z}_p. \qquad \blacksquare$$

受け取った多項式符号 $F(z)$ から多項式語 $f(z)$ を復元するには $f(z) = \dfrac{F(z)}{e(z)}$ の割り算をすればよい. 受信符号での誤りの有無は $F(z) \in C_e$ が成り立つか, 即ち $e(z)$ で $\boldsymbol{Z}_p$ 係数で割り切れるかどうかで判断できる; C_e に属す符号を受け取った時は誤りではないと考えるのである. 次の定義を置く:

定義 5.25. 多項式符号 $F(z) \in C_e - \{0\}$ の持つ 0 でない係数の個数の $C_e - \{0\}$ での最小値 d を符号 C_e の最小ハミング Hamming 距離という. **(定義 5.25. 終り)**

誤りを検出する立場からは, 上で定められる d が符号体系 C_e の誤り検出能力を規定する. 実際任意の異なる符号 $F(z), G(z) \in C_e$ に対しては, 差の多項式 $F(z) - G(z)$ は 0 ではない多項式符号だから, 少なくとも d 個の係数が 0 ではない, 言い換えると $F(z)$ と $G(z)$ は少なくとも d 個の係数で異なり, 途中で d 個以上の誤りが入らない限り同じものと間違える事はない. 誤りが入り多項式符号ではない $F^\sharp(z)$ を受け取った時には, それを最も係数の違いの数が小さい (ハミング Hamming 距離で最も近い) 多項式符号 $F(z) \in C_e$ に訂正する. 正しくない符号の数 s が $d/2$ より小さい場合にはこの訂正は可能であり成功する; 実際 $F^\sharp(z)$ の係数をこの s 個, $s < d/2$, 変えれば正しい符号多項式 $F(z) \in C_e$ が得られるが, $F^\sharp(z)$ から他の任意の符号多項式 $G(z)$ への訂正で変えるべき係数の数を s' とすると, $F(z)$ から $G(z)$ へは係数高々 $s + s'$ 個の変更で達するのだから最小ハミング距離 d の定義から

$$d \leqq \{F(z) \text{ と } G(z) \text{ の係数の異なる数}\} \leqq s + s', \quad s' \geqq d - s > d - d/2 = d/2 > s,$$

が満たされ, 最小の訂正が正しい符号を一意に与えるのである.

再度まとめれば最小ハミング距離 d の多項式符号では d 個未満の誤りは必ず検出可能で $d/2$ 個未満の誤りは必ず訂正可能である.

この様に多項式符号の全体 C_e の最小ハミング距離 d は大切な特性で, 符号化多項式 $e(z)$ にはなるべく大きな d を保証するものを選びたい. $e(z)$ の取り方の 1 つが BCH 符号で, それは次の定理が示す原理に基づいている.

定理 5.26. p は素数, a は有限体 $K = \mathrm{GF}(p^n)$ の乗法群 K^* の生成元とし, $\boldsymbol{Z}_p$ 係数の多項式で a^i を根に持つ最小次数のもの (最小多項式) を $m_i(z)$ と書く. $d \leqq p^n - 1$ となる任意の正の整数 d を取り, $a^1, a^2, a^3, \cdots, a^{d-1}$ のこれら最小多項式の中の異なるものの積を

$$e(z) \equiv \mathrm{LCM}\{m_1(z), m_2(z), \cdots, m_{d-1}(z)\}$$

と置くと:

(a) $e(z)$ の次数 $r < p^n - 1$ である.
(b) 次数 $j \leqq p^n - 1 - r$ である任意の $\boldsymbol{Z}_p$ 係数 j 次多項式 $f(z) \neq 0$, 即ち $F(z) \equiv f(z)e(z)$ の次数 $r + j - 1 < p^n - 1$ となる任意の $\boldsymbol{Z}_p$ 係数 j 次多項式語 $f(z) \neq 0$, について, $e(z)$ を符号化多項式とする多項式符号 $F(z) \equiv f(z)e(z)$ は必ず d 個以上の 0 でない係数を持つ.

$e(z)$ を「最小距離 d の BCH 符号化多項式」と言う.

(証明) (a) 元 a は K^* の原始元で位数 $p^n - 1$, $d - 1 \leqq p^n - 2$ だから $a, a^2, a^3, \cdots, a^{d-1}$ には同一のものはなく, $a^{p^n-1} = 1$ を含まず, またすべて方程式

$$z^{p^n-1} = 1, \text{即ち } z^{p^n-1} - 1 = 0$$

を満たす. 明らかな因数分解

$$z^{p^n-1} - 1 = (z-1)I(z), \quad I(z) = z^{p^n-2} + z^{p^n-3} + \cdots + z^2 + z + 1,$$

によれば $a^1, a^2, a^3, \cdots, a^{d-1}$ は $I(z) = 0$ の解で, これらの数の最小多項式 $m_1(z), m_2(z), \cdots, m_{d-1}(z)$ はどれも $I(z)$ を割り切る. 故に $I(z)$ は $m_1(z), m_2(z), \cdots, m_{d-1}(z)$ の倍数になっていて上の最小公倍数 $e(z)$ によって割り切られる. これは

$$\text{「}e(z) \text{ の次数 } r\text{」} \leqq \text{「}I(z) \text{ の次数 } p^n - 2\text{」} < p^n - 1$$

を証明する.

(b) $f(z) \neq 0$ から $F(z) = f(z)e(z)$ は法 p で 0 ではない係数を必ず持つ. その様な係数の個数を m 個として, $j + r \leqq p^n - 1$, $j + r - 1 \leqq p^n - 2$ から,

$$F(z) = f(z)e(z) = c_1 z^{i_1} + c_2 z^{i_2} + \cdots + c_{m-1} z^{i_{m-1}} + c_m z^{i_m},$$
$$0 \leqq i_1 < i_2 < \cdots < i_{m-1} < i_m \leqq p^n - 2 \tag{5.18}$$

と置ける. $e(z)$ の根 $a^1, a^2, a^3, \cdots, a^{d-1}$ は $F(z) = f(z)e(z)$ の根でもあるから

$$\begin{aligned}
F(a^1) &= 0 = c_1 a^{i_1} + c_2 a^{i_2} + \cdots + c_m a^{i_m} \\
F(a^2) &= 0 = c_1 (a^2)^{i_1} + c_2 (a^2)^{i_2} + \cdots + c_m (a^2)^{i_m} \\
F(a^3) &= 0 = c_1 (a^3)^{i_1} + c_2 (a^3)^{i_2} + \cdots + c_m (a^3)^{i_m} \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
F(a^{d-1}) &= 0 = c_1 (a^{d-1})^{i_1} + c_2 (a^{d-1})^{i_2} + \cdots + c_m (a^{d-1})^{i_m}
\end{aligned}$$

即ち同次方程式

$$\begin{aligned}
0 &= c_1 (a^{i_1})^1 + c_2 (a^{i_2})^1 + \cdots + c_m (a^{i_m})^1 \\
0 &= c_1 (a^{i_1})^2 + c_2 (a^{i_2})^2 + \cdots + c_m (a^{i_m})^2 \\
0 &= c_1 (a^{i_1})^3 + c_2 (a^{i_2})^3 + \cdots + c_m (a^{i_m})^3 \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
0 &= c_1 (a^{i_1})^{d-1} + c_2 (a^{i_2})^{d-1} + \cdots + c_m (a^{i_m})^{d-1}
\end{aligned}$$

が成り立つ. $b_1 = a^{i_1}, b_2 = a^{i_2}, \cdots, b_m = a^{i_m}$ と置けば, a は位数 $q = p^n - 1$ だから (5.18) によって $\{b_1, b_2, \cdots, b_m\}$ は有限体 K の 0 以外の元であり, $i_m \leqq p^n - 2$ によってすべて異なる. 故に $d_j := c_j a^{i_j} \neq 0$ とさらに置けば, 上は 0 ではない $\{d_1, d_2, \cdots, d_m\}$ に対して成立する $d - 1$ 個の m 元連立同次 1 次方程式

$$
\begin{aligned}
0 &= d_1(b_1)^0 + d_2(b_2)^0 + \cdots + d_m(b_m)^0 \\
0 &= d_1(b_1)^1 + d_2(b_2)^1 + \cdots + d_m(b_m)^1 \\
0 &= d_1(b_1)^2 + d_2(b_2)^2 + \cdots + d_m(b_m)^2 \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
0 &= d_1(b_1)^{d-2} + d_2(b_2)^{d-2} + \cdots + d_m(b_m)^{d-2}
\end{aligned}
$$

である事が見える. $m \leqq d-1$ と仮定すれば, この始めの m 個を取る事ができ, その係数行列式は 0 ではない Vandermonde 行列式になる:

$$
D = \begin{vmatrix}
{b_1}^0 & {b_2}^0 & \cdots & {b_m}^0 \\
{b_1}^1 & {b_2}^1 & \cdots & {b_m}^1 \\
{b_1}^2 & {b_2}^2 & \cdots & {b_m}^2 \\
\cdots & \cdots & \cdots & \cdots \\
{b_1}^{m-1} & {b_2}^{m-1} & \cdots & {b_m}^{m-1}
\end{vmatrix}
$$

$$
\begin{aligned}
&= (b_2-b_1)(b_3-b_1)(b_4-b_1)\cdots\cdots\cdots\cdots(b_m-b_1) \\
&\qquad \times (b_3-b_2)(b_4-b_2)\cdots\cdots\cdots\cdots(b_m-b_2) \\
&\qquad\qquad \times (b_4-b_3)\cdots\cdots\cdots\cdots(b_m-b_3) \\
&\qquad\qquad\qquad \times\cdots\cdots\cdots\cdots\cdots\cdots \\
&\qquad\qquad\qquad\qquad \times(b_m-b_{m-1}) \\
&\not\equiv 0 \pmod{p}.
\end{aligned}
$$

故に $\{d_1, d_2, \cdots, d_m\}$ はすべて 0 となり, 矛盾である. これは仮定 $m \leqq d-1$ 即ち $m < d$ の成立はあり得ず, $m \geqq d$ で なければならない事を証明する. ■

勿論余り大きい d では多項式語 $f(z)$ の係数の個数 (通信語の長さ) $j \leqq p^n - 1 - d$ が大きく取れず通信の効率が下がる. これらの事項全般については, 文献 [37),38),39)] を参照せよ.

問題 5.27. $\boldsymbol{Z}_3 = \{0, 1, 2 \equiv -1\}$ 上の 3 次多項式 $g(z) = z^3 - z^2 + 1$ を考える. 3 次の $g(z)$ がもし $\boldsymbol{Z}_3$ で可約なら, 2 次と 1 次因数の積か或いは 1 次因数 3 個の積の筈で, いずれにせよ必ず $\boldsymbol{Z}_3$ の数 $a = 0, 1, 2 \equiv -1$ のどれかの 1 次因数 $z - a$ がある. しかし $g(0) = g(1) = 1$, また $g(-1) = -1$ ですべて 0 にはならないからこの様な 1 次因数は存在せず $g(z)$ は $\boldsymbol{Z}_3$ で既約である. $g(z) = 0$ の根 b は $\boldsymbol{Z}_3$ の 3 次拡大体 $K = \mathrm{GF}(3^3) = \mathrm{GF}(27)$ の数, $\boldsymbol{Z}_3$ から見て「虚数」である. この根 $b \in K^*$ での冪乗 $\{b^k | \ k = 1, 2, \cdots\}$ をすべて b^0,b^1 と b^2 だけで表して求め, $g(z)$ が $\boldsymbol{Z}_3$ 上の 3 次原始多項式である事を示しなさい.

(解) $g(b) = b^3 - b^2 + 1 \equiv 0$ なのだから $b^3 \equiv b^2 - 1$. これから続けて, すべてを $b^0 = 1$, $b^1 = b$, b^2 だけで表すと

$$
\begin{aligned}
b^4 &= b \cdot b^3 = b(b^2-1) = b^3 - b = (b^2-1) - b = b^2 - b - 1, \\
b^5 &= b(b^2 - b - 1) = b^3 - b^2 - b \equiv (b^2-1) - b^2 - b = -b - 1, \\
b^6 &= -b^2 - b, \\
b^7 &= -(b^2-1) - b^2 = b^2 + 1,
\end{aligned}
$$

$$b^8 = (b^2-1)+b = b^2+b-1,$$
$$b^9 = (b^2-1)+b^2-b = -b^2-b-1,$$
$$b^{10} = -(b^2-1)-b^2-b = b^2-b+1,$$
$$b^{11} = (b^2-1)-b^2+b = b-1,$$
$$b^{12} = b^2-b,$$
$$b^{13} = (b^2-1)-b^2 = -1.$$

これから以後は計算しなくても今までの結果から $b^{13+k} = -b^k$ と得られて,

$$b^{14} = -b,$$
$$b^{15} = -b^2,$$
$$b^{16} = -b^3 = -b^2+1,$$
$$b^{17} = -b^2+b+1,$$
$$b^{18} = b+1,$$
$$b^{19} = b^2+b,$$
$$b^{20} = -b^2-1,$$
$$b^{21} = -b^2-b+1,$$
$$b^{22} = b^2+b+1,$$
$$b^{23} = -b^2+b-1,$$
$$b^{24} = -b+1,$$
$$b^{25} = -b^2+b,$$
$$b^{26} = 1.$$

$\mathrm{ord}(b) = 26 = 3^3-1$, $g(z)$ は $\boldsymbol{Z}_3$ 上の 3 次原始多項式である. **(問題 5.27. 終り)**

問題 5.28. $\boldsymbol{Z}_3$ 上の $n=3$ 次原始多項式 $g(z) = z^3-z^2+1$ に基づいて最小ハミング距離 $d=7$ の BCH 符号化多項式 $e(z)$ を求めなさい.

(解) $d = 7 < p^n-1 = 3^3-1 = 26$ が成り立つから次の手順となる.

(i) まず $g(z)=0$ の $\mathrm{GF}(p^n) = \mathrm{GF}(27)$ の解 $z=b$ を取り, $b,\ b^2,\ b^3, \cdots, b^{d-1} = b^6$ の最小多項式 $g_1(z) = g(z),\ g_2(z),\ g_3(z),\ \cdots,\ g_{d-1}(z) = g_6(z)$ を求める.

(ii) 符号化多項式 $e(z)$ として $\{g_1(z),\ g_2(z),\ g_3(z),\ \cdots,\ g_{d-1}(z) = g_6(z)\}$ の $\boldsymbol{Z}_p = \boldsymbol{Z}_3$ の意味での最小公倍数

$$e(z) = \mathrm{LCM}\{g_1(z),\ g_2(z),\ g_3(z),\ \cdots,\ g_{d-1}(z) = g_6(z)\}$$

を算出する. $\{g_1(z),\ g_2(z),\ g_3(z),\ \cdots,\ g_{d-1}(z) = g_6(z)\}$ は皆 $\boldsymbol{Z}_3$ 既約だから, この中で異なるものだけを掛け合せて $e(z)$ を作ればよい.

$\mathrm{GF}(3^3)$ は $\mathrm{GF}(3) = \boldsymbol{Z}_3$ の 3 次拡大で拡大次数 3 の約数は 1 と 3 だけだから, その元は $\boldsymbol{Z}_3$ 係数の 1 又は 3 次の既約 (最小) 多項式の根のはず, 上の $b, b^2, \cdots, b^6$ に $\boldsymbol{Z}_3$ の数 $0,\ \pm 1$ はないか

ら $g_k(z)$ はすべて $\boldsymbol{Z}_3$ 上の 3 次既約多項式である. 根 α, β, γ を持つ 3 次多項式では

$$(z-\alpha)(z-\beta)(z-\gamma) = z^3 - (\alpha+\beta+\gamma)z^2 + (\alpha\beta+\beta\gamma+\gamma\alpha)z - \alpha\beta\gamma$$

の形の解と係数の関係があり, $\boldsymbol{Z}_3$ 上の既約多項式はすべてその 1 根 c と共に $c^p = c^3,\ (c^p)^p = c^{3^2} = c^9,\ \cdots$ もその根とする. 故に問題 5.27. の b の冪乗の結果を以下の様に用いる事ができる.

(1) $g_1(z) = g(z) = z^3 - z^2 + 1$.

(2) b^2 の最小多項式, つまり b^2 を根とする $\boldsymbol{Z}_3$ 係数既約多項式 $g_2(z)$ は b^2 の他に $(b^2)^3 = b^6$, $(b^6)^3 = b^{18}$ も根に持たなければならない. その次の $(b^{18})^3 = b^{54} = b^{26\times 2+2} = b^2$ から先は考えなくてよい. だから

$$\begin{aligned} g_2(z) &= (z-b^2)(z-b^6)(z-b^{18}) \\ &= z^3 - (b^2+b^6+b^{18})z^2 + (b^8+b^{24}+b^{20})z - b^{26} \\ &= z^3 - \{b^2 + (-b^2-b) + (b+1)\}z^2 \\ &\qquad\qquad +\{(b^2+b-1) + (-b+1) + (-b^2-1)\}z - 1 \\ &= z^3 - z^2 - z - 1. \end{aligned}$$

(3) $g(z)$ はその根 b と共に b^3 も根として含むから $g_3(z) = g(z)$ である.

(4) b^4 の最小多項式 $g_4(z)$ は $(b^4)^3 = b^{12},\ (b^{12})^3 = b^{36} = b^{10},\ (b^{10})^3 = b^{30} = b^4$ によって

$$\begin{aligned} g_4(z) &= z^3 - (b^4+b^{12}+b^{10})z^2 + (b^{16}+b^{22}+b^{14})z - b^{26} \\ &= z^3 - \{(b^2-b-1) + (b^2-b) + (b^2-b+1)\}z^2 \\ &\qquad\qquad +\{(-b^2+1) + (b^2+b+1) + (-b)\}z - 1 \\ &= z^3 - z - 1. \end{aligned}$$

(5) b^5 の最小多項式 $g_5(z)$ は $(b^5)^3 = b^{15}$, $(b^{15})^3 = b^{45} = b^{19}$, $(b^{19})^3 = b^{57} = b^5$ だから,

$$\begin{aligned} g_5(z) &= z^3 - (b^5+b^{15}+b^{19})z^2 + (b^{20}+b^{34}+b^{24})z - b^{39} \\ &= z^3 - (b^5+b^{15}+b^{19})z^2 + (b^{20}+b^8+b^{24})z - b^{13} \\ &= z^3 - \{(-b-1) + (-b^2) + (b^2+b)\}z^2 \\ &\qquad\qquad +\{(-b^2-1) + (b^2+b-1) + (-b+1)\}z + 1 \\ &= z^3 + z^2 - z + 1. \end{aligned}$$

(6) b^6 の最小多項式 $g_6(z)$ は $(b^6)^3 = b^{18}$, $(b^{18})^3 = b^{54} = b^2$ だから, $g_6(z) = g_2(z)$ である. 故に $\boldsymbol{Z}_3$ 上の 3 次原始多項式 $g(z)$ に基づく最小ハミング距離 $d = 7$ の符号化多項式 $e(z)$ は異なる 4 個の既約多項式

$$\begin{aligned} &g_1(z) = g(z) = z^3 - z^2 + 1 = g_3(z), \quad g_2(z) = z^3 - z^2 - z - 1 = g_6(z), \\ &g_4(z) = z^3 - z - 1, \qquad\qquad g_5(z) = z^3 + z^2 - z + 1 \end{aligned}$$

の積であり,

$$e(z) = (z^3 - z^2 + 1)(z^3 - z^2 - z - 1)(z^3 - z - 1)(z^3 + z^2 - z + 1)$$

$$= z^{12} - z^{11} - z^{10} + z^9 - z^6 + z + 1.$$ **(問題 5.28. 終り)**

6. 線形漸化式の最長周期とM系列乱数

6.1. 線形漸化式の解の周期

群の知識が乗算合同法乱数の構造を明らかにした様に, 有限体の知識は任意の有限体, $F = \mathrm{GF}(q)$, の上で定義された n 次線形漸化式

$$x_k = b_1 x_{k-1} + b_2 x_{k-2} + \cdots + b_n x_{k-n}, \quad b_k \in F, \quad b_n \neq 0 \tag{6.1}$$

とその解に対して多くの見通しを与える. この特性多項式 (決定多項式)$\in F[z]$ は

$$f(z) = z^n - b_1 z^{n-1} - b_2 z^{n-2} - \cdots - b_{n-1} z^1 - b_n \tag{6.2}$$

である. 応用上は $f(z)$ が F 上の n 次既約多項式となる場合に最も興味がある. この時方程式 $f(z) = 0$ は F の n 次拡大体 $\mathrm{GF}(q^n) =: K$ の乗法群 K^* の元である同位数の互いに共役 conjugate な単根, すべて異なる n 個の根, の 1 組

$$\{a_1 =: a,\ a_2 = a^q,\ a_3 = a^{q^2},\ \cdots,\ a_n = a^{q^{n-1}}\} \tag{6.3}$$

を持つ. 共役根の全部に共通の位数 h (h は $q^n - 1$ を割り切る, $h | q^n - 1$) は F 既約多項式 $f(z)$ の指数 exponent と呼ばれた. 特に $f(z)$ として F 上の n 次原始多項式を取る事も常に可能で, その指数或いは根の位数は構造上限界の $q^n - 1$ である. 原始多項式というものの存在はもはや K^* の巡回性, 生成元の存在からの真っ直ぐな帰結で, 理屈上は神秘的でも不思議でもないと認識はされる. しかし依然としてこれは驚くべき意味を持つ.

乗算合同法のスペクトル検定で導入した様に, 漸化式 (6.1) の解系列の相続く n 個の組,[60]

$$\boldsymbol{x}_k := {}^t(x_k, x_{k+1}, x_{k+2}, \cdots, x_{k+n-1}) \tag{6.4}$$

を「n 連」と呼び, 0 ばかりの n 連は「0 連」と名付ける. 次の視界が広がる:

定理 6.1. (a) 有限体 $F = \mathrm{GF}(q)$ 上の n 次既約多項式 $f(z)$ が (6.2) で与えられ, その指数が h ($h | q^n - 1$) であるとする. 線形漸化式 (6.1) の解系列 $\{x_k |\ k = 0, 1, 2, \cdots\}$ は

$$x_k = c_1 {a_1}^k + c_2 {a_2}^k + \cdots + c_n {a_n}^k, \quad k = 0,\ 1,\ 2,\ \cdots \tag{6.5}$$

と $K = \mathrm{GF}(q^n)$ の係数 $\{c_1, c_2, \cdots, c_n\}$ で表現される. 0 連を除く K 内の任意の出発 n 連 $\boldsymbol{x}_0$,

$$\boldsymbol{x}_0 := {}^t(x_0, x_1, x_2, \cdots, x_{n-1}),\ \ 1 \leqq k \leqq n \text{ で } x_k \in K, \tag{6.6}$$

に対してこの解系列の周期は同一の h である. 特に $f(z)$ が n 次原始多項式なら, 周期 h は理論的最長の $T = q^n - 1$ である.

(b) 出発の n 連を F 内に取れば, 系列 $\{x_k\}$ は常に F 内を動き, 展開 (6.5) の係数 $\{c_1, c_2, \cdots\}$ に 0 のものは存在しない. この場合を特に「F 上の n 次最大周期列, F 上の最長周期列 maximum length sequence, F 上の M 系列」と呼ぶ.

(証明) (a) 解系列の表現 (6.5) の成立は第 5 章冒頭の実数, 複素数上での議論でそのまま成り立つ. この再現は省き, (6.5) が出発 n 連 $\boldsymbol{x}_0 = {}^t(x_0, x_1, \cdots, x_{n-1})$ を持つ式を再記しよう. こ

[60] 再び, 縦 (列) ベクトルを太文字で表す約束を確認する. 故にその転置 transpose ${}^t\boldsymbol{x}$ は横 (行) ベクトル, 横 (行) ベクトルの転置は縦 (列) ベクトルである.

れは係数 $\{c_1, c_2, \cdots, c_n\}$ の n 元連立 1 次方程式

$$\boldsymbol{x}_0 = \begin{pmatrix} x_0 \\ x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} c_1{a_1}^0 + c_2{a_2}^0 + \cdots + c_n{a_n}^0 \\ c_1{a_1}^1 + c_2{a_2}^1 + \cdots + c_n{a_n}^1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ c_1{a_1}^{n-1} + c_2{a_2}^{n-1} + \cdots + c_n{a_n}^{n-1} \end{pmatrix} = V \begin{pmatrix} c_1 \\ c_2 \\ \cdot \\ \cdot \\ \cdot \\ c_n \end{pmatrix},$$

$$V = \begin{pmatrix} {a_1}^0 & {a_2}^0 & \cdots & {a_n}^0 \\ {a_1}^1 & {a_2}^1 & \cdots & {a_n}^1 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ {a_1}^{n-1} & {a_2}^{n-1} & \cdots & {a_n}^{n-1} \end{pmatrix}, \tag{6.7}$$

である. (6.7) の係数行列 V の行列式は前にも見た Vandermonde 行列式である:

$$|V| = \begin{vmatrix} {a_1}^0 & {a_2}^0 & \cdots & {a_n}^0 \\ {a_1}^1 & {a_2}^1 & \cdots & {a_n}^1 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ {a_1}^{n-1} & {a_2}^{n-1} & \cdots & {a_n}^{n-1} \end{vmatrix} = \begin{aligned} &(a_2 - a_1)(a_3 - a_1)(a_4 - a_1)\cdots(a_n - a_1) \\ &\times (a_3 - a_2)(a_4 - a_2)\cdots(a_n - a_2) \\ &\times (a_4 - a_3)\cdots(a_n - a_3) \\ &\times \quad \cdots\cdots\cdots \\ &\times (a_n - a_{n-1}) \end{aligned}.$$

我々が既に有限体 F 或いは拡大体 K の数を成分とする線形代数に立ち入っている事に注意しよう. $f(z)$ が単根しか持てないと示す有限体の構造は, この行列式が体 K 上の 0 ではない元の積として 0 ではない, 上の連立 1 次方程式が必ず解ける, と示す. 実際, 上の式 (6.7) は展開 (6.5) の係数の作る n 次元列ベクトル $\boldsymbol{c} := {}^t(c_1, c_2, \cdots, c_n) \in K^n$ の連立 1 次方程式 $\boldsymbol{x}_0 = V\boldsymbol{c}$ であり, 行列 V は正則, $|V| = D(a_1, a_2, \cdots, a_n) \neq 0$ だから, 計算の手間を問題にせず言えば実数や複素数体上と同じ形の D と行列 V の余因子とによる公式を体 F でもそのまま用いて逆行列 V^{-1} を作る事ができて, それから $\boldsymbol{c} = V^{-1}\boldsymbol{x}_0$ が一意に得られるからである. 特に 0 系列には 0(ばかりの) ベクトル $\boldsymbol{c} = \boldsymbol{0}$ が対応し, 0 ベクトルではない出発 n 連ベクトルには 0 ばかりではない $\boldsymbol{c}$ が対応する.

解系列 $\{x_k\}$ の周期 T は同じ n 連の再現, 即ちすべての $k = 0, 1, 2, \cdots$ での $\boldsymbol{x}_k = \boldsymbol{x}_{k+T}$ を実現する正で最小の T である. (6.1) と (6.4) によればそれは,

$$\boldsymbol{x}_k = \begin{pmatrix} x_k \\ x_{k+1} \\ \cdot \\ \cdot \\ \cdot \\ x_{k+n-1} \end{pmatrix} = \begin{pmatrix} c_1{a_1}^k + c_2{a_2}^k + \cdots + c_n{a_n}^k \\ c_1{a_1}^{k+1} + c_2{a_2}^{k+1} + \cdots + c_n{a_n}^{k+1} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ c_1{a_1}^{k+n-1} + c_2{a_2}^{k+n-1} + \cdots + c_n{a_n}^{k+n-1} \end{pmatrix}$$

$$= V \begin{pmatrix} {a_1}^k c_1 \\ {a_2}^k c_2 \\ \cdot \\ \cdot \\ \cdot \\ {a_n}^k c_n \end{pmatrix} = \boldsymbol{x}_{k+T} = V \begin{pmatrix} {a_1}^{k+T} c_1 \\ {a_2}^{k+T} c_2 \\ \cdot \\ \cdot \\ \cdot \\ {a_n}^{k+T} c_n \end{pmatrix}$$

の成立であり, 下段の式の両辺に左から正則関数 V の逆行列を掛け, $1 \leqq j \leqq n$ であるすべての番号 j について $a_j \neq 0$, 従って逆数 ${a_j}^{-1}$ が存在する事を用いて

$$({a_j}^T - 1)c_j \equiv 0, \quad 1 \leqq j \leqq n$$

である, と見られる. 考えているベクトル $\boldsymbol{c}$ は零ベクトルではないから, $\{c_1, c_2, \cdots, c_n\}$ の中に 0 でないものが必ずある. それが c_j なら, それに対応して ${a_j}^T - 1 = 0$ が成り立たなければならない. F 既約な $f(z)$ の K 内の特性根 $\{a_j |\ 1 \leqq j \leqq n\}$ は全て共役で, これは T が根の共通な位数 h の倍数である事, $T \geqq h$, を要求する. こうして $T = h$ の成立が示された.
(b) F 係数線形漸化式 (6.1) の解であるから, 出発の n 連が F 内から選ばれれば以後の解系列が F 内に留る事は明らかである. この場合 Corollary 5.11.(b) によって

$$\begin{aligned} x_k = (x_k)^q &= (c_1 {a_1}^k)^q + (c_2 {a_2}^k)^q + \cdots + (c_n {a_n}^k)^q \\ &= (c_1)^q ({a_1}^q)^k + (c_2)^q ({a_2}^q)^k + \cdots + (c_n)^q ({a_n}^q)^k \end{aligned}$$

が成り立つ; F の元は q 乗によって変わらず, q 乗によって F 既約な $f(z)$ の特性根は共役なものに移る事に注意しよう. これと (6.3) とから次の関係が判明する:

$$(c_j)^q = c_{j+1}, \quad j,\ j+1 \in \boldsymbol{Z}/n.$$

故に (6.5) の係数 $\{c_j |\ 1 \leqq j \leqq n\}$ の中に 0 のものがあればすべて 0 であり, $\boldsymbol{x}_0 \in F^n$ が 0 連でなければ $\{c_j |\ 1 \leqq j \leqq n\}$ の中には 0 のものは存在しない. ■

上の結論, 特に任意の有限体 F 上に必ず存在する M 系列の最長周期構造は再度の注意に値する. 実際, 系列の取る n 連 $\boldsymbol{x}_k := {}^t(x_k, x_{k+1}, \cdots, x_{k+n-1})$ の可能な値は, F の位数が q なのだから q^n だけであり, それから 0 連を除けば $q^n - 1$ しかないのに, M 系列はその全てを 1 度ずつ律儀に巡って周期を完成している. 驚くべきではないか!

この知識は次の様に逆に用いる事もできる.

Lemma 6.2. (a) 特性多項式 $f(z)$ が n 次 F 既約であり指数 h を持てば, 線形漸化式 (6.1) の解で 0 系列ではないものは初期の n 連に関わらず周期 h であり, 1 つの系列上の出発位置の違いを無視すれば $\dfrac{q^n - 1}{h}$ 個の系列に分けられる. 特に $f(z)$ が F 上の n 次原始多項式なら得られる F 上の M 系列は系列の出発位置の違いを除いてただ 1 通りである.
(b) F 係数 n 次線形漸化式の解が理論的最長の $q^n - 1$ を持てば M 系列であり, 特性多項式は n 次 F 係数原始多項式である.
(証明) (a) 指数 h の n 次既約多項式の場合得られる周期は $h | q^n - 1$ で, 系列は 0 連でない任意の初期 n 連で定まり, その可能な全体 $q^n - 1$ 個のうち h 個毎のものは同一系列に属するから, 命題の通り $\dfrac{q^n - 1}{h}$ 個の解系列の組がある.

(b) 一般に $m \leqq n$ である次数 m, 指数 $h|q^m-1$ の F 既約因数 $g(z)$ が $f(z)$ に含まれ, $g(z)$ の特性根が $a_1, a_2, \cdots, a_m$ なら, 実際に周期 $h(\leqq q^m-1 \leqq q^n-1)$ を実現する解

$$x_k = c_1 {a_1}^k + c_2 {a_2}^k + \cdots + c_m {a_m}^k, \quad k = 0,\ 1,\ 2,\ \cdots \tag{6.9}$$

がある初期条件と対応して確かに存在する. しかし 1 つの初期条件の解が理論的に最長の周期 q^n-1 を持てば, この系列内に 0 連以外のすべての n 連は含まれ, 0 連ではないこれらすべての初期 n 連に対して漸化式周期は最長である. 故に $f(z)$ の F 既約因数 $g(z)$ の指数は $h = q^n-1$ であり, $g(z)$ の次数が n で $f(z)$ そのもの, $f(z)$ 自体が最大指数 q^n-1 の F 既約 n 次原始多項式, 系列は F 上の M 系列である以外の可能性はない. ■

乱数問題は最長周期を求め, また初期条件によらず同一漸化式系列が得られる利便は大きいから, 原始多項式と対応する M 系列の利用が殆どただ 1 つの選択肢である. 残る大切な事柄はどの様にして原始多項式を見出すかである. これは古くからの大問題[61]だが, この本の中で出会う程度に係数体 F もその上の次数も小さければ, それこそ原始的だが, $f(z) \in F[z]$ を特性多項式とする線形漸化式 (6.1) の解を直接コンピュータで計算し, Lemma 6.2.(b) によってその周期が最長である事を確かめればよく, $f(z)$ が既約かどうかは確認しなくて構わない. しかし実際の問題, $p=2,\ n=500$ 程度, では p^n-1 は巨大で, この様な計算は峻拒される.[62] 存在が証明されていても算出できなければ不存在と変わらない. この点で素数 2 は他の (3 以上の奇数の) 素数とは大変異質で, 理論応用の多面で法 2 の原始多項式は特別な重要性を持つ. 実際 2^n-1 が素数になるメルセンヌ Mersenne 指数 n は奇数の素数にはないもので, 次の素晴らしい $\boldsymbol{Z}_2$ 原始性判定を与える:

定理 6.3. $n \geqq 3$ が Mersenne 指数の時, n 次多項式 $f(z) \in \boldsymbol{Z}_2[z]$ が原始多項式である必要十分条件は, $G(z) = z^{2^n} - z$ が $\boldsymbol{Z}_2$ 係数で $f(z)$ の倍数である,[63] 即ち $f(z)$ が $\boldsymbol{Z}_2$ 上で $G(z) = z^{2^n} - z$ を割り切る事である.

(証明) (必要性) $f(z)$ が $\boldsymbol{Z}_2$ 上の n 次原始多項式なら $G(z)$ を割り切る事は定理 5.16.(b) で既に見られている.

(十分性) $\boldsymbol{Z}_2$ の算法で因数分解 $G(z) = f(z)u(z)$ が成立するとしよう. $G(z)$ は $K = \mathrm{GF}(2^n)$ のすべての数を**その単根とする** 1 次因数の積なのだから, 3 次以上の $f(z)$ も単根しか持てず, それらの 3 個以上の根の中には必ず $\boldsymbol{Z}_2 = \{0,1\}$ には含まれないもの, K の元で位数 $h \geqq 2$ のもの, が存在する. h は K の乗法群 K^* の位数 2^n-1 の約数であり, 2^n-1 が素数なので $h = 2^n-1$ が成り立つ. 故に $f(z)$ は K^* の生成元を根に持つ $\boldsymbol{Z}_2$ 係数の n 次多項式であり, $\boldsymbol{Z}_2$ 上の n 次原始多項式である. ■

即ちメルセンヌ指数 n を次数に持つ $\boldsymbol{Z}_2$ 上の任意多項式 $f(z)$ では原始多項式かどうかを判定するのに $f(z)$ の既約性を確かめる必要もない; 単に z^2, $(z^2)^2 = z^{2^2}$, $\{(z^2)^2\}^2 = z^{2^3}$, $\cdots$ と 2 乗を n 回繰り返し, 途中 z^{2^k} の次数が n 以上になるたびに $f(z)$ で法 2 で割った余りを取って次数を n 次未満に下げ, $z^{2^n} = z +$「$f(z)$ の倍数」が成り立ちさえすれば原始多項式だ

---

[61] 例えば Golomb[40] の第 5,6 章から Zierler[41], Varshamov[42] や最近の Shoup[43] 等.

[62] $\boldsymbol{Z}_p$ 上の整数計算を浮動小数点計算の 10^6 倍の早さでできると大変甘く評価しよう. 1 秒間に 10^{12} 回の浮動小数点計算が可能な超高速計算機で素数の $p=2$ での $n=500$ 次の線形漸化式の最長周期 $p^n-1 \approx 2^{500} \approx 10^{150}$ に相当する回数だけ線形漸化式を計算するには次の年数が必要である:

$$10^{150}/10^{12+6} \text{秒} = 10^{132}/(60\times 60\times 24\times 365)\ \text{年} \approx 10^{132}/(3.2\times 10^7)\ \text{年} \approx 3.1\times 10^{124} \text{年}.$$

[63] 後の第 7 章の言葉で言うと,「法 $(2, f(z))$ で $z^{2^n} \equiv z$ が成り立つ」という意味である.

とわかるのである; 整数 m を法とする計算と同様に, $f(z)$ で法 2 で割った余りを取る ($f(z)$ の倍数を捨てる, 無視する) 操作を計算の任意の段階で何回行っても計算結果の $f(z)$ で割った ($f(z)$ の倍数を捨てた, 無視した) 余りは変わらない事に注意しよう. メルセンヌ指数の次数に限るとは言っても, 一般の素数 $p \geqq 3$ の法や法 2 での他の次数の場合と比べたこの計算作業の容易さは驚くべきで 2 という法の特別な重要性が納得される. このメルセンヌ次数での原始性判定法は, Matsumoto-Nishimura[44] によってごく最近さらに大きい次数の漸化式系列の周期計算の形に発展させられ, 目覚しい成果を与えられた. 第 8 章参照.

6.2. Z_p 上の M 系列の性質

$\boldsymbol{Z}_2$M 系列の性質は文献, 例えば[40] に詳しい. この節ではそれらの必要部分を取り出して議論する. ただ全体構造の見通しを良くするためには $\boldsymbol{Z}_2$ に限定しない方がよいので, 任意の素数 $\boldsymbol{Z}_p$ での Zierler[36] の結果等も含め, また議論の再確認が容易になる様に既に与えた証明との重複も避けないで再現に努める. なお自己相関関数を除く以下の議論は係数がもっと一般の有限体 F の数でも成り立ち, $\boldsymbol{Z}_p$ への限定も必要ではないが, その一般化は $\boldsymbol{Z}_p$ を F と書き変え, p を q で置き換えて容易に得られる. 状況と用語を再確認しよう:

(a) p は素数として, n 次線形漸化式

$$x_k = b_1 x_{k-1} + b_2 x_{k-2} + \cdots + b_n x_{k-n}, \ \ b_n \neq 0 \pmod p, \ \ (k \geqq n) \tag{6.10}$$

の解は, $b_n \in \boldsymbol{Z}_p^*$ によって存在する ${b_n}^{-1}$ を上に掛けて得られる逆行漸化式:

$$x_{k-n} = b_n^{-1}(-b_{n-1}x_{k-n+1} - b_{n-2}x_{k-n+2} - \cdots \\ -b_1 x_{k-\{n-(n-1)\}} + x_k) \pmod p,$$

の解系列も考え併せて, 常に x_k が $-\infty < k < \infty$ で定義されているとしてよい.

(b)「$\boldsymbol{Z}_p$ 上の n 次 M 系列」とは n 次 $\boldsymbol{Z}_p$ 係数原始多項式

$$f(z) = z^n - b_1 z^{n-1} - b_2 z^{n-2} - \cdots - b_{n-1}z^1 - b_n, \quad b_n \neq 0, \tag{6.11}$$

を特性多項式とする線形漸化式 (6.10) で作られる 0 ばかりでない $\boldsymbol{Z}_p$ 値系列とし, $\{\cdots, 0, 0, 0, \cdots\}$ は 0 系列と呼ぶ. 即ち, 我々は $\boldsymbol{Z}_p$ の n 次拡大体 $\mathrm{GF}(p^n) = K$ の乗法群 K^* の中を動く一般の M 系列, 例えば生成元 a_i に基づく $x_k = {a_i}^k$, は考えない.

(c) 同一の原始多項式に基づく M 系列は「同値」と呼び, 違う原始多項式に基づく時に「異なる M 系列」と言う事にする.

応用で大切な M 系列の性質を, 次の定理 6.4(a)–(e) に順次まとめる. 既に述べた事との重複は, 記憶の再生と理解の深化を求めて恐れない.

定理 6.4. (a) 位数 p^n の有限体 K の乗法群 K^* の原始元 · 生成元は $\phi(p^n - 1)$ 個存在する. それに対応して $\boldsymbol{Z}_p$ 上の n 次原始多項式及び n 次 M 系列は, どちらも共に $\dfrac{\phi(p^n-1)}{n}$ 個の異なるものが存在する. 特に $f(z)$ が $\boldsymbol{Z}_p$ 上の n 次原始多項式, a が伴われる原始元の 1 つで $\boldsymbol{Z}_p$ の n 次拡大体 $K = \mathrm{GF}(p^n)$ の乗法群 K^* の元なら, 原始元 $a^{-1} \in K^*$ を根に持つ「$f(z)$ の逆 reverse」と呼ばれる $f^*(z) = z^n f(\dfrac{1}{z})$ も n 次原始多項式である. この $f^*(z)$ に対応する M

系列 $\{x_k{}^*|\ -\infty < k < \infty\}$ は $f(z)$ に基づくある M 系列 $\{x_k|\ -\infty < k < \infty\}$ の逆行系列である:

$$x_k{}^* = x_{-k}.$$

(証明) K^* をその生成元 a によって $K^* = \{a^j|\ 1 \leqq j \leqq p^n - 1\}$ と巡回表現する. K^* の一般元 a^j の位数は $\dfrac{p^n-1}{(j, p^n-1)}$ だから, a^j が K^* の生成元である必要十分条件は $(j, p^n-1) = 1$, j が $p^n - 1$ と素で共通素因数を持たない事で, K^* の生成元の数はオイラーの関数 $\phi(p^n-1)$, 即ち $p^n - 1$ と素な $1 \leqq j \leqq p^n - 1$ の整数 j の総数, で与えられる. それらは n 個の組毎に $\boldsymbol{Z}_p$ 上の 1 つの n 次原始多項式を構成するから, 「異なる n 次原始多項式=同値でない M 系列」の総数は $\dfrac{\phi(p^n-1)}{n}$ 個になる. $a^{-1} := a^{p^n-2}$ も a と同位数の生成元で, $f(z)$ の逆 $f^*(z) := z^n f(\dfrac{1}{z})$ は $b_n \neq 0$ により n 次で monic に取る事もできて a^{-1} の $\boldsymbol{Z}_p$ 上の最小多項式, 原始多項式である. 故に $f^*(z)$ を決定方程式とする任意の M 系列は, 表現 (6.5) を持つ M 系列 $\{x_k\}$ に対応して

$$y_k = c_1(a_1^{-1})^k + c_2(a_2^{-1})^k + \cdots + c_n(a_n^{-1})^k = x_{-k}$$

であり, 明らかに $\{x_k\}$ の逆行系列である. ■

定理 6.4. (b) $\boldsymbol{Z}_p$ 上の同値な n 次 M 系列 $\{x_k\},\ \{y_k\}$ についてはある整数 s があって, ずらし (シフト)shift, $s:\ y_k \to y_{k+s}$, で一致する. $\{d_k,\ s(k)|1 \leqq k \leqq m\}$ を任意の個数 m の整数の任意の組とするとき, M 系列 $\{x_k\}$ のシフトの 1 次結合

$$z_k = d_1 x_{k+s(1)} + d_2 x_{k+s(2)} + \cdots + d_m x_{k+s(m)} \pmod p \qquad (6.12)$$

は「x_k と同値な M 系列か, 或いは 0 系列か」である. この性質はシフト加法性と呼ばれる.[4)]

(証明) 特性多項式 $f(z)$ が同じなら漸化式も同一で, 系列は出発値で一意に決められる. $f(z)$ が原始多項式なら M 系列 $\{x_k\}$, $\{y_k\}$ は 0 連ではないすべての n 連を同じ順序で経由し, 一方の出発値の n 連は必ず他方のどこかに存在するからずらしによって 2 系列は合致する. (6.12) の $\{z_k\}$ は同値 M 系列の和で, 漸化式の線形性から再び同じ漸化式の解である. 故に, 例えばその出発値が 0 連なら 0 系列, 0 連ではなければ M 系列で, $\{x_k\}$ と同値である. ■

定理 6.4. (c) (Zierler) 任意の自然数 $m \leqq n$ と 与えられた m 連 $\{a_1, a_2, \cdots, a_m|\ a_k \in \boldsymbol{Z}_p\}$ が $\boldsymbol{Z}_p$ 上 n 次の任意の M 系列の 1 周期に出現する回数は

$$\{a_1, a_2, \cdots, a_m\} \neq \{0, 0, \cdots, 0\} \text{ なら } p^{n-m},$$

$$\{a_1, a_2, \cdots, a_m\} = \{0, 0, \cdots, 0\} \text{ なら } p^{n-m} - 1$$

である.

(証明) 0 連でない n 連 $\{a_1, a_2, \cdots, a_m, a_{m+1}, \cdots, a_n|\ a_k \in \boldsymbol{Z}_p\}$ は M 系列上 1 度ずつ均等に出現する. 始めの m 個が同一の m 連 $\{a_1, a_2, \cdots, a_m\}$ である異なる n 連の数は

$$\{a_1, a_2, \cdots, a_m\} \neq \{0, 0, \cdots, 0\} \text{ なら } p^{n-m} \text{ 個},$$

$$\{a_1, a_2, \cdots, a_m\} = \{0, 0, \cdots, 0\} \text{ なら } p^{n-m} - 1 \text{ 個},$$

だから, 命題は明らか. ■

M 系列の上に述べた性質は重要である. 我々は素数の法 p の乗算合同法乱数のスペクトル検定を考えて, 相続く m 連が m 次元空間で占める点の密度は $\dfrac{p-1}{p^m}$, 即ちほぼ $p^{-(m-1)}$ に比例して m の増大につれて減少する事を見た. これは乗算合同法の本質的な弱点である. これに比較すると n 次 M 系列は $1 \leqq m \leqq n$ である任意の整数 m に対して法 p での m 次元空間のすべての整数点 (すべての m 連) を 0 連以外は完全に均等に, しかも 1 周期に p^{n-m} 度ずつ取る. この性質, 上の定理 6.5.(c) の内容は

「n 次 M 系列は n 次均等分布する, n-distribution を実現する」

と形容される. 1 次漸化式である乗算合同法に比べて, n 次 M 系列を生成するには n ステップ以前までのデータのメモリー保持を必要とするが, n 連までのすべての m 連の均等な出現は n ステップ離れた乱数迄の独立性の近似としては目覚ましい進歩, 可能性である.

勿論, この均等分布は 1 周期全体で見ての話だから, 系列のある小部分を用いる時それが独立乱数列を (例えば統計的検定の意味で) 常に良く近似する事は保証外である. 特に均等分布の要求そのものが乱数系列の局所的な性質の悪化に関わっているのではないか, という疑問や論争が今でも多く専門家の間に存在する. しかし乗算合同法のスペクトル検定でも事情は同じである; 1 周期にわたるスペクトル検定の結果が良くても系列の小部分が統計的に良好とは言えないが実際にスペクトル検定でよい性質を示す事が乗算合同法乱数の品質の良さの必要条件である事については疑議は少ない. それから見ても n 次均等分布, 或いはそれに近いの性質の 1 周期での実現は, 独立一様乱数の良い近似であるための「十分」とは言えなくても「必要」な条件だと主張する根拠があり,[45] ここではその立場に立つ.

定理 6.4. (d) $\boldsymbol{Z}_p$ 上の任意 n 次 M 系列 $\{x_k|\ -\infty < k < \infty\}$ から s 番目毎に取った系列 (s-系統 sampling) を定義する:

$$\{y_k^{(s)} := x_{sk+u(s)}|\ -\infty < k < \infty\},\ \ u(s) \text{ は } s \text{ 毎に定めた任意の出発番号.}$$

(i) $\{\cdots, y_0^{(s)}, y_1^{(s)}, y_2^{(s)}, \cdots\}$ が M 系列となる必要十分条件は次である:

$$(s, p^n - 1) = 1 \text{ 即ち } s \text{ は } p^n - 1 \text{ と素} \Leftrightarrow s \text{ は法 } p^n - 1 \text{ での既約剰余群 } \boldsymbol{Z}^*_{p^n-1} \text{ に属す.}$$

(ii) 法 $p^n - 1$ での整数 p の冪乗の集合 $H_p^{(p^n-1)} := \{p^k \pmod{p^n - 1} | \ k \geqq 1 \text{ は整数 }\}$ は既約剰余乗法群 $\boldsymbol{Z}^*_{p^n-1}$ の位数 n の部分群, $p \in \boldsymbol{Z}^*_{p^n-1}$ の生成する巡回部分群である. 2 系列 $\{y_k^{(s)}\}$, $\{y_k^{(t)}\}$ が同値 M 系列である必要十分条件は, s, t が $\boldsymbol{Z}^*_{p^n-1}$ の部分群 $H_p^{(p^n-1)}$ に関する同一剰余類に属す事, 即ち次の成立である:

$$t = p^k s \pmod{p^n - 1}, \quad 0 \leqq k \leqq n - 1. \tag{6.13}$$

(iii) 既約剰余群 $\boldsymbol{Z}^*_{p^n-1}$ の部分群 $H_p^{(p^n-1)}$ に関する剰余類の各々から任意に 1 つずつ取った代表全体 $\dfrac{\phi(p^n - 1)}{n}$ 個の上を s が動けば $\{y_k^{(s)}\}$ は $\boldsymbol{Z}_p$ 上のすべての異なる n 次 M 系列を掃過し, 各 s に対して $0 \leqq u(s) \leqq p^n - 2$ 全体を $u(s)$ が動けば $\{y_k^{(s)}\}$ はこの s の指定する n 次 M 系列のあらゆる初期条件を掃過する.

(iv) 蛇足ながら, 任意の素数 p と自然数 n について n は $\phi(p^n - 1)$ を割り切る.

(証明) (i) 一般性を失う事なく, M 系列 $\{x_k\}$ は $\boldsymbol{Z}_p$ の n 次拡大体 $\mathrm{GF}(p^n) = K$ の乗法群 K^* の生成元の組 $\{a_i = a_1^{p^{i-1}} | \ 1 \leqq i \leqq n\}$ を根に持つ原始多項式に基づくと仮定し, 表現

$$x_k = c_1 {a_1}^k + c_2 {a_2}^k + \cdots + c_n {a_n}^k, \quad k = n, n+1, \cdots \tag{6.14}$$

を持つとしてよい. この時

$$\{y_k^{(s)} = x_{sk+u(s)} = \sum_{i=1}^{n} c_i {a_i}^{sk+u(s)} = \sum_{i=1}^{n} d_i \{({a_1}^s)^{p^{i-1}}\}^k | \ -\infty < k < \infty, \ d_i := c_i {a_i}^{u(s)}\}$$

は ${a_1}^s$ とその共役な元の最小多項式の生成する漸化式の解系列である. これが M 系列なら ${a_1}^s$ は K^* の生成元で, 逆に ${a_1}^s$ が K^* の生成元なら上の $\{y_k^{(s)}\}$ が M 系列になる事は明らかである. ${a_1}^s$ は $(s, p^n - 1) = 1$ を満たす時, 即ち s が $p^n - 1$ と互いに素な時, さらに言い換えると $s \in \boldsymbol{Z}_{p^n-1}^*$ の時, その時に限り生成元で, これが $\{y^{(s)}\}$ が M 系列となる必要十分条件である.

(ii) 任意の素数 p は $p^n - 1$ と素で, p は既約剰余群 $\boldsymbol{Z}_{p^n-1}^*$ の元である. 故に $\boldsymbol{Z}_{p^n-1}^*$ の中で p の冪乗の全体 $H_p^{(p^n-1)} := \{p^k \pmod{p^n - 1} | \ k = 1, 2, \cdots\}$ は p が生成する巡回部分群である. 法 $p^n - 1$ で考えるとまず $p^n - 1 \equiv 0$, $p^n \equiv 1$ であり, 次に $p^1, p^2, \cdots, p^n$ は自明に異なる. 故に $H_p^{(p^n-1)}$ の位数即ち元 $p \in \boldsymbol{Z}_{p^n-1}^*$ の位数は n で $H_p^{(p^n-1)} = \{p^k | \ 1 \leqq k \leqq n\}$ であり, 当然 p^k の逆元は p^{n-k} である,

$$p^k p^{n-k} = p^n = (p^n - 1) + 1 \equiv 1 \pmod{p^n - 1}.$$

$\boldsymbol{Z}_{p^n-1}^*$ に属する s, t が同一の $H_p^{(p^n-1)}$ 剰余類 $uH_p^{(p^n-1)}$ の元で $s = up^j, \ t = up^k = sp^{k-j}$ となるなら, ${a_i}^t = ({a_i}^s)^{p^{k-j}}$ と ${a_i}^s$ とは共役な生成元で同一原始多項式に属し, 0 系列でない $\{y_k^{(s)}\}$ と $\{y_k^{(t)}\}$ は同値 M 系列である. 逆に $\{y_k^{(s)}\}$ と $\{y_k^{(t)}\}$ が同値 M 系列なら, ${a_i}^t = ({a_i}^s)^{p^k}$ がある k について成り立たなければならないから法 $p^n - 1$ で $t \equiv sp^k \in sH_p^{(p^n-1)}$, t は s と同じ $\boldsymbol{Z}_{p^n-1}^*/H_p^{(p^n-1)}$ の剰余類に属す.

(iii) s が既約剰余群 $\boldsymbol{Z}_{p^n-1}^*$ の部分群 $H_p^{(p^n-1)}$ に関する $\phi(p^n - 1)/n$ 個の全剰余類それぞれの任意の代表元を, $u(s)$ が $0 \leqq u(s) \leqq p^n - 2$ の範囲を動けば, (a) と (b) によって $y_k^{(s)}$ はすべての非同値 M 系列のすべてのシフト, 即ち $\boldsymbol{Z}_p$ 上の異なる及び同値な M 系列全体を掃過する.

(iv) 上の通り $\boldsymbol{Z}_{p^n-1}^*$ は位数 $\phi(p^n - 1)$ の群で位数 n の部分群 $H_p^{(p^n-1)}$ を持つ. 故に Lagrange の定理によって $n | \phi(p^n - 1)$ でなければならない. ■

定理 6.4. (e) $\boldsymbol{Z}_p$ 上の n 次 M 系列 $\{x_k\}$ から複素数系列 $\{\zeta_k = \exp\dfrac{2\pi i x_k}{p} | \ k = 0, 1, 2, \cdots\}$ を定義する. $\{\zeta_k\}$ の 1 周期 $T = p^n - 1$ にわたる自己相関関数 $C(t)$ について次が成り立つ:

$$C(t) := \frac{1}{T} \sum_{k=1}^{T} \zeta_k^* \zeta_{k+t} = \begin{cases} 1 & (t = 0 \mod p^n - 1), \\ -\dfrac{1}{p^n - 1} & (\text{それ以外}). \end{cases}$$

ここで ζ_k^* は ζ_k の複素共役を表す.

(証明) $\zeta_k^* \zeta_{k+t} = \exp\dfrac{2\pi i (x_{k+t} - x_k)}{p}$ だから $y_k := x_{k+t} - x_k$ の値は mod p で取ればよく, $\{x_k\}$ は $\boldsymbol{Z}_p$ 値 M 系列だから $\{y_k\}$ は t が周期 $T = p^n - 1$ の倍数なら 0 系列であり, それ以外は必ず $y_k \neq 0$ となる番号 k があるので $\{x_k\}$ と同値な M 系列になる (定理 6.4. (b)). 前者の場合は自明に $\zeta_k^* \zeta_{k+t} = 1$ がすべての k で成り立ち $C(t) = T/T = 1$ である. 後者では法 p で y_k が 0 から $p - 1$ 迄の p 個の値を 1 周期 $T = p^n - 1$ にそれぞれ p^{n-1} 回ずつ, 但し 0 は 1 回だけ少なく取る (定理 6.4.(c)) から, $\zeta_k^* \zeta_{k+t} = \exp(2\pi i y_k / p)$ は 1 の p 乗根のすべてを均等に

p^{n-1} 回, 但し 1 だけ 1 回少なく巡り,

$$C(t) = \frac{(1 \text{ の } p \text{ 乗根の総和 } 0) \times p^{n-1}}{T} - \frac{1}{T} = -\frac{1}{T} = -\frac{1}{p^n - 1}. \qquad \blacksquare$$

6.3. Z_p 上の M 系列の一様乱数への組み上げ: 伏見-手塚の定理

現実に $p = 2^{31} - 1 = 2147483647$ の様な大きい素数を法とする $\boldsymbol{Z}_p$ 上の n 次原始多項式 $f(z)$ が生成する M 系列 $\{x_k | \ k = 0, 1, \cdots\}$ が得られれば, $\{u_k := \dfrac{x_k}{p} | \ k = 0, 1, \cdots\}$ と直ちに置いて, 可能な $p^n - 1$ 個の値の組を相続く n 連がすべて均等に取り, その初期値は 0 ばかりでない事以外設定自由, 自己相関関数もほぼ理想的 (定理 6.4. (e)) など, 大変優秀と見える一様乱数発生ルーチンが得られる. しかし問題がその様な大きな p の法でのしかも高次の原始多項式 $f(z)$ の実際算出の困難にある. 現在群を抜いて高次の原始多項式が調べられているのは $\boldsymbol{Z}_2$ 上だから, 工学での $\boldsymbol{Z}_2$ に限った議論は殆ど唯一の選択肢である. M 系列による実数一様乱数生成方式はこうして,

(a) $\boldsymbol{Z}_2$ 上の大きい次数 n を持つ原始多項式を用い,

(b) それらを m 個連結 concatenate して m ビット一様乱数を作る

方向に主として進んで来た. この応用方針の範囲内での大問題とその解決 (伏見-手塚の定理) の主要部分とを考える. 高次の $\boldsymbol{Z}_2$ 原始多項式を利用して $\boldsymbol{Z}_2$ 上の M 系列を実用乱数, 例えば $m = 32$ の 4 バイト実数乱数へ組み上げる問題の実際は, Tausworthe[10] がまず 1 つの方向を与え, Lewis and Payne[11] がより実際的と見える他の方法を提案して発展が始まった. これらの方法を T 型及び LP 型と名付けて問題点を具体的に見て進もう. 但し $\boldsymbol{Z}_2$ に限定しない方が全体構造の見通しが良いので, 我々は一般には $\boldsymbol{Z}_p$ で議論を進める.

T 型及び LP 型の方法では $\boldsymbol{Z}_p$ 上の n 次原始多項式, $\mathrm{GF}(p^n)$ でのその根を再び $\{a_1, a_2, \cdots, a_n\}$ としよう, の作る M 系列 $\{x_k\}$ の相続く m 個を p 進小数の m 桁とする数列

$$\begin{aligned} (\text{T 型}) \ u_k &= 0.x_{ks}x_{ks+1}x_{ks+2}\cdots x_{ks+m-1}, \\ (\text{LP 型}) \ v_k &= 0.x_k x_{k+t} x_{k+2t} \cdots x_{k+(m-1)t} \end{aligned} \tag{6.15}$$

を組み上げる.[64] Tausworthe 系列では, 周期の最長性を損なわない様に s は $p^n - 1$ と素, つまり既約剰余群 $\boldsymbol{Z}^*_{p^n-1}$ の元に取られる. s の $\boldsymbol{Z}^*_{p^n-1}$ での逆元を t, $st \equiv 1 \pmod{p^n - 1}$ と置くと, T 型系列は

$$x_{ks+j} = \sum_{i=1}^{n} c_i {a_i}^{s(k+tj)} = \sum_{i=1}^{n} c_i ({a_i}^s)^{k+tj} =: y_{k+tj}, \tag{6.16}$$

と表される. $\{y_k | \ k = 0, 1, \cdots\}$ は生成元 $\{{a_i}^s | \ 1 \leqq i \leqq n\}$ に基づく LP 型 M 系列で, $\boldsymbol{Z}^*_{p^n-1}$ で s が属する $H_p^{(p^n-1)}$ 剰余類で決定される (定理 6.4.(d)). これが「T 型系列と LP 型系列の相反則 (伏見 [46])」で, $t \in \boldsymbol{Z}^*_{p^n-1}$ の場合 2 つの組み上げ方法は原始多項式, 即ち M 系列の生成漸化式を適当に取り換えれば互いに同じものと見てよい.

だから T 型と LP 型の連結 M 系列乱数は美点も欠点も共有する. 勿論この認識を経なく

[64] LP 型系列の取り方は (6.15) で尽くされるものではないが, これ以外の取り方をしても LP 型連結 M 系列乱数の問題点の一般解決が得られるわけではない, 解決は伏見-手塚の定理に頼る以外に道がない, ので, ここでは T 型系列に対応する (6.15) の形に限定する.

ても, 例えば T 型系列の一般的難点は古く Tootill et al.[47] がその p.393 で (1 つの対策と共に) 指摘している通りで, 条件「s と p^n-1 とが素」であるだけでは Tausworthe 乱数系列は理論的には可能なはずの $[n/s]:=$「(n/s) の整数部分」次の均等分布を取れない.[65] 乱数生成手順から見て容易で望ましいのは LP 型系列だが, T 型のこの難点はそのまま LP 型の難点でもあるから,「与えられた M 系列或いはその漸化式に対してどのような出発ベクトルの選択が理論的に可能な最大の均等分布を連結 M 系列乱数に保証するか」, という問題が浮び上がる. これが伏見-手塚によって一般にそして完全に解決された.

問題の理解は視覚化すると容易になる. $\boldsymbol{Z}_2$ 上の 10 次原始多項式 $f(z)=z^{10}+z^7+1$ が生成する 10 次 M 系列を, 列方向に並べた次の 5 組の初期値で考えよう:

$$\boldsymbol{x}^{(1)}\!\to\!\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\1\\0\\0\\0\end{pmatrix}\quad \boldsymbol{x}^{(2)}\!\to\!\begin{pmatrix}0\\1\\0\\0\\0\\0\\0\\0\\1\\0\\0\end{pmatrix}\quad \boldsymbol{x}^{(3)}\!\to\!\begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\0\\0\\1\\0\end{pmatrix}\quad \boldsymbol{x}^{(4)}\!\to\!\begin{pmatrix}0\\0\\0\\1\\0\\0\\0\\0\\0\\0\\1\end{pmatrix}\quad \boldsymbol{x}^{(5)}\!\to\!\begin{pmatrix}0\\0\\0\\0\\1\\0\\0\\0\\0\\0\\0\end{pmatrix}. \tag{6.17}$$

$f(z)$ が $\boldsymbol{Z}_2$ 上の原始多項式である事は原始多項式表からも見られるが, 対応する法 2 の線形漸化式解の周期を計算しても簡単に知る事ができる. 上から出発する 5 組の同値な 10 次 M 系列無限次元列ベクトル $\{\boldsymbol{x}^{(1)},\boldsymbol{x}^{(2)},\cdots,\boldsymbol{x}^{(5)}\}$,

$$\begin{aligned}\boldsymbol{x}^{(j)}={}^t(&x_0^{(j)},\,x_1^{(j)},\,x_2^{(j)},\,\cdots,\,x_9^{(j)},\,x_{10}^{(j)}=x_7^{(j)}+x_0^{(j)},\\ &x_{11}^{(j)}=x_8^{(j)}+x_1^{(j)},\,\cdots,\,x_k^{(j)}=x_{k-3}^{(j)}+x_{k-10}^{(j)},\,\cdots)\end{aligned} \tag{6.18}$$

を 2 進第 j 桁に組み上げて得られる 5 ビットの実数列 $\{v_k=0.x_k^{(1)}x_k^{(2)}x_k^{(3)}x_k^{(4)}x_k^{(5)}|\,k\geqq 0\}$ を LP 型一様乱数出力系列としよう. 明らかに上の出発値 10 次元列ベクトルの 5 個の組は 1 次独立であり, この性質は系列 $\{v_k\}$ と同様に組み立てられた一般の乱数出力の値の均等分布を保証する. これは下の 2 段の議論で知られる:

Lemma 6.5. $\boldsymbol{Z}_p$ 上の同一の n 次 M 系列漸化式,

$$x_k^{(j)}=b_1x_{k-1}^{(j)}+b_2x_{k-2}^{(j)}+\cdots+b_nx_{k-n}^{(j)}\pmod p,\;\; b_n\not\equiv 0,\;\; 1\leqq j\leqq n \tag{6.19}$$

に従う n 個の系列 $\{x_k^{(1)},x_k^{(2)},\cdots,x_k^{(n)}|\,k=0,1,\cdots\}$ を考え, どれも 0 系列ではないとする. これらをそれぞれ k を行指定子とする無限次列ベクトル $\boldsymbol{x}^{(j)}:={}^t(x_0^{(j)},x_1^{(j)},x_2^{(j)},\cdots)$ とみなし, 第 k 行からの n 行で作られる下の $n\times n$ 行列 $M_k(\boldsymbol{x}^{(1)},\boldsymbol{x}^{(2)},\cdots,\boldsymbol{x}^{(n)})$ を取る. この行列の行列式 $\det M_k=|M_k|$ はすべての k で 0 か, 0 である k は存在しないか, の二者択一である:

[65] 大部の Tootill et al. を p.393 まで読み通す事, 或いは Tausworthe の原論文 [10] の, さらに言えば Fushimi-Tezuka[12] の一瞬の記述, "$\cdots$ (Tausworthe generator can attain $[n/s]$-distribution) if parameters are appropriately chosen" の紙背にまで眼光を徹するのは難しいので, 付録 A に簡単な反例を掲げる.

$$M_k(\boldsymbol{x}^{(1)},\boldsymbol{x}^{(2)},\cdots,\boldsymbol{x}^{(n)}) := \begin{pmatrix} x_k^{(1)} & x_k^{(2)} & \cdots & x_k^{(n)} \\ x_{k+1}^{(1)} & x_{k+1}^{(2)} & \cdots & x_{k+1}^{(n)} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ x_{k+n-1}^{(1)} & x_{k+n-1}^{(2)} & \cdots & x_{k+n-1}^{(n)} \end{pmatrix}.$$

(証明) 一般に $\{y_k, z_k|\ k_0 \leqq k \leqq k_0+n-1\}$ が同値である 2 つの n 次 M 系列上の任意の番号 $k=k_0$ から始る n 連なら, それらの 1 次結合の n 連 $\{x_k = ay_k + bz_k|\ k_0 \leqq k \leqq k_0+n-1\}$ を k_0 からの出発値とし, 同一の線形漸化式或いは対応する逆行の線形漸化式に従う同値な M 系列 $\{x_k\}$ はすべての番号 k で $x_k = ay_k + bz_k$ を満たさなければならない. $n\times n$ 行列の行列式 $=0$ とその列の 1 次従属性とは (任意体上) 同値だから, 上の $M_k(\boldsymbol{x}^{(1)},\boldsymbol{x}^{(2)},\cdots,\boldsymbol{x}^{(n)})$ がどれかの k_0 で行列式 $|M_{k_0}|=0$ を与える, 即ちその列に 1 次従属関係を持つ事はすべての k で行列 M_k の列が 1 次従属である事, 行列式 $|M_k|=0$ が成り立つ事, と同値である. 故に命題通り, 行列式 $|M_k|$ はすべての k で同時に 0 となるか, 0 となる k は存在しないか, の二者択一である. ■

上の僅かな「或いは逆行漸化式に従う」という記述がこの証明全体の鍵である. 大切な所だから少しぶっきらぼうだが別証明を 1 つ添える.

(Lemma 6.5. 別証) $1\leqq j\leqq n$ の任意の第 j 列ベクトルの M 系列 $\boldsymbol{x}^{(j)}$ の成分は (6.19) の漸化式に従う. だから $n\times n$ 遷移行列 (transfer matrix) を T,

$$T := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 \\ b_n & b_{n-1} & b_{n-2} & \cdots & b_1 \end{pmatrix},$$

として $\det T = (-1)^{n+1}b_n \neq 0$ 及び $M_{k+1}(\boldsymbol{x}^{(1)},\boldsymbol{x}^{(2)},\cdots,\boldsymbol{x}^{(n)}) = TM_k(\boldsymbol{x}^{(1)},\boldsymbol{x}^{(2)},\cdots,\boldsymbol{x}^{(n)})$ が任意の整数 $k=0,\pm1,\pm2,\cdots$ に対して成り立つ. これらは

$$M_k(\boldsymbol{x}^{(1)},\boldsymbol{x}^{(2)},\cdots,\boldsymbol{x}^{(n)}) = T^kM_0(\boldsymbol{x}^{(1)},\boldsymbol{x}^{(2)},\cdots,\boldsymbol{x}^{(n)}),\quad \det M_k = |T|^k \det M_0$$

を意味し, $\det M_k(\boldsymbol{x}^{(1)},\boldsymbol{x}^{(2)},\cdots,\boldsymbol{x}^{(n)})$ はすべての k で同時に 0 となるか 0 である k は存在しないか, の二者択一である. ■

Bright と Enison[48] は次を示した.

定理 6.6. (Bright-Enison) $\boldsymbol{Z}_p$ 上の (6.18) の形の同値 n 次 M 系列 m 個 $(m\leqq n)$, $\boldsymbol{x}^{(1)},\boldsymbol{x}^{(2)},\cdots,\boldsymbol{x}^{(m)}$, に与えられた $\boldsymbol{Z}_p$ の意味での 1 次独立な任意の出発値列ベクトルから作られる p 進 m 桁の実数の列

$$\{v_k = 0.x_k^{(1)}x_k^{(2)}\cdots x_k^{(m)}|\ k\geqq 0\} \tag{6.20}$$

は 1 次均等分布を持つ. 即ち

v_k は 1 周期 $0\leqq k < p^n-1$ の間に $[0,1]$ の p^{-m} 毎のすべての数値を p^{n-m} 回ずつ, 但し 0 は 1 度だけ少なく取る.

(証明) $\boldsymbol{x}^{(1)}$ から $\boldsymbol{x}^{(m)}$ の初期値の n 次元列ベクトルの 1 次独立性から, さらに $n-m$ 個の n 次元列ベクトルを補って次の $\boldsymbol{Z}_p$ での $n\times n$ 正則行列を作る;

$$M_k(\boldsymbol{x}^{(1)},\boldsymbol{x}^{(2)},\cdots,\boldsymbol{x}^{(n)})=\begin{pmatrix} x_k^{(1)} & x_k^{(2)} & \cdots & x_k^{(n)} \\ x_{k+1}^{(1)} & x_{k+1}^{(2)} & \cdots & x_{k+1}^{(n)} \\ x_{k+2}^{(1)} & x_{k+2}^{(2)} & \cdots & x_{k+2}^{(n)} \\ \cdot & \cdot & \cdots & \cdot \\ x_{k+n-1}^{(1)} & x_{k+n-1}^{(2)} & \cdots & x_{k+n-1}^{(n)} \end{pmatrix}.$$

$M_0:=V$ と記そう. 補う列ベクトルは V が正則になるなら何でもよい. 付加された非 0 初期値ベクトルが生成する $\boldsymbol{Z}_p$M 系列を (6.18) の形の無限次元列ベクトルで $\boldsymbol{x}^{(m+1)},\boldsymbol{x}^{(m+2)},\cdots,\boldsymbol{x}^{(n)}$ と記す. Lemma 6.5 によれば, 全体の n 系列から作った $n\times n$ 行列は $\det M_0=\det V=|V|\neq 0$ の仮定によってすべての k で正則である. n 次元行ベクトル[66]

$${}^t\boldsymbol{X}_k=(x_k^{(1)},x_k^{(2)},\cdots,x_k^{(n)}),\ \ k=0,1,\cdots,$$

を定義すると, 列ベクトル $\boldsymbol{x}^{(j)}$ の共通漸化式 (6.19) から次の行ベクトル漸化式が成り立つ:

$${}^t\boldsymbol{X}_k=b_1{}^t\boldsymbol{X}_{k-1}+b_2{}^t\boldsymbol{X}_{k-2}+\cdots+b_n{}^t\boldsymbol{X}_{k-n}. \qquad (6.21)^{67}$$

必要ならこれとその逆行漸化式とを繰り返し用いれば, 任意の k に対する行ベクトル ${}^t\boldsymbol{X}_k$ は任意の j からの n 連の行ベクトル ${}^t\boldsymbol{X}_j,{}^t\boldsymbol{X}_{j+1},\cdots,{}^t\boldsymbol{X}_{j+n-1}$ で

$${}^t\boldsymbol{X}_k=d_{k-j}{}^t\boldsymbol{X}_j+d_{k-j-1}{}^t\boldsymbol{X}_{j+1}+\cdots+d_{k-j-(n-1)}{}^t\boldsymbol{X}_{j+(n-1)}, \qquad (6.22)$$

と表せる. (6.22) もその逆も定数係数差分方程式だから, 上の係数は一般の $d_{k,j}$ ではなく d_{k-j} の形になる. またこの係数 $\{d_{k-j},\cdots,d_{k-j-(n-1)}\}$ は一意である; もし

$$\begin{aligned}{}^t\boldsymbol{X}_k&=d_{k-j}{}^t\boldsymbol{X}_j+d_{k-j-1}{}^t\boldsymbol{X}_{j+1}+\cdots+d_{k-j-(n-1)}{}^t\boldsymbol{X}_{j+(n-1)}\\&=e_{k-j}{}^t\boldsymbol{X}_j+e_{k-j-1}{}^t\boldsymbol{X}_{j+1}+\cdots+e_{k-j-(n-1)}{}^t\boldsymbol{X}_{j+(n-1)}\end{aligned}$$

が異なる係数の組 $\{e_{k-j},e_{k-j-1},\cdots,e_{k-j-(n-1)}\}$ についても成り立てば, n 個の相続く行ベクトル ${}^t\boldsymbol{X}_j,{}^t\boldsymbol{X}_{j+1},\cdots,{}^t\boldsymbol{X}_{j+(n-1)}$ は 1 次従属で $n\times n$ 行列 $M_j(\boldsymbol{x}^{(1)},\boldsymbol{x}^{(2)},\cdots,\boldsymbol{x}^{(n)})$ の正則性に反するからである. $\boldsymbol{Z}_p$ 上の n 次 M 系列の周期は $T=p^n-1$ だから, ${}^t\boldsymbol{X}_{k+T}={}^t\boldsymbol{X}_k$ の成立は明らか. n 次元行ベクトル ${}^t\boldsymbol{X}_k$ の成分の取る事の可能な値の組は, 行列式 $\det M_k\neq 0$ から 0 ベクトルは取れないから, M 系列と同数の $p^n-1=T$ 個ある. ある番号 k に対して ${}^t\boldsymbol{X}_k={}^t\boldsymbol{X}_{k+L},\ 0<L<T$ となる L を考えると, すべての k,j で成り立つ (6.22) で $k\to k+L, j\to k$ と置いて,

$${}^t\boldsymbol{X}_k={}^t\boldsymbol{X}_{k+L}=d_L{}^t\boldsymbol{X}_k+d_{L-1}{}^t\boldsymbol{X}_{k+1}+\cdots+d_{L-(n-1)}{}^t\boldsymbol{X}_{k+(n-1)},$$

故に一意に $d_L=1, d_{L-1}=d_{L-2}=\cdots=d_{L-(n-1)}=0$, 即ちすべての k について ${}^t\boldsymbol{X}_{k+L}={}^t\boldsymbol{X}_k$ である. これは L 離れた 2 つの行ベクトルが一致する様な L は, 実は ${}^t\boldsymbol{X}_k$ のす

---

[66] 太文字は縦の列ベクトルを表すと約束した. 故に横の行ベクトルを表すには, 縦ベクトル $\boldsymbol{X}$ の転置 transpose ${}^t\boldsymbol{X}$ を使わなければならない.

[67] 勿論我々の $p=2, m=5$ の例なら (6.21) に対応して $\boldsymbol{Z}_2$ 上の 5 次漸化式 ${}^t\boldsymbol{X}_k={}^t\boldsymbol{X}_{k-3}+{}^t\boldsymbol{X}_{k-10}$ となる. この様な漸化式の解の実際計算機上での生成は, (6.20) の 2 進 5 桁の数 $\{v_k=0.x_k^{(1)}x_k^{(2)}x_k^{(3)}x_k^{(4)}x_k^{(5)}\,|\,k\geqq 0\}$ をむしろ直接使って $v_k=v_{k-3}\oplus v_{k-10}$, $\oplus$ は 2 進桁毎の繰り上がりなしの $\boldsymbol{Z}_2$ 和, exclusive or, XOR とも呼ばれる, とすればより簡単に実現できる.

べての列成分である M 系列 $\{x_k^{(j)}\}$ の k の周期 T の倍数に限られる事を意味する. こうして行ベクトル ${}^t\boldsymbol{X}_k$ も同じものは $T = p^n - 1$ 毎に出現し, その間にはすべての可能な n 連を経由しなければならない. この行ベクトル ${}^t\boldsymbol{X}_k$ の前半の m 連を p 進法で読んだ (6.20) の v_k は定理 6.4.(c) によって可能な p^m の各桁の組合わせを各 p^{n-m} 回, 但し $(00\cdots0)$ は 1 度少なく, 取る. ■

この定理は我々が $\boldsymbol{Z}_2$ 上で考えた 10 次 M 系列 5 個の連結による 2 進 5 桁の乱数列 $\{v_k\}$ にも, その出発 10 連ベクトルの 1 次独立性によって, 1 次均等分布を保証する. しかし v_k の 1 次均等分布にも関わらず, 例えば相続く 2 つの数の対 (v_k, v_{k+1}) には強い相関の可能性がある. 下の図 (a) はこの様子の 1 周期 $0 \leqq k \leqq 2^{10} - 2$ にわたるプロットで, 同様の鳥の足跡の様な強い相関を示すプロットは $\dfrac{10}{5} = 2$ 次元均等分布からは程遠いこの形の乱数の性質の悪さの証拠として多くの研究に記されている. 原因は出発の 10 連初期ベクトルの取り方に

(a) (b)

あるが, 議論の前に納得のため上の 5 ビット乱数で 2 次元均等分布が得られる簡単な初期値設定の 1 つを下に示そう. 結果としての 5 ビット乱数 $\{v_k |\ 0 \leqq k \leqq 1022\}$ の対 (v_k, v_{k+1}) のきれいな均等分布は, 0 の 10 連の不在から (0,0) だけは出現しない事と共に, 再び上の図 (b) から見られる:

$$\boldsymbol{x}^{(1)} \to \begin{pmatrix} 1\\0\\0\\0\\0\\0\\0\\0\\0\\0 \end{pmatrix} \quad \boldsymbol{x}^{(2)} \to \begin{pmatrix} 0\\0\\1\\0\\0\\0\\0\\0\\0\\0 \end{pmatrix} \quad \boldsymbol{x}^{(3)} \to \begin{pmatrix} 0\\0\\0\\0\\1\\0\\0\\0\\0\\0 \end{pmatrix} \quad \boldsymbol{x}^{(4)} \to \begin{pmatrix} 0\\0\\0\\0\\0\\1\\0\\0\\0\\0 \end{pmatrix} \quad \boldsymbol{x}^{(5)} \to \begin{pmatrix} 0\\0\\0\\0\\0\\0\\0\\0\\1\\0 \end{pmatrix} \tag{6.23}$$

一般に均等分布を理論的に保証された乱数系列は必ず上の図 (b) の様なプロットを与え, 改めて図を描く必要はないが, プログラム, 証明, 論理や推論は無欠とは限らないので「目で見るまで信じない」のが (もし間に合えば) 安全な戦略とは言える. 勿論文献では普通 $\boldsymbol{Z}_2$ 上 500 次あるいはそれ以上の高次原始多項式が用いられ, 全周期のプロットは困難だが, 部分的な様子からでも多くの示唆があり得る. 再度強調すべき大切な認識は

(a) 連結 M 系列乱数では本当にこの様な高次均等分布が得られ,

(b) 文献にしばしば示された鳥の足跡様の 2 連図は初期値設定の誤りで,
(c) 高次均等分布の完璧な処方は伏見-手塚の定理である,
であろう.

Fushimi and Tezuka[12] による最終的解決に向かう. $\boldsymbol{Z}_p$ 上の n 次 M 系列 $\{x_k\}$ から m 個 ($m \leqq n$) を取って p 進 m 桁乱数列 (念のため再記する)

$$v_k = 0.x_k^{(1)}x_k^{(2)}\cdots x_k^{(m)}, \quad k = 0, 1, \cdots \tag{6.20}$$

とする時, 理論的に可能な最大の均等分布次元 d は, $[\cdots]$ をガウスの記号 ($\cdots$ を越えない最大の整数) として $d = [n/m]$ である. この最大次元均等分布を保証する各桁の M 系列 $\boldsymbol{x}^{(j)}$ の出発値の与え方は次で与えられる:[12]

定理 6.7. (Fushimi-Tezuka) 初期値 $1 \times m$ 行ベクトル ${}^t\boldsymbol{X}_k$ を定義する:

$$ {}^t\boldsymbol{X}_k := (x_k^{(1)}, x_k^{(2)}, \cdots, x_k^{(m)}), \ \ 0 \leqq k \leqq n-1.$$

n 次 M 系列漸化式から $d = [n/m]$ 次の最大次均等分布が得られるための必要十分条件は, これらの初期値から漸化式で生成される ${}^t\boldsymbol{X}_n, {}^t\boldsymbol{X}_{n+1}, \cdots$ を補って得られる次の $n \times dm$ 行列の列ベクトルの 1 次独立性である:

$$\begin{pmatrix} {}^t\boldsymbol{X}_0 & {}^t\boldsymbol{X}_1 & {}^t\boldsymbol{X}_2 & \cdots & {}^t\boldsymbol{X}_{d-1} \\ {}^t\boldsymbol{X}_1 & {}^t\boldsymbol{X}_2 & {}^t\boldsymbol{X}_3 & \cdots & {}^t\boldsymbol{X}_d \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ {}^t\boldsymbol{X}_{n-2} & {}^t\boldsymbol{X}_{n-1} & {}^t\boldsymbol{X}_n & \cdots & {}^t\boldsymbol{X}_{n+d-3} \\ {}^t\boldsymbol{X}_{n-1} & {}^t\boldsymbol{X}_n & {}^t\boldsymbol{X}_{n+1} & \cdots & {}^t\boldsymbol{X}_{n+d-2} \end{pmatrix} \tag{6.24}$$

(証明) (必要性) 仮に行列 (6.24) の列ベクトルが 1 次従属なら, Lemma 6.5 の証明で見た様に, この 1 次従属性はこれらの列ベクトルを出発 n 連とする無限次元列ベクトルの全体, 同値な md 個の M 系列, のすべて (の行番号) の上にわたって同一の係数で成り立つ. 上の行列 (6.24) の構造から見て, それは任意の番号 k での行ベクトル ${}^t\boldsymbol{X}_k, {}^t\boldsymbol{X}_{k+1}, {}^t\boldsymbol{X}_{k+2}, \cdots, {}^t\boldsymbol{X}_{k+d-1}$ の中で ${}^t\boldsymbol{X}_k$ の中のどれかの列成分が必ずその右の ${}^t\boldsymbol{X}_{k+1}, {}^t\boldsymbol{X}_{k+2}, \cdots, {}^t\boldsymbol{X}_{k+d-1}$ の列成分の同一の 1 次結合で表される, 言い換えると (6.20) の v_k のある桁の数 $x_k^{(j)}$ がすべての番号 k で $v_{k+1}, v_{k+2}, \cdots, v_{k+d-1}$ のそれぞれきまった桁の数値の同一の 1 次結合で表される, という事を意味する. (6.20) の p 進数 v_k が $\boldsymbol{Z}_p$ 上での最大の d 次均等分布であるためにはこれらが全く関係なく値を取らなければならないから, この 1 次従属の仮定とは両立しない. 故に (6.20) の v_k が d 次均等分布なら (6.24) の行列は 1 次独立な列ベクトルを持つ.
(十分性) 定理 6.6 の証明で見たように, (6.24) が最大 $\mathrm{rank}(= md \leqq n)$ の $n \times md$ 行列であれば ($n - md > 0$ で必要なら)$n - md$ 個の列 (とそれから出発する M 系列) を補って正則な $n \times n$ 行列 A を作る事ができる. その上で, 定理 6.6 の証明の完全なトレースがこの行列の n 次元行ベクトルの周期 $p^n - 1$ での 1 次均等分布を示す事は明らか. 故に 1 つの行の中の m 桁の数は d 次均等分布をする. ■

列の 1 次独立性は列の交換で不変だから, 行列 (6.24) は

$x_0^{(1)}$ から $x_{n-1}^{(1)}$ を第 1 列に,

$x_1^{(1)}$ から $x_n^{(1)}$ を第 2 列に,

. . . . . .

$x_{d-1}^{(1)}$ から $x_{n+d-2}^{(1)}$ を第 d 列に,
$x_0^{(2)}$ から $x_{n-1}^{(2)}$ を第 $d+1$ 列に,
. . . . . .

と, 要するに各 j 桁目の系列の長さ $n+d-1$ の部分 $\{x_0^{(j)}, x_1^{(j)}, \cdots, x_{n+d-2}^{(j)}\}$ を 1 つずつずらしながら作った d 個の n 次元の列 (行として構成しても差し支えない) ベクトルの $1 \leqq j \leqq m$ にわたる全体 md 個の 1 次独立性の問題である.

6.4. Z_p の上でのベクトルの 1 次独立性

伏見-手塚の定理の応用で我々は $\boldsymbol{Z}_p$ のベクトルの 1 次独立性の判定の必要に面する. これはベクトルの作る行列の $\boldsymbol{Z}_p$ での rank を計算して得られる. 任意の $m \times n$ 行列 $A = (a_{ij})$ について, その「$\boldsymbol{Z}_p$ での階数, rank, 位数」は次で定義される正または 0 の整数 $\mathrm{rank}A$ である:

定義 6.8. $m \times n$ 行列 $A = (a_{ij})$ から n 個の行, その行番号は $1 \leqq i_1 < i_2 < \cdots < i_n \leqq m$, と n 個の列, その列番号は $1 \leqq j_1 < j_2 < \cdots < j_n \leqq n$ を取って作られる n 次の小行列 A',

$$A' = \begin{pmatrix} a_{i_1 j_1} & a_{i_1 j_2} & \cdots & a_{i_1 j_n} \\ a_{i_2 j_1} & a_{i_2 j_2} & \cdots & a_{i_2 j_n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i_n j_1} & a_{i_n j_2} & \cdots & a_{i_n j_n} \end{pmatrix}$$

の中に $\boldsymbol{Z}_p$ の意味で行列式 $|A'| \neq 0$ となるものがあり, $(n+1)$ 次以上の小行列の行列式はすべて 0 の時, 「$\boldsymbol{Z}_p$ での A の階数, 位数, ランク $\mathrm{rank}A = n$ である」と言う. 行列 A の成分 a_{ij} がすべて 0 なら $\mathrm{rank}A = 0$ とする. **(定義 6.8. 終り)**

小行列式 $|A'| = 0$ なら A' の行ベクトルの中に他の行ベクトルに $\boldsymbol{Z}_p$ 係数で 1 次従属のものがあり, 同様に列ベクトルの中に他の列ベクトルに $\boldsymbol{Z}_p$ 係数で 1 次従属のものがある.
従って

$\mathrm{rank}A =$「A の 1 次独立行ベクトルの最大数」=「1 次独立列ベクトルの最大数」

である事, は実数体, 複素数体上の線形代数, 特に連立 1 次方程式論でよく知られている通りでここでは証明しない. 常に $\mathrm{rank}A \leqq \min(m, n)$ が成り立つ事も勿論である.

上の定義での $\mathrm{rank}A$ の計算は難しいが, 実際は消去法による連立 1 次方程式の解法や行列式の計算より遥かに容易に, しかも一般の体の中で, $\mathrm{rank}A$ は求められる. 要点は次である:

Lemma 6.9. 行列の行や列, 或いは行の間, 列の間の次の基本操作或いは基本変形 (a)-(c) で行列の rank は不変である:

(a) 2 つの行または列を交換する.
(b) 1 つの行または列に逆数を持つ数を掛ける.
(c) 1 つの行の任意定数倍を他の行に加える. 或いは 1 つの列の任意定数倍を他の列に加える.

(証明) (a) 行や列の交換はそれらベクトルの $\boldsymbol{Z}_p$ 係数での 1 次独立性や 1 次独立なものの総数に関係ないから rank は変らない.
(b) 行列 A の 1 つの行や列を逆数を持つ数 c 倍する事も同様である.

(c) これも 1 次独立性から明らかである.[68] ■

上の Lemma は, rank$A$ の計算は A の**行の間, 或いは列の間**に変形 (a)–(c) を施して rank の見やすい対角行列

$$A \to \begin{pmatrix} a & 0 & 0 & \cdot & \cdot & \cdot \\ 0 & b & 0 & \cdot & \cdot & \cdot \\ 0 & 0 & c & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & l \end{pmatrix}$$

に変形すれば, 対角成分で 0 でないものの数, として見られる事を示している. 勿論必ずしも対角行列まで変形する必要はない. 例えば上 (或いは下)3 角形でも, 0 ではない行 (或いは列) は列や行の交換で必ず対角成分に逆数を持つ因子を置く様に pivoting してあれば (それから対角形への変形は一足跳びだがそのままで), 0 ではない対角成分数が rank である.

ベクトルの 1 次独立性, 行列のランク等々が普通の数 (実数, 複素数) ばかりでなく任意の素数の法 p の数体系 $\boldsymbol{Z}_p$ でも (もっと一般には任意の体 F でも) 考えられ, 行列のランクを求める上の議論はそのまま成り立つ事に再度注意する. ただ $\boldsymbol{Z}_p$ の場合は普通の整数の加減乗算で最後に法 p で簡約しても結果が同じだから, 実数計算で**行や列の割り算と p 倍とを含まず**行って最後に対角線の法 p で 0 でない成分の数を勘定してもよい. ここで述べた考え方はさらに「単因子」とその応用にまで深める事もできるが, これは付録 C に委ね, 以下具体的に問題で考えてみよう.

問題 6.10. (a) 次の行列の rank を求めよ.

$$(1)\ A = \begin{pmatrix} 1 & 2 & 4 & 4 \\ 2 & 3 & 3 & 5 \\ 6 & 7 & 1 & -9 \\ -1 & 1 & 1 & 2 \end{pmatrix} \qquad (2)\ B = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & -2 & 3 & 5 \\ 1 & 3 & -1 & 2 \\ 2 & -2 & 1 & -1 \end{pmatrix}$$

(b) 同じ行列 A, B の法 2,3 での rank を求めよ.

(解) (a) 行や列の基本変形を行って (上)3 角形にする.

---

[68] 別の technical な証明を与えておく. 行列 A の列ベクトル $\boldsymbol{a}$ の c 倍を列ベクトル $\boldsymbol{b}$ に加えて行列 A が行列 B になり, A の $n \times n$ 小行列 A' が B の $n \times n$ 小行列 B' になるとする. 次を示す:

「もし A' が正則なら, B にも必ず $|B''| \neq 0$ である $n \times n$ 小行列 B'' がある.」

これが成り立てば rank$A \leqq$ rank$B$ が示される; 一方変形された行列 B の列 $\boldsymbol{b}$ に $\boldsymbol{a}$ の $-c$ 倍を加えれば行列 B から行列 A が変形 (c) で得られる事は明らかで rank$A \geqq$ rank$B$ も成り立ち, これは rank$A =$ rank$B$ を証明する.

正則な小行列 A' が列ベクトル $\boldsymbol{b}$ を含まなければ, たとえ列ベクトル $\boldsymbol{a}$ を含もうと含むまいと $B' = A'$ であり $\det B' =: |B'| = |A'| \neq 0$ は明らかで $B'' = B'$ とすれば良い. A' が $\boldsymbol{a}, \boldsymbol{b}$ 両方とも含めば, $|B'| = |A'| \neq 0$ なので再び $B'' = B'$ でよい. A' が $\boldsymbol{a}$ を含まず $\boldsymbol{b}$ は含む場合でも $|B'| \neq 0$ ならよいので, 残るのは

$$|A'| \neq 0 \text{ が成り立ち, } A' \text{ が } \boldsymbol{a} \text{ を含まず } \boldsymbol{b} \text{ は含み, しかも } |B'| = 0 \text{ となる場合}$$

である. この時 $0 = |B'| = |A'| + c|B''|$ と書ける; B'' は A' の $\boldsymbol{b}$ 列を $\boldsymbol{a}$ 列に置き換えた行列である. $c = 0$ なら $|A'| = 0$ で矛盾だから $c \neq 0$, $|B''| = -|A'|c^{-1} \neq 0$ であり, 小行列 B'' は確かに行列 B から取った $n \times n$ 小行列の 1 つで, 命題は示された. 転置行列で考えて, 行についても同じ結論が得られる事は明らか.

$$(1)\ A \to \begin{pmatrix} 1 & 0 & 4 & 0 \\ 2 & -1 & 3 & 2 \\ 6 & -5 & 1 & -10 \\ -1 & 3 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & -5 & 2 \\ 6 & -5 & -23 & -10 \\ -1 & 3 & 5 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & -5 & 2 \\ 0 & -5 & -23 & -10 \\ 0 & 3 & 5 & 1 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & -5 & 2 & -20 \\ 0 & 3 & -10 & 7 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & -20 \\ 0 & 0 & -10 & 7 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & -20 \\ 0 & 0 & 0 & -93 \end{pmatrix}.$$

故に $\mathrm{rank}A = 4$.

$$(2)\ B \to \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & -2 & 3 & 5 \\ 0 & 2 & -2 & 2 \\ 0 & -4 & -1 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -2 & 3 & 5 \\ 0 & 0 & 1 & 7 \\ 0 & 0 & -7 & -11 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -2 & 3 & 5 \\ 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 48 \end{pmatrix}.$$

故に $\mathrm{rank}B = 4$.

(b) 上の (a) での変形は行や列の割り算も $p = 2$ 或いは 3 倍も含んでいないから, 結果で法 2 或いは法 3 で考えればよい. 法 2 で

$$A \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & -20 \\ 0 & 0 & 0 & -93 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

故に $\mathrm{rank}A = 3 \pmod 2$. 勿論はじめから法 2 で取って計算しても構わない:

$$A \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

同じ結果 $\mathrm{rank}A = 3 \pmod 2$ である. 同様に B の最終形を法 2 で見れば,

$$B \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -2 & 3 & 5 \\ 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 48 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

即ち $\mathrm{rank}B = 2 \pmod 2$ である. 法 3 でも同様で,

$$\mathrm{rank}A = 3 \pmod 3, \quad \mathrm{rank}B = 4 \pmod 3. \qquad \textbf{(問題 6.10. 終り)}$$

問題 6.11. 伏見-手塚の定理の条件を具体的に, text の例の $n = 10,\ m = 5,\ d = 2$ の場合について行列の rank を調べて考えよう. 漸化式 $x_k = x_{k-3} + x_{k-10}$ を用い, p.106 の (a) 図の 5 つの初期値列ベクトル (6.17), 同じページの図 (b) の初期値列ベクトル (6.23) の隣に次の step からの 10 次元列ベクトルをそれぞれ並べて 10×10 行列 A, B を組み上げると,

$$A=\begin{pmatrix}1&0&0&1&0&0&0&0&0&0\\0&0&1&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&1&0&0\\0&0&0&0&0&0&1&0&0&1\\0&0&0&0&0&0&0&0&1&0\\0&1&0&0&0&0&0&0&0&0\\1&0&0&1&0&0&0&0&0&0\\0&0&1&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&1&0&0\\0&1&0&1&0&0&1&0&0&0\end{pmatrix}\quad B=\begin{pmatrix}1&0&0&0&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0&0\\0&0&0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0&0&0\\0&0&0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0&0&0\\0&0&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&0&1&0\\0&1&0&0&0&0&0&0&0&0\end{pmatrix}$$

となる. 明らかに $\mathrm{rank}B=10$ で, Fushimi-Tezuka の定理 6.7. は p.106 の (b) 図を経なくても出発値 (6.23) からの系列

$$\{v_k=0.x_k^{(1)}x_k^{(2)}x_k^{(3)}x_k^{(4)}x_k^{(5)}|\ k\geqq 0\}\tag{6.25}$$

の 2 次均等分布を保証する. A の行, 列の基本変形を行い, 法 2 での $\mathrm{rank}A$ を求め, 行列 A の 1 次従属列ベクトルの個数を求めて, p.106 の (a) 図の内容を説明せよ.

(解) 行列 A の基本変形としては, 例えば次のページにわたる図の様に, 列変形 2 回から始める事もできる; 最後は行の変形とそれらの交換による pivoting である. $\boldsymbol{Z}_2$ で $\mathrm{rank}A=7$ であり, 例えば第 3 番目の行列から見て A の第 6,7,8 列ベクトルは他の列に 1 次従属である. 定理 6.7 はこれらが他の列によっていつも値を決定されていて, 独立な場合の各列の 0 倍或いは 1 倍を取る 2 自由度, 全体で $2^3=8$ の自由度が失われていると示唆する. 実際, 図 (a) によれば, (v_k,v_{k+1}) の各実現には 10 連の 1024 個ではなくその $1/8=1/2^3$ の 128 の自由度しかない. Bright-Enison の定理 6.6. によってこの場合も v_k は 1 次均等分布をしている; 実

$$A\to\begin{pmatrix}1&0&0&1&0&0&0&0&0&0\\0&0&1&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&1&0&0\\0&0&0&0&0&0&1&0&0&1\\0&0&0&0&0&0&0&0&1&0\\0&1&0&0&0&0&0&0&0&0\\1&0&0&1&0&0&0&0&0&0\\0&0&1&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&1&0&0\\0&1&0&1&0&0&1&0&0&0\end{pmatrix}\to\begin{pmatrix}1&0&0&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0&0&0\\0&0&0&0&0&0&1&0&0&1\\0&0&0&0&0&0&0&0&1&0\\0&1&0&0&0&0&0&0&0&0\\1&0&0&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0&0&0\\0&1&0&1&0&0&1&0&0&0\end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&0&0&1&0\\ 0&1&0&0&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&0 \end{pmatrix} \rightarrow \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&0&0&1 \end{pmatrix}$$

際, 図 (a) の横軸の 32 個の値の上にはすべてドットがある. しかし平面内の点の総数 128 と可能な点の総数 1024 から見れば, 各点が 8 回ずつ, 但し (00000) は 1 度少なく, 打たれていると判明する. **(問題 6.11. 終り)**

問題 6.12.(a) $\boldsymbol{Z}_2$ 上の 4 次原始多項式 $f(z) = z^4 + z^3 + 1$ の与える漸化式

$$x_k = x_{k-1} + x_{k-4} \pmod 2, \quad k = 4, 5, \cdots$$

が作る $\boldsymbol{Z}_2$M 系列の周期は $T = 2^4 - 1 = 15$ だった. $x_0 = x_1 = x_2 = x_3 = 1$ を出発値とする M 系列 $\{x_0, x_1, x_2, x_3, \cdots, x_{13}, x_{14}\}$ と, 違う出発値, 同じ漸化式の M 系列 $\{y_0 = x_4, y_1 = x_5, \cdots, y_{13} = x_{17} = x_2, y_{14} = x_3\}$ とは次で与えられる:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x_k	1	1	1	1	0	1	0	1	1	0	0	1	0	0	0
y_k	0	1	0	1	1	0	0	1	0	0	0	1	1	1	1

2 ビットの小数列 $v_k = 0.x_k y_k$ を作るのに, Fushimi-Tezuka の定理を適用してその分布の均等性を調べよう. 出発値の 4 次列ベクトルとそれを 1 ステップずらしたものを付加した下の 4×4 行列を作り, そのランクを調べて, v_k が 2 次均等分布かどうかを判定せよ.

(解)

$$A = \begin{pmatrix} x_0&x_1&y_0&y_1\\ x_1&x_2&y_1&y_2\\ x_2&x_3&y_2&y_3\\ x_3&x_4&y_3&y_4 \end{pmatrix} = \begin{pmatrix} 1&1&0&1\\ 1&1&1&0\\ 1&1&0&1\\ 1&0&1&1 \end{pmatrix} \rightarrow \begin{pmatrix} 1&0&0&0\\ 1&0&1&1\\ 1&0&0&0\\ 1&1&1&0 \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1&0&0&0\\ 0&0&0&1\\ 0&0&0&0\\ 0&1&1&0 \end{pmatrix} \rightarrow \begin{pmatrix} 1&0&0&0\\ 0&0&0&1\\ 0&0&0&0\\ 0&1&0&0 \end{pmatrix} \rightarrow \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&0\\ 0&0&0&1 \end{pmatrix}$$

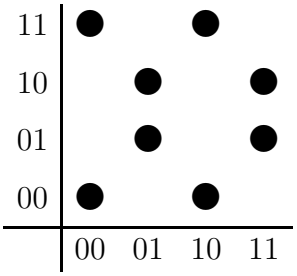
故に $\mathrm{rank} A = 3$, 2 次均等分布しない. **(問題 6.12.(a) 終り)**

問題 6.12.(b) 上の $\{x_1, x_2, x_3, \cdots, x_{13}, x_{14}\}$, $\{y_0, y_1, y_2, \cdots, y_{13}, y_{14}\}$ が作る 2 ビット小数列 $v_k = 0.x_k y_k$ の小数, その値は

$$.00_{(2)} = 0, \quad .01_{(2)} = 0.25, \quad .10_{(2)} = .5, \quad .11_{(2)} = .75,$$

の列 $\{v_0, v_1, \cdots, v_{15}, v_{16} = v_0\}$ の Marsaglia 図を描いて, 問題 6.12.(a) の結論を確かめよ.

(解) Marsaglia 図は次の通り:



点 $(00, 00)$ は 1 度, 他の点はそれぞれ 2 度現れている. 確かに, この連結 M 系列は 2 次均等分布しない. **(問題 6.12.(b) 終り)**

問題 6.12.(c) $\boldsymbol{Z}_2$ 上の 4 次原始多項式 $f(z) = z^4 + z^3 + 1$ の与える漸化式

$$x_k = x_{k-1} + x_{k-4} \pmod 2, \quad k = 4, 5, \cdots$$

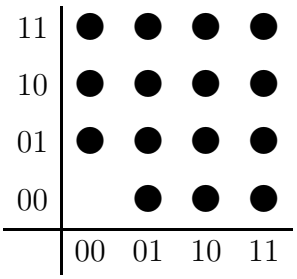
が生成する $\boldsymbol{Z}_2$M 系列 $\{x_0, x_1, x_2, x_3, \cdots, x_{13}, x_{14}\}$, , $\{y_0, y_1, y_2, \cdots, y_{13}, y_{14}\}$ が作る 2 進小数列 $v_k = 0.x_k y_k$ が 2 次均等分布をするよう, 初期値 $\{x_0, x_1, x_2, x_3\}$, $\{y_0, y_1, y_2, y_3\}$ を Fushimi-Tezuka の定理に基づいて 1 組設計せよ. また 2 進 2 桁の小数 $\{v_0, v_1, \cdots, v_{15}, v_{16} = v_0\}$ の 2 次元 Marsaglia 図を描いて, 2 次均等分布を確かめよ.
(解) 乱数列の性質は問わないなら, できるだけ 1 の少ない初期値が設計には楽で, 例えば

$$B = \begin{pmatrix} x_0 & x_1 & y_0 & y_1 \\ x_1 & x_2 & y_1 & y_2 \\ x_2 & x_3 & y_2 & y_3 \\ x_3 & x_4 & y_3 & y_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

なら明らかに $\mathrm{rank} B = 4$ である. 実際 M 系列 $\{x_k, y_k\}$ を作り, $v_k = .x_k y_k$ を読む:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x_k	1	0	0	0	1	1	1	1	0	1	0	1	1	0	0
y_k	0	0	1	0	0	0	1	1	1	1	0	1	0	1	1

Marsaglia 図は次の通り 2 次均等分布を保証する:



(問題 6.12.(c) 終り)

7. 乱数の加算生成法と算術演算的方法

7.1. まえおき: 法 p^r の加算生成法と整数の環

加算生成法 (lagged Fibonacci 法, 遅れ lag させられたフィボナッチ法, とよく呼ばれる) は次の方式で乱数系列を発生する:

$$x_k = x_{k-p} + x_{k-q} \pmod m, \quad m = 2^r, \quad 0 < p < q. \tag{7.1}$$

整数全体を $\boldsymbol{Z}$, 法 2^r での整数の体系を $\boldsymbol{Z}/2^r$ と書く約束を再確認する. 「乱数の乗算合同法: 法 2^r の場合」でも見た通り, $r \geqq 2$ に対し $\boldsymbol{Z}/2^r$ の 0 以外の数の全体は乗法で閉じないから乗法群を作れず,[69] $\boldsymbol{Z}/2^r$ は体ではない. 乗法群を作るのは 2^r とは素な (2^r と共通因数がない, 即ち 2 を素因数に持たない) 奇数の全体が作る既約剰余群 $\boldsymbol{Z}^*_{2^r} \subset \boldsymbol{Z}/2^r$ だった.

考えを進める上では (7.1) はもっと一般に

$$x_k = b_1 x_{k-1} + b_2 x_{k-2} + \cdots + b_n x_{k-n} \pmod{2^r}, \quad b_1, b_2, \cdots, b_n \in \boldsymbol{Z}/2^r,$$

の形に取って困難はないから以下この形を考え, $n \geqq 2$ と常に仮定する. 更に言うと, 法 2^r は最も実際的に大切だが, この法への議論の限定は問題の一般性を隠すので, 我々は以下, 任意の素数 p と整数 $r \geqq 2$ に対する法 p^r の加算生成法の n 次線形漸化式

$$x_k = b_1 x_{k-1} + b_2 x_{k-2} + \cdots + b_n x_{k-n} \pmod{p^r}, \quad b_1, b_2, \cdots, b_n \in \boldsymbol{Z}/p^r, \tag{7.2}$$

を考える. 係数 b_n には係数体 F 或いは $\boldsymbol{Z}_p$ の中で 0 ではない, という前章までの制限に似た条件を課す. この問題の解析には Marsaglia と Tsay[14] の与えた行列に基づく法 2^r での定式化があり, 一方ずっと古く Ward[49] が非常に一般の法 $m = p^r (p')^{r'} (p'')^{r''} \cdots$ で与えた結果があり,[70] そして最近 Brent[50] が法 2^r で導いた端的で重要な最長周期判定条件がある. この章の主目的はこの Brent の結果の伝達である. この章のもう 1 つの目的は, 今までの我々の議論には登場しなかった乱数問題での他の有力な方法, 算術演算的 arithmetic と呼ばれるもの, の 1 概観を Ward の結果の導出も兼ねて提示する事にある. M 系列法までに限れば前章までの群や体の議論を経る方が視点が明確で応用も広いと思われる. しかし算術演算的な方法はその様な見方ができない場合についても, 議論は抽象的で (「見えた」という理解の意味での) 視覚化は中々難しいが, 端的強力な結論を与える事が見られるだろう.

法 p^r の乗算合同法では勿論 a は素因数 p を含んではならず, 乗数 a は最大位数の元に取られ, 既約剰余群 $\boldsymbol{Z}^*_{p^r}$ の元であり, 乱数のための漸化式解系列 $\{a^k x_0\}$ は実際上 $\boldsymbol{Z}^*_{p^r}$ の中だけを動いた. しかし $r \geqq 2$ に対し法 p^r で (7.2) の結果を考える場合には, 係数 $b_1, b_2, \cdots, b_{n-1}$ が素数 p の異なる因数を含めば結果も異なる. だから考察を p と素な数の集合 $\boldsymbol{Z}^*_{p^r}$ だけに限る事はできず, p の低次因数も含む $\boldsymbol{Z}/p^r$ で考える必要がある. 数学的には $r > 1$ での法 p^r では数の集合 $\boldsymbol{Z}/p^r$ は可換環 commutative ring と呼ばれるもの [35),37),39),17),18),51)] になる. 但し整数の素因数分解や多項式の既約分解の一意性の議論 (次章) を除いて, 我々は環の詳細な性質を用いる必要には余り出会わないが, 体との違いを把握し環構造を明確に認識する事は大切

[69] 偶数 $a = 2b < 2^r$ は $a \neq 0 \pmod{2^r}$ で $\boldsymbol{Z}/2^r - \{0\}$ に属すが, 十分大きい k に対し $a^k \equiv 0 \pmod{2^r}$.
[70] 今迄通り $p, p', p'', \cdots$ は素数 prime を表すとする.

だから, 幾つかの特記すべき事柄にここから少しずつ触れる.

環 R は体と同様に加法 $+$ と乗法 $\times = \cdot$ を持つ[71]集合である. 但し体の公理のうち乗法について群を作る事は求めない.[72] 環には乗法が可換な「可換環」と, 典型的には行列の様にそれが可換ではないものとがある. しかし乱数に限れば非可換性は考えなくても済むので, 以下何よりも簡単さを求めて可換環だけを考え, それだけを単に環と呼ぶ. 環は次の公理系で定義される:

可換環の公理 7.1. 環 R は次の公理 1, 2 を満たす集合を言う.
(公理 1) R の任意の元 $x, y, \cdots$ の間には加法 $x+y$ と可換な乗法 $x \cdot y = xy = yx$ が定義されていて, 次の結合法則と分配法則が成り立つ:

$$(x+y)+z = x+(y+z), \quad (xy)z = x(yz), \quad \text{(結合法則)}$$

$$(x+y)z = xz+yz, \quad x(y+z) = xy+xz. \quad \text{(分配法則)}$$

(公理 2) 加法について R はそのある元 0 を単位元とする群であり, 加法の逆演算である減法 $-$ も定義される. 乗法については $R-\{0\}$ には群である事を求めない. **(環の公理終り)**

次の (a)–(d) は, それぞれ加減法と乗法が可能な環である事は自明だが, 重要な例である:

例 7.2. (a) 体はその加法と乗法に関して環でもある.
(b) 整数の全体 $\boldsymbol{Z}$ は通常の加減法 $\pm$ と乗法 $\times$ に関して環である. 零元は 0, 乗法の単位元は 1 である.
(c) 任意の正の整数 m に対して, 整数の法 m での剰余類の全体 $\boldsymbol{Z}/m = \{0, 1, \cdots, m-1\}$ も法 m での加減法, 乗法に関して環である.
(d) 任意の (可換) 環 R を係数に持ち, R の元と同じ計算規則に従う文字 z の多項式の全体を $R[z]$ と記す. 整式の加法, 乗法に関して, $R[z]$ は環であり, その 0 元は定数関数 $f(z) = 0$, 乗法の単位元は定数関数 $f(z) = 1$, 1 は環 R の乗法の単位元, である. 具体的には
(d1) 整数係数多項式の全体 $\boldsymbol{Z}[z]$,
(d2) 任意の整数 $m > 0$ を法とする整数の環 $R = \boldsymbol{Z}/m$ を係数とする多項式の全体 $R[z]$,
(d3) 或いは任意の体 F を係数に持つ多項式の全体 $F[z]$
は環である. **(例 7.2 終り)**

我々は以前に素数でない法 m を持つ数を係数とする多項式ではその根や因数分解について通常のイメージとは掛け離れた演算結果が多く生じる事, それが体係数では簡潔整然とまとまる事, をそれぞれ見た. 環の与えるこの様な姿は非常に複雑で, 一般状況には第 8 章での少しの記述以外は踏み入れないが, ここでは最小限として環でのある事情を確かめて言葉を準備し, 我々の既に持つ知識に関連付けて進む:

Lemma 7.3. 環 R の元 x が可逆元 invertible element[73]であるとは, x が乗法に関して逆元 x^{-1}, 即ち $x \cdot x^{-1} = 1$ となる $x^{-1} \in R$ が存在する事を言う.
(a) 環 R の可逆元の全体 U は乗法で群を作る.
(b) 特に任意の整数 $m > 0$ に対する環 $R = \boldsymbol{Z}/m$ では, その可逆元の全体 U は既約剰余群 $\boldsymbol{Z}_m^*$, m と素な (m と共通な素因数を持たない) 整数の全体が法 m の乗法で作る群, である.

[71]環の元 x, y の積は特に紛らわしくない限り $x \times y = x \cdot y$ を xy と略記する.
[72]だから特に, 環には 1 が含まれない事も可能だが, 我々は 1 を含む環だけを考える.
[73]正則元 regular element, 或いは単元 unit とも言う.

(証明) (a) 群の公理の成立を確かめれば良い. $x, y, \cdots \in U$ を任意に取る.
(公理 3, 0) $x \in U$ であれば逆元 $x^{-1} \in R$ があり, $xx^{-1} = x^{-1}x = 1$ から明らかに x^{-1} の逆元 $(x^{-1})^{-1}$ は $x \in R$ である. 故にまず任意の $x \in U$ に対して $x^{-1} \in R$ は可逆で, $x^{-1} \in U$(公理 3) が成り立つ. 環 R での乗法に関する結合法則と乗法の可換性から

$$(xy)(x^{-1}y^{-1}) = (xx^{-1})(yy^{-1}) = 1{\cdot}1 = 1,$$

即ち xy は逆元を持ち $xy \in U$ が成り立って U は (環の) 乗法で閉じている (公理 0 の成立).
(公理 1) 環 R では乗法の結合法則が成り立つから, 部分集合 $U{\subset}R$ でも乗法の結合法則は成り立つ.
(公理 2) $1{\cdot}1 = 1$ から $1 \in R$ も可逆元で $1 \in U$, U は乗法の単位元を含む.
(b) m が素数 p なら $\boldsymbol{Z}/m = \boldsymbol{Z}_p$ であり, 0 以外はすべて逆数を持つ可逆元で乗法の群 $\boldsymbol{Z}_p^* = \{1, 2, \cdots, p-1\}$ を作る, と示されているので議論の必要はない. m が合成数の場合を考え, p をその 1 つの素因数とする. 環 $\boldsymbol{Z}/m$ の可逆元 x に対しては, $x{\cdot}x^{-1} \equiv 1 \pmod{m}$, 即ち

$$x{\cdot}x^{-1} = 1 + cm = 1 + dp, \quad c, d \text{ は整数},$$

なのだから x は m の素因数 p を含めない; 含めば上の式左辺は p で割り切れ, 右辺は割り切れない矛盾になるからである. 故に $x \in \boldsymbol{Z}_m^*$ であり, $U{\subset}\boldsymbol{Z}_m^*$ が成り立つ. 逆に $\boldsymbol{Z}_m^*$ は法 m の乗法で群であり, その任意の数 (m と共通素因数を持たないつまり m と素な数)x が $xy = 1 \pmod{m}$ となる逆数 $y \in \boldsymbol{Z}_m^*$ を持つ事は既に p.24, 問題 2.7. で示されている. 故に逆の包含関係 $\boldsymbol{Z}_m^* \subset U$ も成り立ち, 実は $U = \boldsymbol{Z}_m^*$ である. ■

得られた言葉を早速用いて, 議論で本質的でない複雑化を避けるための条件, 限定を述べる. 以下漸化式

$$x_k = b_1x_{k-1} + b_2x_{k-2} + \cdots + b_nx_{k-n} \pmod{p^r}, \quad b_1, b_2, \cdots, b_n \in \boldsymbol{Z}/p^r, \qquad (7.2)$$

で係数 b_n は法 p^r で可逆, 即ち素因数 p を持たない数だと常に仮定する. さらに

系列を決定する出発の n 連 $\{x_0, x_1, \cdots, x_{n-1}\}$ は法 p で零連ではない

と常に限定する. 最初の仮定によって (7.2) は, b_n の逆数 b_n^{-1} を掛けて

$$x_{k-n} = -c_{n-1}x_{k-n+1} - c_{n-2}x_{k-n+2} - \cdots - c_1x_{k-1} + b_n^{-1}x_k \pmod{p^r},$$
$$c_j = b_n^{-1}b_j, \quad 1 \leqq j \leqq n-1 \qquad (7.3)$$

と x_{k-n} について解けて系列は逆行可能である事が知られる. だから (必要なら) 漸化式の解系列 $\{x_k\}$ は (7.2), (7.3) によって $-\infty < k < \infty$ で定義されていると考えてもよい. また, 法 p で零ベクトルの n 連 $\{x_k, x_{k+1}, \cdots, x_{k+n-1}\}$ があれば線形漸化式 (7.2) 或いはその逆行によって解系列のすべての n 連は法 p で零ベクトルになるから, 第 2 の限定の下では

(7.2) の解系列には法 p での (従って法 p^r での)0 の n 連は決して現れない.

加算生成法の全体的構造の概観へ向い, それに基づいて方法の乱数問題での位置を考えよう. 我々はなぜ原始根が存在するか, M 系列を与える原始多項式は一体何か, を考えて来た. 加算生成法の基礎構造は何か, 周期は何か, その周期はなぜ得られるのか, を当然問うべきである. M 系列の理解に立てば定性的には答は誠に単純で, 加算生成法は

M 系列に加算に伴う繰り上がり carry を切り混ぜ shuffling 機構として加えたもの

に過ぎない. 実際漸化式 (7.2) の解系列 $\{x_k\}$ は 0 から p^r-1 までの数の列で, p 進数で表せば各 x_k の桁数 $\log_p x_k+1$ は高々r である. その p 進表現を

$$x_k = y_k^{(r-1)} y_k^{(r-2)} \cdots y_k^{(1)} y_k^{(0)}$$

と置こう. $0 \leqq y_k^{(j)} \leqq p-1$ は p^j の桁の数値を表す. p 進最下位の $y_k^{(0)} \equiv x_k \pmod p$ は次の漸化式に従う:

$$y_k^{(0)} = b_1 y_{k-1}^{(0)} + b_2 y_{k-2}^{(0)} + \cdots + b_n y_{k-n}^{(0)} \pmod p, \quad b_1, b_2, \cdots, b_n \in \boldsymbol{Z}/p^r. \qquad (7.4)$$

係数 $\{b_k\}$ はこの式 (7.4) の中では $\boldsymbol{Z}_p$ の元と見てもよく, (7.4) は第 6 節で見た方式で, その理論的最長周期は特性多項式

$$f(z) = z^n - b_1 z^{n-1} - \cdots - b_n z^0, \quad b_k\text{は法 } p^r\text{での可逆元}, \qquad (7.5)$$

が $\boldsymbol{Z}_p$ 上の n 次原始多項式である M 系列の場合の p^n-1 である. 系列 $\{x_k\}$ の周期は常にこの最下位桁の周期の倍数だし, M 系列の周期が出発値によらない性質は乱数機構には必須だから, 以下特に断らない限り $f(z)$ は法 p での原始多項式, 法 p で $\{y_k^{(0)}\}$ は周期 p^n-1 とする.

x_k の p 進下 2 桁目 $y_k^{(1)}$ を考えよう. $y_k^{(1)}$ に対する漸化式は (7.4) と同じ法 p での漸化式に従う部分の他に $\{y_k^{(0)}\}$ の普通の加法 $b_1 y_{k-1}^{(0)} + \cdots + b_n y_{k-n}^{(0)}$ からの p^1 への繰り上がり $w_k^{(1)}$ が加わった法 p での和:

$$y_k^{(1)} = b_1 y_{k-1}^{(1)} + b_2 y_{k-2}^{(1)} + \cdots + b_n y_{k-n}^{(1)} + w_k^{(1)} \pmod p, \qquad (7.6)$$

で作られる. 最下位桁 $\{y_k^{(0)}\}$ が周期 p^n-1 だから繰り上がり $w_k^{(1)}$ も同周期で, どんな場合でもこれを p 回繰返せば下 2 桁目への繰り上がり総計は p の倍数となって効果が消える. 故に p 進下 2 桁の可能な最長周期は $p^{2-1}(p^n-1) = p(p^n-1)$ である. また同じ議論が p 進下 j 桁の $y_k^{(j)}$ への $y_k^{(j-1)}$ からの繰り上がり carry でも成り立って, 法 p^r での最上桁, 第 r 桁, を含む可能な最長周期は $p^{r-1}(p^n-1)$ である.

我々は殆ど加算生成法の全体像に達した. 透視は乱数生成方式の中での位置付けも明確にする. 加算生成法 (lagged Fibonacci 法) は既知の簡単な方法の中で単独で最長周期を与え, 一部で (特に M 系列法との対比で) 飛び抜けて優れたものと断定された事もある. しかしこれは必ずしも当らないと思われる. 困難は方式の設計にある. 一般に言って加算生成法乱数は平均的に悪くない性質を保証されている様に見えるが, 他のすべての方式と同様に**任意の出発値に対して任意に選ばれた最長周期乱数加算生成方式が常に優れたものであるという保証はない**. だからその使用に際しては多くの選択が必要となり, 「原理的性質, 美点も欠点も, が共に明らかでない」という方式の難点, 即ち「出発値や生成方式をどの様に選べばよいか, 設計すれば最もよい性質となるか」がわからないという難問に突き当たる.[45] 周期は非常に長く, 例えば 2^{500} 以上は普通だから, 以前に別の文脈で述べたように全周期にわたる検定は不可能である. 当然方式の選択は乱数系列の 1 部分についての統計的検定に依拠するしか考えられないが, 他の方式の乱数系列同様にどれだけの部分のどれだけの検定が十分な性能を保証するのかは明確ではない. 原理的な性能保証の欠落はこの様な長周期乱数については大変大きな困難である. 実際のシミュレーションでは, だから, 加算生成法乱数を採用するとすれば

「他の simulation で用いてよい結果を得た方式選択をそのまま用いてみる」

事が実際的な殆ど唯一の選択肢になる. しかし原理的性質の不明な乱数方式がいくつか検

定, 使用に合格してもそれだけで良いと考える危険はしばしば注意される所である.

この意味で最近の加算生成法の原理的な性能改善提案[13),52)]は注目に値する. 大まかに言って, それは方式の与える長い周期を利用し, いわば「十分切り混ぜ shuffling を利かせる」様に加算生成法から大きな間隔を置いた部分系列を抜き出して利用する事に当たる. 勿論生成速度の低下[53)]と引き換えの性能向上策であり, また shuffling 自体に依然一般論, 理論的見通しが余りないという事情からも特定の漸化式と初期条件の場合どれだけ間隔を空ければ十分な性能が得られるか, についてはやはり多くの応用と経験を積み重ね, 洞察を得なければならないが, 提案で与えられた展望は重要で十分な検討に値するものと思われ, 実際にこれからも多くの応用やそれに基づく評価がなされる事になるだろう.

理論的に容易に透視できる事が多くはない中で, 加算生成法の周期構造については遥か以前の Ward[49)] から非常に一般的な解析結果が存在する. 考えるべき問題は,

$$\text{法 } p^r \text{ で最長の周期 } p^{r-1}(p^n-1) \text{ を保証する法 } p \text{ での原始多項式}$$
$$f(z) \text{ の特徴付けとそれを与える出発値 } \{x_0, x_1, \cdots, x_{n-1}\} \text{ の指定}$$

である. Brent[50)] はこの問題を法 2^r に限って, 大変簡潔強力な解を与えた. 彼の解析は Ward の一般の素数 p に対する法 p^r での結果を経る事も必要としないものだけれど, Brent の結果自体の素晴らしさを理解し, 問題の一般構造や既にのべた算術演算的方法へも視野を深めるには Ward の結果の理解から始める方がよい. 我々はこれを次の節で行い, Brent の方法と結果とは 7.3 節に提示する. 差し当たってさらに 1 つ, 以下の問題に必要な環の性質を付言して, 次の節からの準備としよう.

線形漸化式 (7.2) の特性多項式は (7.5) は係数を法 $m = p^r$ で同定する. それは法 m での整数の環 $R = \boldsymbol{Z}/m$ 係数の文字 z の多項式の全体 $R[z]$ を考える事である. 我々はこのような多項式全体をさらに特性多項式 $f(z)$ を法として見なければならない. 次の定義を置く:

定義 7.4. 整数係数多項式 $a(z), b(z)$ について

$$a(z) = b(z) + f(z)u(z) + mv(z)$$

となる整数係数多項式 $u(z), v(z)$ があるとき,

$$a(z) \equiv b(z) \mod (m, f(z)) \tag{7.7}$$

と記し,「法 $(m, f(z))$ で多項式 $a(z)$ と $b(z)$ は合同」と記述する. **(定義 7.4. 終り)**

$f(z)$ がどのような $R = \boldsymbol{Z}/m$ 係数多項式でも法 $(m, f(z))$ での同値関係は定義できるが, $f(z)$ の最高次の項の係数が法 m で可逆でないと一般に $f(z)$ による他の整数係数多項式の割り算が行えない. 割り算できなくても定義として困る事はない.[74] しかしこの様な複雑な場合は我々には必要ないので, 以下では

法となる多項式 $f(z)$ の最高次 $n \geqq 1$ 次の係数は法 m で可逆である

と限定して事柄を視覚化する.[75] 故にある整数係数多項式 $a(z)$ が法 $(m, f(z))$ で 0 かどうか

[74]多項式因数への分解が一意でなくても, 既約かどうか, 或いはある任意の多項式 $f(z)$ を因数に含むか含まないか, は 2 者択一で不明確なしに定まる. また疑似除算 pseudo-division を用いる事もできる.[54)]

[75]以下の議論の興味の中心はモニックな法多項式 $f(z)$ だから細かく言わなくてもよい事も多いが, 最高次係数が 1 ではないものを含める必要にも出会う.

を調べるには, $a(z)$ を $f(z)$ で法 m で割り算して $f(z)$ より低次に残る余りが 0 かどうかを調べればよい. 任意の整数 m を法とする合同算法で見た様に, 法 $(m, f(z))$ での簡約も四則算法のどの段階で行っても, そして何回行っても結果は同じである.

この同値関係で分類した整数係数多項式の全体を $\boldsymbol{Z}[z]/(m, f(z))$ とも記す. $\boldsymbol{Z}[z]/(m, f(z))$ は明らかに加法について群を作り, 乗法も可能な環である. 我々は主として $m = p^r$ と取る. $r = 1$ で法 m が素数 p, そして $f(z)$ が $\boldsymbol{Z}/m = \boldsymbol{Z}_p$ 係数の既約多項式なら, 前章までで見た様に (7.7) は「$f(z) = 0$ の根 i を体 $\boldsymbol{Z}_p$ に添加した n 次拡大体での元 $a(i)$ と $b(i)$ が等しい」, という内容だったが, 以下では一般に $r = 1$ とも, そして暫くは $f(z)$ が既約とも制限しないからこの様な意味は考えない. ただ, 任意の整数係数多項式 $g(z)$ を法 $(m = p^r, f(z))$ の環で考えるのに同時に法 p での体 $\boldsymbol{Z}_p$ 係数の多項式として視る事はしばしば重要になる. 実際法 $(m = p^r, f(z))$ 整数係数多項式の環 $\boldsymbol{Z}[z]/(m, f(z))$ の可逆元は次の特長付けができる:

定理 7.5. (Hensel の lemma) 素数 p の r 乗の $m = p^r$ と (7.5) の $f(z)$ とを法とする整数係数多項式の環 $\boldsymbol{Z}[z]/(m, f(z))$ の元 $g(z)$ が可逆である必要十分条件は次で与えられる:

法 p での整数の体 $\boldsymbol{Z}_p$ 係数の多項式と見て $g(z)$ は $f(z)$ と素,
即ち $g(z)$ は $f(z)$ と共通な $\boldsymbol{Z}_p$ 係数多項式因数を持たない.

(証明) (必要性) 法 $(m, f(z))$ で $h(z)$ が可逆なら,

$$g(z)u(z) = 1 + p^r k(z) + f(z)v(z)$$

となる整数係数多項式 $u(z),\ v(z),\ k(z)$ が存在する. 故に法 p で見て

$$g(z)u(z) - f(z)v(z) \equiv 1 \pmod{p}$$

が成り立つ. $g(z)$ と $f(z)$ に共通な $\boldsymbol{Z}_p$ 係数多項式因数は右辺の 1 を割り切るものに限られ, 体 $\boldsymbol{Z}_p$ の 0 ではない定数以外あり得ない. 故に $g(z)$ と $f(z)$ とは $\boldsymbol{Z}_p$ 係数で互いに素である.
(十分性)[76] 法 p で $g(z)$ と $f(z)$ が互いに素と仮定する. $\boldsymbol{Z}_p$ は体であり, その 0 以外の任意の数が逆数を持つ. 故に $g(z)$ と $f(z)$ の低次のもの, 例えば $g(z)$ で他方を割って一意な除法等式

$$f(z) = g(z)q(z) + r(z), \quad q(z) \text{ は商, } r(z) \text{ は次数が } g(z) \text{ より低い余り},$$

が得られる. これは $g(z)$ と $r(z)$ との任意の公約数は $f(z)$ を割り切る約数でもあって $f(z)$ と $g(z)$ との公約数に含まれる事を意味し, この変形 $f(z) - g(z)q(z) = r(z)$ は $f(z)$ と $g(z)$ の公約数がすべて $r(z)$ の約数にもなって $g(z)$ と $r(z)$ の公約数に含まれる事を意味する. $g(z)$ と $r(z)$ の公約数全体は $f(z)$ と $r(z)$ の公約数全体と一致する. 故に $f(z)$ と $g(z)$ の最大次共通因数, $\boldsymbol{Z}_p$ 係数での最大公約数 $d(z) = \mathrm{GCD}(f(z), g(z)) = \mathrm{GCD}(f, g)$, は $g(z)$ とそれよりは低次の $r(z)$ との最大公約数 $\mathrm{GCD}(g, r)$ として求められ, また割り算の余り $r(z)$ は上の通り $f(z)$ と $g(z)$ の 1 次結合 $f(z) - g(z)q(z)$ で表される. 同様に $\mathrm{GCD}(g, r)$ を求めるには $g(z)$ を $r(z)$ で $\boldsymbol{Z}_p$ の計算で割って

$$g(z) = r(z)q'(z) + r'(z), \quad q'(z) \text{ は商, } r'(z) \text{ は次数が } r(z) \text{ より低い余り},$$

と計算し, $\mathrm{GDC}(r, r')$ の計算に移せばよい. また $r'(z) = g(z) - r(z)q'(z) = -f(z)q'(z) + g(z)\{1 + q(z)q'(z)\}$ となって余り $r'(z)$ が再び $g(z)$ と $f(z)$ の一次結合で表される. よく知られたユークリッドの互除法のこの原理は体 $\boldsymbol{Z}_p$ 係数で何度でも反復使用できて, 最後に余り

[76] 下の議論は体を係数に持つ多項式の一般性質として次の章でも統一的な立場から見られる.

として最大公約数 $d(z)$ そのものが出るまで, 次の段階で余り 0 になるまで続けられる. またその際に得られる最大公約数 $d(z)$ は整数係数多項式を係数とする $f(z)$ と $g(z)$ の 1 次結合で表現される. 現在の $g(z)$, $f(z)$ の最大公約数は (${\boldsymbol Z}_p{}^*$ の適当な逆数を掛けて)1 なのだから,

$$g(z)u(z)+f(z)v(z)=1+pk(z)\quad(\equiv 1\pmod p) \tag{7.8}$$

となる整数係数多項式 $u(z),\ v(z),\ k(z)$ が存在する. この式に $pk(z)$ をかけた

$$\{g(z)u(z)+f(z)v(z)\}pk(z)=pk(z)+p^2k^2(z)$$

を (7.8) の両辺から引くと,

$$u(z)\{1-pk(z)\}g(z)+v(z)\{1-pk(z)\}f(z)=1-p^2k^2(z).$$

故に $u_1(z):=u(z)\{1-pk(z)\},\ v_1(z):=v(z)\{1-pk(z)\}$ と置けば次が得られる:

$$u_1(z)g(z)+v_1(z)f(z)=1-p^2k^2(z)\equiv 1\pmod{p^2}.$$

p の次数を高めるこの手続き (Hensel) は明らかに何回でも行えて, すべての $r\geqq 1$ に対して

$$u_r(z)g(z)+v_r(z)f(z)\equiv 1\pmod{p^r}$$

となる整数係数多項式列 $\{u_r(z),v_r(z)\}$ があり

$$u_r(z)g(z)\equiv 1\mod(p^r,f(z)).$$

これは各 $r\geqq 1$ に対して法 $(p^r,f(z))$ で $g^{-1}(z)=u_r(z)$ である事, 即ち ${\boldsymbol Z}[z]/(p^r,f(z))$ で $g(z)$ が可逆である事を意味する. ■

7.2. 一般の法 p^r の加算生成法と算術演算的方法: Ward の最長周期条件

乱数の加算生成法に立ち戻って算術演算的方法の一般的理解を目指し, また Brent の証明解読の準備も兼ねて, Brent[50] が与えた方法で Ward[49] の結果の 1 部, 法 p^r での最長周期条件, を再導出しよう. まず天下りに任意の環の上の無限列 $\{x_k|\ k=0,1,2,\cdots\}$ を考える; 具体的には漸化式の解系列である. 番号 $j=0,1,2,\cdots$ を固定してすべての番号 $k\geqq j$ に対して $x_k=x_{k+S}$ となる整数 $S\geqq 0$ を「$\{x_k\}$ の j 以後での一般周期」と呼び, その全体を集合 A_j と記そう. 明らかにすべての $j\geqq 0$ に対して常に $0\in A_j$ だが, 数列によっては 0 以外の一般周期は存在せず $A_j=\{0\},\ j=0,1,2,\cdots$ の事もある. しかし次は常に成り立つ:

Corollary 7.6. (a) 集合列 $\{A_0,A_1,\cdots\}$ は増大列, $A_j\subset A_{j+1}$ である.
(b) 任意の番号 $j\geqq 0$ を固定する. 漸化式の解も含め環上の任意の無限列で番号 j 以後の一般周期集合 A_j が正の数を含めば, その正の最小値を T として $A_j=\{qT|\ q=0,1,2,\cdots\}$ の形である.
(c) 任意の番号 $j\geqq 0$ で一般周期集合 A_j が素数 P を含めば P は A_j の正の最小値である. なおこの時すべての $j'\geqq j$ に対し $A_{j'}=A_j=\{qP|\ q=0,1,2,\cdots\}$ が成り立つ.
(証明) (a) A_j の定義から明らかである.

(b) A_j の任意の 2 数 $a, b > 0$ を取り一般性を失わず $a \geqq b$ とする. 任意の $k \geqq j$ に対して

$$x_k = x_{k+a} = x_{k+a+b} = x_{k+(a+b)},$$
$$x_k = x_{k+a} = x_{k+(a-b)+b} = x_{k+(a-b)}, \quad k = 0, 1, 2, \cdots.$$

故に a, b と共に $a+b,\ |a-b| \in A_j$ が成り立つ. A_j の正の最小の数 T については上の事から T のすべての倍数 $qT = T + T + \cdots + T \in A_j$ であり, $\{qT |\ q = 0, 1, 2, \cdots\} \subset A_j$ が成り立つ. 逆の包含関係を示して証明を終えよう. 任意の $a \in A_j$ を取り T で整数の範囲の割り算をすると $a = qT + r,\ 0 \leqq r < T$ と商 q, 余り r が得られるが, qT, a は A_j の数で $r = |a - qT| \in A_j$ であり, T が A_j の正の最小数なのだから $r = 0$ である. 故に A_j の任意の数 a は T の倍数で $A_j \subset \{qT |\ q = 0, 1, 2, \cdots\}$ が成立する.
(c) 上の (a),(b) によって P は $A_{j'}$ の正の最小元 T の倍数だが, 素数の P はそれより小さい因数を含めず $P = T$, $A_{j'} = \{qP |\ q = 0, 1, 2, \cdots\} = A_j$ が成り立つ. ■

上の補題の (b) が任意の数列 $\{x_k |\ k = 0, 1, 2, \cdots\}$ に伴われる一般構造を述べている事は強調に値するが, 限定なしの数列の上での一般周期の様相は複雑である. 例えば法 2^r での系列 $\{x_k |\ k = 0, 1, 2, \cdots\}$ に対する A_0 が一般周期 T を持つとしても, 系列 $y_k := 2^k + x_k \pmod{2^r}$ では番号 r 以後だけに T が一般周期として現れる. だから一般には集合列 $\{A_0, A_1, \cdots\}$ の増大性から極限集合 $A := \lim_{j\to\infty} A_j$ を考え, A の正で最小の「漸近的周期」を取らなければならない. しかし興味は**可逆な定数係数線形漸化式 (7.2) の解系列**にある. この場合状況は遥かに明快である:

Corollary 7.7. 定数係数で可逆な線形漸化式 (7.2) の解系列 $\{x_k |\ k = 0, 1, 2, \cdots\}$ の場合, その一般周期の集合 A_j はすべての j で同一である: $A_0 = A_1 = \cdots = A_j = \cdots$.
(証明) 包含関係 $A_0 \subset A_1 \subset \cdots \subset A_{j-1} \subset A_j \subset \cdots$ は既知だから逆の $A_{j-1} \supset A_j$ を示そう. 任意の $S \in A_j,\ S > 0$ を取る. 漸化式 (7.2) の逆行漸化式 (7.3) は簡単化して

$$x_{j-1} = d_0 x_j + d_1 x_{j+1} + \cdots + d_{n-1} x_{j+n-1},\ j \text{ は任意},$$

の形の表現を持つ. $k \geqq j$ に対して $x_{k+S} = x_k$ なのだから,

$$\begin{aligned} x_{j-1+S} &= d_0 x_{j+S} + d_1 x_{j+S+1} + \cdots + d_{n-1} x_{j+n-1+S} \\ &= d_0 x_j + d_1 x_{j+1} + \cdots + d_{n-1} x_{j+n-1} = x_{j-1}. \end{aligned}$$

故に $S \in A_{j-1}$ であり, $A_{j-1} \supset A_j$ が, 従って $A_{j-1} = A_j$ が示された. ■

以下, 我々はつねに Corollary 7.7. の成り立つ状況の中で動く. 次は Corollary 7.6.(b) とよく似た構造である:

Corollary 7.8. 任意の整数 $m > 0$ と $f(z) \in \boldsymbol{Z}[z]/m$ を取り,

$$z^a - 1 \equiv 0, \quad \text{即ち } z^a \equiv 1 \pmod{(m, f(z))}$$

の成り立つ整数 $a \geqq 0$ の全体を集合 B とする. もし B が正の数を含めば, B の正の最小値を P として次が成り立つ: $B = \{qP |\ q = 0, 1, 2, \cdots\}$.

(証明) B の任意の数 $a > 0$ を取れば $a \geqq P$ である. P で割り算をして $a = qP + r$, $q \geqq 0$ は整数の商, $0 \leqq r < P$ は整数の余りと置くと,

$$1 \equiv z^a = z^{r+qP} = z^{r+(q-1)P+P} \equiv z^{r+(q-1)P} \equiv \cdots \equiv z^r.$$

これは $r \in B$ を意味し, P の正の最小性から $r = 0$ でなければならない. 故に B の任意数 a は $a = qP$ の形であり, $B \subset \{qP|\ q = 0, 1, 2, \cdots\}$ である. 逆に任意の整数 $q \geqq 0$ に対して $qP \in B$, 即ち $\{qP|\ q = 0, 1, 2, \cdots\} \subset B$ は上の Corollary 7.6.(b) の証明と同様に明らかで $B = \{qP|\ q = 0, 1, 2, \cdots\}$ が成り立つ. ■

天下りばかり続くが, さらに法 $(p^r, f(z))$ で冪 z^i を表す問題を考えよう. n 次の $f(z)$ の最高次係数は可逆と仮定したから, 任意の整数の法 p^r で $f(z)$ は他の整数係数多項式を割る事ができる. 故に問題の解は z^i を $f(z)$ で法 p^r で割り算して商 $a(z)$, 余り $b(z)$ を求めて得られる. 余り $b(z)$ の次数は $f(z)$ の次数より低い $n-1$ 以下で,

$$z^i \equiv f(z)a(z) + b(z) \equiv b(z) = \sum_{j=0}^{n-1} c_{i,j} z^j \pmod{p^r, f(z)} \tag{7.9}$$

となる. この係数 $\{c_{i,j}\}$ は次を満たす:

$$\begin{aligned}
&z^0 \text{ の時の余り} = z^0;\ c_{0,0} = 1,\ c_{0,1} = \cdots = c_{0,n-1} = 0,\\
&z^1 \text{ の時の余り} = z^1;\ c_{1,1} = 1,\ c_{1,0} = c_{1,2} = \cdots = c_{1,n-1} = 0,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,\\
&z^{n-1} \text{の時の余り} = z^{n-1};\quad c_{n-1,n-1} = 1,\ c_{n-1,0} = c_{n-1,1} = \cdots = c_{n-1,n-2} = 0.
\end{aligned}$$

$i+1 \geqq n,\ i \geqq n-1$ に対しては z^{i+1} を $f(z)$ で法 p で割った余りは「z^i を割った余りに z を掛けたものを再び $f(z)$ で割った余りに等しい」から,

$$\begin{aligned}
z^{i+1} &= \sum_{j=0}^{n-1} c_{i,j} z^j \cdot z\\
&= \sum_{j=0}^{n-2} c_{i,j} z^{j+1} + c_{i,n-1} \sum_{j=0}^{n-1} c_{n,j} z^j\\
&= \sum_{j=0}^{n-1} (c_{i,j-1} + c_{i,n-1} c_{n,j}) z^j,\ \ (\text{但し } c_{i,-1} := 0)\\
&\cdots\cdots\cdots\cdots\cdots\cdots.
\end{aligned}$$

だから係数 $\{c_{i,j}\}$ は $0 \leqq j \leqq n-1$ に対し次の漸化式で順次定まる:

$$\begin{aligned}
&c_{i,j} = \delta_{ij}\ (0 \leqq i \leqq n-1),\\
&c_{i+1,j} = c_{i,j-1} + c_{i,n-1} c_{n,j}\ (i \geqq n-1),\quad c_{i,-1} = 0.
\end{aligned} \tag{7.10}$$

いよいよ Brent による解析の第 1 の鍵である:

定理 7.9. (a) 漸化式 (7.2) の解は任意の整数 i, 素数 p, 整数 $r \geqq 1$ に対し次の表現を持つ:

$$x_i = \sum_{j=0}^{n-1} c_{i,j} x_j \pmod{p^r}. \tag{7.11}$$

(b) 特に $z^P \equiv 1 \mod (p^r, f(z))$ となる整数 P(があればそれ) に対して $x_{i+P} = x_i$ が成り立つ.

(証明) (a) 漸化式 (7.2) の解は, 任意の番号 k に対して表現

$$x_{k+i} = \sum_{j=0}^{n-1} d_{i,j} x_{k+j} \tag{7.12}$$

を持つ. 漸化式の係数が k に関係しないから係数は $d_{i,j} = d_{i-j}$ の形で, これは後に使う. 解を

特に $k=0$ の場合で, つまり出発値 $\{x_0, x_1, \cdots, x_{n-1}\}$ で表して考えると,

$$x_0 = x_0; \quad d_{0,0} = 1, \quad d_{0,1} = \cdots = d_{0,n-1} = 0,$$
$$x_1 = x_1; \quad d_{1,1} = 1, \quad d_{1,0} = d_{1,2} = \cdots = d_{1,n-1} = 0,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$
$$x_{n-1} = x_{n-1}; \quad d_{n-1,n-1} = 1, \quad d_{n-1,0} = d_{n-1,1} = \cdots = d_{n-1,n-2} = 0.$$

$i \geqq n-1$ に対しては (7.12) を $k=1$ で考えて,

$$x_{1+i} = \sum_{j=0}^{n-1} d_{i,j} x_{1+j} = \sum_{j=0}^{n-2} d_{i,j} x_{j+1} + d_{i,n-1} \sum_{j=0}^{n-1} d_{n,j} x_j$$
$$= \sum_{j=0}^{n-1} (d_{i,j-1} + d_{i,n-1} d_{n,j}) x_j \quad (\text{但し } d_{i,-1} := 0)$$

が成り立つ. 故に $0 \leqq j \leqq n-1$ に対する係数 $\{d_{i,j}\}$ は次の漸化式で定まる:

$$d_{i,j} = \delta_{ij} \ (0 \leqq i \leqq n-1),$$
$$d_{i+1,j} = d_{i,j-1} + d_{i,n-1} d_{n,j} \ (i \geqq n-1), \quad d_{i,-1} = 0. \tag{7.13}$$

(7.10) と (7.13) とは同じ漸化式と出発値だから, すべての i と $0 \leqq j \leqq n-1$ について $d_{i,j} = c_{i,j} = c_{i-j}$ である.

(b) 仮定 $z^P \equiv 1 \mod (p^r, f(z))$ によって, (7.9) より,

$$z^P \equiv \sum_{j=0}^{n-1} c_{P,j} z^j = z^0 \pmod{p^r, f(z)}.$$

故に $c_{P,0} = c_{P-0} = 1, \ c_{P,j} = c_{P-j} = 0 \ (1 \leqq j \leqq n-1)$, (a) によって

$$x_{i+P} = \sum_{j=0}^{n-1} c_{i+P-(i+j)} x_{i+j} = \sum_{j=0}^{n-1} c_{P-j} x_{i+j} = x_i. \qquad \blacksquare$$

第 2 の鍵, 母関数 generating function を導入する:

Lemma 7.10. 法 p^r での漸化式 (7.2) の任意の解系列に伴われる母関数 $G(z)$ を

$$G(z) := \sum_{j=0}^{\infty} x_j z^j \tag{7.14}$$

で定義する. G(z) は次を満たす:

$$G(z) g(z) = Q(z),$$
$$g(z) := 1 - b_1 z - b_2 z^2 - \cdots - b_n z^n = z^n f(\frac{1}{z}),$$
$$Q(z) := \sum_{k=0}^{n-1} x_k z^k - \sum_{j=1}^{n-1} \sum_{k=0}^{n-j-1} b_j x_k z^{j+k}. \tag{7.15}$$

(証明) 母関数 $G(z)$ は $\boldsymbol{Z}/p^r$ 上の形式的冪級数 [37),39),17)] と考えてその加減乗法を定義する; これらの加減乗法では z の各次数の係数は有限回の計算で確定し, それらを結果の型式的冪級数の係数とする. この定義で形式的冪級数全体は加減乗法の定義された環 ring になる.[17)] 或

いは複素解析の知識が邪魔をする場合にはこの考え方を使わず, 後に必要になる計算のためも含めて次の様にも議論できる. 状態有限の $\boldsymbol{Z}/p^r$ 上の漸化式の解 $\{x_k\}$ の n 連は有限個の状態しか取れず, 必ずある番号 j と $T'>0$ とがあって j からの n 連と $j+T'$ からの n 連が合致する. 同じ n 連の再現後は漸化式解は同じ発展を示すから, これは $T'\in A_j$ が成り立つ事を意味し, Corollary 7.7. によってすべて同一の一般周期の集合 $A=A_0=A_1=\cdots$ は必ず正の数 T' をその元として含む. 故に A の正で最小の元 T, 系列の周期, が必ず存在して $A=\{qT|\ q=0,1,2,\cdots\}$ であり, 考えている出発値に対する解系列の作る母関数 (7.14) は実際は 1 周期 T にわたる和 $\sum_{k=0}^{T-1} x_k z^k$ と z^T の無限等比級数との積であって任意の整数 j,k について $x_{kT+j}=x_j$ だから

$$G(z)=\sum_{j=0}^{\infty} x_j z^j=\sum_{k=0}^{\infty}\sum_{j=0}^{T-1} x_{kT+j}z^{kT+j}=\left\{\sum_{k=0}^{\infty}(z^T)^k\right\}\sum_{j=0}^{T-1} x_j z^j \qquad (7.16)$$

である. これは $|z^T|<1$, 即ち $|z|<1$ で収束する. だから $|z|<1$ に制限し, (7.14) が表す「収束円 $|z|<1$ 内での複素数 z の冪級数」と多項式との項別加減乗法を行う, と考えても (必要ではないが) 正しい. さて $k\geqq n$ の漸化式 (7.2) に z^k を掛けて $k=n$ から ∞ まで加えると, 次が得られる:

$$G(z)-\sum_{k=0}^{n-1}x_k z^k=b_1 z\left\{G(z)-\sum_{k=0}^{n-2}x_k z^k\right\}+b_2 z^2\left\{G(z)-\sum_{k=0}^{n-3}x_k z^k\right\}+\cdots+b_n z^n G(z).$$

左辺に $G(z)$ の項を, 右辺に残りを集めて (7.15) 全体に達する. ■

上の $g(z)=z^n f(\frac{1}{z})$ は $f(z)$ が体 $\boldsymbol{Z}_p$ 係数の原始多項式の場合に生成する M 系列の逆行系列を生成するものとして登場し $f^*(z)$ と記された. ここでは $f(z)$ はまだ $\boldsymbol{Z}_p$ 係数原始多項式とは限定しないが, 一般に $f^*(z)=:g(z)$ も $f(z)$ の逆 reverse と呼ぼう. 任意の法 m で $f(z)=f_1(z)f_2(z)$ と因数分解されれば $g(z)$ も, $g(z)$ が因数分解されれば $f(z)$ も同様に分解され, $f(z)$ とその逆 $g(z)$ の既約可約はそれぞれ同値である. また $g(z)$ の逆は $z^n g(\frac{1}{z})=f(z)$ である. これらは自明だが確認のため記して進む:

Corollary 7.11. (a) 整数係数 n 次多項式 $f(z)$ とその逆 $g(z)=f^*(z)$ とは任意の法 $m=p^r$ での既約可約を共にし, $f(z)$ は $g(z)$ の逆である.
(b) $f(z)$ は (7.7) の形で係数 b_n は法 p^r での可逆元, 即ち素因数 p を含まない $\boldsymbol{Z}_{p^r}$ の整数とする. 任意の法 p^r での特性多項式 $f(z)$ の漸化式系列に対しその逆行系列は逆 $g(z)$(の ${b_n}^{-1}$ 倍) を特性多項式とし, 2 系列の周期は等しい.
(c) $g(z)$ の最高次係数 b_n が法 p^r で可逆だから, $g(z)$ による任意の整数係数多項式の法 p^r での割り算は可能である. **(Corollary 7.11. 終り)**

我々は Ward[49](その p.606) の主要定理に達した:

定理 7.12. (7.5) の特性多項式 $f(z)=z^n-b_1z^{n-1}-\cdots-b_nz^0$ が $\boldsymbol{Z}_p$ 上で n 次**既約**とする. **法 p で零ベクトルではない任意の出発値** $(x_0,x_1,\cdots,x_{n-1})$ **に対して** (7.2) の n 次線形漸化式

$$x_k=b_1x_{k-1}+b_2x_{k-2}+\cdots+b_nx_{k-n}\pmod{p^r},\quad b_1,b_2,\cdots,b_n\in\boldsymbol{Z}/p^r,\quad b_n\text{は可逆},$$

の解の周期 T は出発値に関係なく一定で

$$z^P \equiv 1 \mod (p^r, f(z)) \tag{7.17}$$

となる最小の正の整数 P と等しい: $T = P$.

(証明) 既に Lemma 7.10. の母関数の性質 (7.15) の証明で記した様に, 漸化式の解系列を法 p^r で考えるとき正の, 従って正で最小の周期 $T > 0$ は存在して

$$G(z) = \sum_{k=0}^{\infty}(z^T)^k\{\sum_{j=0}^{T-1} x_j z^j\}, \quad (1 - z^T)G(z) = \sum_{j=0}^{T-1} x_j z^j =: R(z)$$

が成り立つ.[77] ここで $R(z)$ は法 p で高々 $T-1$ 次で, **系列の出発値の仮定から** 0 ではない多項式である. 右式両辺に $g(z) = z^n f(\frac{1}{z})$ を掛け (7.15) の関係 $G(z)g(z) = Q(z)$ を用いると

$$(1 - z^T)Q(z) = R(z)g(z)$$

の多項式関係に引き戻される. $f(z)$ は法 p で既約な n 次の多項式だから, Corollay 7.11.(a) により $g(z)$ も法 p で既約であり, $R(z)g(z)$ は法 p で 0 ではないから高々 $n-1$ 次の多項式 $Q(z)$ も法 p で 0 ではなく, n 次既約の $g(z)$ とは法 p で素で, Hensel の定理 7.5. は任意の $r \geqq 1$ に対する法 $(p^r, g(z))$ での $Q(z)$ の高々 $n-1$ 次の逆多項式 $Q^{-1}(z) \in \boldsymbol{Z}[z]/p^r$ の存在を保証する. 即ち

$$1 - z^T = Q^{-1}(z)R(z)g(z) \equiv 0 \mod (p^r, g(z)).$$

上の議論は $g(z)$ の生成する同じ周期 T の逆行系列でも成り立ち, $g(z)$ の逆が $f(z)$ だから, $1 - z^T \equiv 0 \pmod{(p^r, f(z))}$, 即ち

$$z^T \equiv 1 \mod (p^r, f(z)), \tag{7.18}$$

の成立が判明する. 故に法 $m = p^r$ での Corollary 7.8. の集合 B は正数 T を正で最小の P と共に含み, T は P の倍数で $T \geqq P$ である. 逆に定理 7.9.(b) から $x_{k+P} = x_k \pmod{p^r}$ であり, P は $\{x_k\}$ の法 p^r の周期 T の倍数で $T \leqq P$ も成り立って $P = T$ と判明する. ■

$\boldsymbol{Z}_p$ 上での特性多項式の既約性だけに基づく線形漸化式解の法 p^r での周期の初期値不依存性の算術演算的証明の力を見よう.[78] 勿論 $r = 1$ に限れば, それは体 $\boldsymbol{Z}_p$ 上の既約多項式 $f(z)$ が同位数の共役根を持つ構造の結果として我々が知る通りであるが.

我々は 7.1 節で p 進表示での繰り上がり機構を議論し, 法 p^r での加算生成法 (7.2) の最長周期 $p^{r-1}(p^n - 1)$ を得た. その実現の 1 つの必要十分条件を導いて, 法 2^r での乗算合同法とよく似た構造を認識する:

定理 7.13. 任意の素数 p と正の整数 n 及び $r \geqq 2$ を定める. $\boldsymbol{Z}_p$ の意味で 0 ベクトルではないすべての出発値 $(x_0, x_1, \cdots, x_{n-1})$ に対して n 次線形漸化式 (7.2) が法 p^r で最大周期 $p^{r-1}(p^n-1)$ を実現する必要十分条件は, (7.2) の解系列を $\{x_k\}$ として:

---

[77] 単純に項別計算して $(1 - z^T)\sum_{k=0}^{\infty}(z^T)^k = 1$, としてよい. 収束の知識が邪魔するなら, $|z| < 1$ と制限して無限等比級数の公式から納得しても構わない.

[78] 乱数問題ではあまり必要ではないが, 一般問題としては重要な「特性多項式が重解を持つ様な線形漸化式」の場合, 周期は出発値のとり方にも依存する. しかしこの周期の特徴付けにも上の議論は用いる事ができる. この興味ある点に関しては Appendix C 参照.

(a) $p \geqq 3$ の場合, $\boldsymbol{Z}_p$ の意味で 0 ベクトルでない任意の 1 つの出発値 $(x_0, x_1, \cdots, x_{n-1})$ に対し $\{x_k\}$ が次の 2 条件を満たす事である:

(i) 法 p で $\{x_k\}$ の周期は $p^n - 1$ である.

(ii) 法 p^2 での $\{x_k\}$ の周期は $p(p^n - 1)$ である.

(b) $p = 2$ の場合で $r \geqq 3$ に対しては, 上の (1),(2) と次の (3) とが必要十分条件である:

(iii) 法 2^3 での $\{x_k\}$ の周期が $2^2(2^n - 1)$ となる.

(証明) [必要性] (7.2) の解が法 p^r で最長周期 $p^{r-1}(p^n - 1)$ であるには, $1 \leqq m \leqq r$ のすべての m に対しても法 p^m での最長周期 $p^{m-1}(p^n - 1)$ が実現される必要は p 進の各桁毎の繰り上がりを考えて見られている. 故に (a),(b) は必要である.

[十分性] $p \geqq 3$ としよう. (i) が成り立てば n 次漸化式の解 $\{x_k\}$ が $\boldsymbol{Z}_p$ 上の n 次 M 系列であり, $f(z)$ が $\boldsymbol{Z}_p$ 上の n 次原始多項式であることは既に見た. また定理 75 によって (i) は

$$z^{p^n-1} \equiv 1 \mod (p, f(z)),$$

即ち

$$z^{p^n-1} = 1 + a(z)f(z) + pb(z)$$

となる整数係数多項式 $a(z), b(z)$ の存在を意味する. ここで $b(z)$ は法 $(p, f(z))$ で 0 ではない; 仮に $b(z) = c(z)f(z) + pd(z)$ であれば

$$z^{p^n-1} = 1 + \{a(z) + pc(z)\}f(z) + p^2 d(z)$$

であって法 $(p^2, f(z))$ で $z^{p^n-1} \equiv 1$ となり, 定理 7.7.(b) によって法 p^2 での $\{x_k\}$ の周期は $p^n - 1$ 以下で仮定 (ii) に反するからである. 故に仮定 (i),(ii) は

$$z^{p^n-1} = 1 + a(z)f(z) + pb(z), \quad b(z) \not\equiv 0 \mod (p, f(z))$$

或いは

$$z^{p^n-1} \equiv 1 \mod (p, f(z)), \tag{7.19}$$

$$z^{p^n-1} \not\equiv 1 \mod (p^2, f(z)), \tag{7.20}$$

$$\begin{aligned}(z^{p^n-1})^p = z^{p(p^n-1)} &= \{1 + a(z)f(z) + pb(z)\}^p \\ &= 1 + {}_p\mathrm{C}_1\{a(z)f(z) + pb(z)\} + {}_p\mathrm{C}_2\{a(z)f(z) + pb(z)\}^2 + \cdots \\ &= 1 + a_1(z)f(z) + p^2\{b(z) + pc_1(z)\}\end{aligned}$$

$$\equiv 1 \mod (p^2, f(z)) \tag{7.21}$$

$$\not\equiv 1 \mod (p^3, f(z)) \tag{7.22}$$

を与える. 再び定理 7.12 によって, (7.20) と (7.21) とは $\boldsymbol{Z}_p$M 系列 $\{x_k\}$ の法 p^2 での周期が, 可能な値のうち $p^n - 1$ ではなく最長の $p(p^n - 1)$ であると決定する. ここ及び以下で $c_k(z)$ は z のある整数係数多項式を表す. もう 1 度 p 乗すれば全ては見通される:

$$\begin{aligned}\{(z^{p^n-1})^p\}^p = z^{p^2(p^n-1)} &= \{1 + a_1(z)f(z) + p^2[b(z) + pc_1(z)]\}^p \\ &= 1 + a_2(z)f(z) + p^3\{b(z) + pc_2(z)\} \\ &\equiv 1 \mod (p^3, f(z))\end{aligned} \tag{7.23}$$

$$\not\equiv 1 \mod (p^4, f(z)). \tag{7.24}$$

(7.23) と (7.24) とは, 定理 7.12 によって, 法 p^3 での $\{x_k\}$ の周期が最長の $p^2(p^n-1)$ であると決定する. 以下 p 乗を繰返して, 一般に (i),(ii) が満たされれば法 p^r での $\{x_k\}$ の周期は $p^{r-1}(p^n-1)$ である事が示される.

$p=2$ の場合, 上の議論は (7.22) の所だけで成り立たない; ${}_2\mathrm{C}_1=2$ だが ${}_2\mathrm{C}_2=1$ にはもはや因数 2 は含まれないからである. 実際その計算は

$$\begin{aligned}(z^{2^n-1})^2 = z^{2(2^n-1)} &= \{1+a(z)f(z)+2b(z)\}^2\\ &= 1+2\{a(z)f(z)+2b(z)\}+\{a(z)f(z)+2b(z)\}^2\\ &= 1+a_1(z)f(z)+2^2\{b(z)+b^2(z)\}\\ &\equiv 1 \mod (2^2, f(z)).\end{aligned}$$

しかし $b(z)+b^2(z)$ が 2 で割り切れる事があり得るから

$$(z^{2^n-1})^2 = z^{2(2^n-1)} \equiv 1 \mod (2^3, f(z))$$

となる可能性があって, 法 2^3 で $\{x_k\}$ の周期が最長の $2^{3-1}(2^n-1)=2^2(2^n-1)$ ではなく $2(2^n-1)$ かもしれないのである. これを除外するのが条件 (iii) で, 法 2^3 での最長周期が保証される. これ以後は (7.23),(7.24) と同様に進む. ■

古典的な Ward の論文 [49] は, 既に 1933 年に上の結論を特別の場合として含む遥に一般の形 (定理 13.1) に与えている. Knuth の教科書第 2.2 節の演習問題 11(文献 [2]pp.35-36) も参照せよ. 今や明らかだが, Ward の結論は次の形に述べられる:

定理 7.14 (Ward). 法 p で 0 ベクトルではない任意の出発 n 連 $(x_0, x_1, \cdots, x_{n-1})$ $(n \geqq 2)$ に対して n 次線形漸化式 (7.2) が法 p^r で最大周期 $p^{r-1}(p^n-1)$ を実現する必要十分条件は, (7.6) の n 次特性多項式 $f(z)$ が既約で次を満たす事である:
(a) $p \geqq 3$ の場合次の (i),(ii) が成り立つ:

(i) $s < p^n-1$ に対して $z^s \not\equiv 1 \mod (p, f(z))$.

(ii) $z^{p^n-1} \not\equiv 1 \mod (p^2, f(z))$.

(b) $p=2$ の場合で $r \geqq 3$ に対しては, 上の (i),(ii) と次の (iii) とが成り立つ:

(iii) $z^{2(2^n-1)} \not\equiv 1 \mod (8, f(z))$.

(証明) 条件の必要性は明らかだから十分性だけを述べる.
(a) $f(z)$ は体 $\boldsymbol{Z}_p$ 上 n 次既約と仮定されたから必ず $z^{p^n-1}-1$ を法 p で割り切り, $z^{p^n-1} \equiv 1 \pmod{p, f(z)}$ は成り立つ. 故に (i) は $f(z)$ が $\boldsymbol{Z}_p$ 上の n 次原始多項式だと制限する. 同様に (ii) は「法 p^2 で $f(z)$ は $z^{p^n-1}-1$ を割り切らない」, と言い換えてもかまわない. 条件 (i) によって法 p^2 での線形漸化式周期は p^n-1 以上である事を保証され, 実際に周期はこれか或いはこれではなく最長の $p(p^n-1)$ か, の二者択一である. 即ち定理 7.12. によれば

$f(z)$ は $z^{p^n-1} \equiv 1 \pmod{p^2, f(z)}$ を与える, 即ち法 p^2 で $f(z)$ は $z^{p^n-1}-1$ を
　　或いは $z^{p^n}-z$ を割り切って漸化式は最長周期ではないか,
或いは $z^{p^n-1} \equiv 1 \pmod{p^2, f(z)}$ を与えない, 即ち法 p^2 で $f(z)$ は $z^{p^n-1}-1$ を
　　或いは $z^{p^n}-z$ を割り切らず漸化式は最長周期であるか,

の二者択一である. 条件 (ii) は前者の可能性を打ち消すから, 法 p^2 でも漸化式は最長周期を与え, 定理 7.13.(a) と $p \geqq 3$ とによって全ての $r \geqq 1$ に対して線形漸化式の解は法 p^r での最長周期を保証される.
(b) $p = 2$ について, 上の (a)(ii) と全く同じで定理 7.13.(b) による. ■

7.3. 法 2^r での Brent の最長周期判定条件の証明

法 2^r の場合の加算生成法について最近 Brent[50] が与えた結論は最長周期判定を特性多項式 $f(z)$ の上だけで行う事を可能にし, 誠に簡潔で強力である. まず結果を次の定理にまとめて, 全貌の把握から始める様に努める:

定理 7.15.(Brent[50]) (a) 法 2^r での線形漸化式 (7.2) のモニックな特性多項式 $f(z)$ は $\boldsymbol{Z}_2$ 上原始的とする. 全てが偶数ではない (法 2 で 0 ベクトルではない) 任意の出発値 $(x_0, x_1, \cdots, x_{n-1})$ に対して (7.2) が最長周期 $2^{r-1}(2^n - 1)$ を実現する必要十分条件は

$$\{f(z)\}^2 + \{f(-z)\}^2 \not\equiv 2f(z^2) \pmod 8 \tag{7.25}$$

$$\{f(z)\}^2 + \{f(-z)\}^2 \not\equiv 2(-1)^n f(-z^2) \pmod 8 \tag{7.26}$$

の両方の成立である.
(b) 次数 $n \geqq 3$ の時, n 次 $\boldsymbol{Z}_2$ 原始 3 項式 $f(z)$ を特性多項式に選べば, 任意の $r = 1, 2, \cdots$ の法 2^r で見たその形に関係なく, また偶数ばかりではない任意の出発値ベクトル $(x_0, x_1, \cdots, x_{n-1})$ に対しても, 法 2^r での加算生成法 (7.2) は最長周期 $p^{r-1}(p^n - 1)$ を持つ. **(定理 7.15. 終り)**

証明は誠に精巧簡潔だが, 予備知識が求められる. 以下これを紹介するのにいくつかの説明を補うので, 原論文の端的さをかなり損うものである事を断らなければならない. 是非原論文も参照して頂きたい. まず一般の法 p^r での多項式の既約, 可約について注意, Lemma 1.14 の系列の事柄, を確認する:

Corollary 7.16. 素数 p と整数 $r \geqq 2$ に対する p^r を法とする整数 $\boldsymbol{Z}/p^r$ 係数のモニックな多項式 $f(z)$ が法 p で既約であれば, 法 p^r でも既約である.
(証明) 対偶を示す. 法 p^r で $f(z)$ が可約で $s > 0,\ n - s > 0$ に対するある因数分解

$$f(z) = z^n + \cdots \equiv (z^s + \cdots)(z^{n-s} + \cdots) \mod p^r, \tag{7.27}$$

を持てば, $z^s + \cdots,\ z^{n-s} + \cdots$ は共に 1 次以上の z の多項式で, 合同式ではなく等式としてはこの残余は p^r にある整数係数多項式を掛けたものだから (7.27) は法 p でも $f(z)$ の因数分解を与え $f(z)$ は $\boldsymbol{Z}_p$ 可約である. ■

次は証明の第 1 準備である:

Lemma 7.17. 任意の整数係数多項式 $x(z),\ y(z),\ f(z)$ について:
(a) 任意の $r \geqq 1$ について次が成り立つ:

$$x(z) \equiv y(z) \mod (2^r, f(z)) \text{ なら } x^2(z) \equiv y^2(z) \mod (2^{r+1}, f(z)).$$

(b) もし $f(z)$ が $\boldsymbol{Z}_2$ 既約 (従って上の通り $\boldsymbol{Z}/2^r$ 既約でもある) とすれば,

(i) $\{x(z)\}^2 \equiv \{y(z)\}^2 \mod (2, f(z))$,

$$\text{(ii)}\ \{x(z)\}^2 \equiv \{y(z)\}^2 \mod (4, f(z)),$$

の 2 つは同値であり,

$$\text{(i')}\ \{x(z)\}^2 \equiv \{y(z)\}^2 \mod (8, f(z)),$$

$$\text{(ii')}\quad x(z) \equiv \pm y(z) \mod (4, f(z)),$$

の 2 つも同値である.

(証明) (a) $x(z) \equiv y(z) \mod (2^r, f(z))$ なら, $x(z) = y(z) + 2^r a(z) + A(z)f(z)$ となる整数係数多項式 $a(z), A(z)$ がある. 故に

$$\{x(z)\}^2 = \{y(z)\}^2 + 2^{r+1}a(z)y(z) + A(z)f(z) \equiv \{y(z)\}^2 \mod (2^{r+1}, f(z)).$$

(b) (ii) が成り立てば $\{x(z)\}^2 = \{y(z)\}^2 + 4a(z) + A(z)f(z)$ となる整数係数多項式 $a(z), A(z)$ があり, 自明に

$$\{x(z)\}^2 \equiv \{y(z)\}^2 \pmod{2, f(z)}$$

であって (ii)→(i) は $f(z)$ が $\boldsymbol{Z}_2$ 既約かどうかに関係なく成り立つ. 逆に (i) を仮定すると,

$$\{x(z)\}^2 - \{y(z)\}^2 = (x-y)(x+y) \equiv (x-y)^2 = A(z)f(z) \pmod 2$$

となる整数係数多項式 $A(z)$ が存在する. $\boldsymbol{Z}_2$ で $f(z)$ は既約だから 2 つの因数には分けられず, これは $x(z) - y(z)$ が法 2 で $f(z)$ を因数に含むか 0 に合同かで, どちらにしても $x(z) \equiv y(z) \mod (2, f(z))$ であり, (a) から $\{x(z)\}^2 \equiv \{y(z)\}^2 \mod (4, f(z))$ であって (i)→(ii) が成り立つ.

最後に $\boldsymbol{Z}_2$ で既約, 従って法 4 でも法 8 でも既約な $f(z)$ について, (i') の成立を仮定すると, $\{x(z)\}^2 - \{y(z)\}^2 \equiv A(z)f(z) \pmod 8$ となる整数係数多項式 $A(z)$ がある. 法を 2 としてもこの式は成立し,

$$\{x(z)\}^2 - \{y(z)\}^2 = (x-y)(x+y) \equiv (x-y)^2 = A(z)f(z) \pmod 2$$

が成り立つ. $f(z)$ の $\boldsymbol{Z}_2$ 既約性からこれは

$$x(z) - y(z) = 2a(z) + B(z)f(z) \tag{7.28}$$

となる整数係数多項式 $a(z), B(z)$ の存在, 変数 z を省いて $x = y + 2a + Bf$ の成立であり,

$$x^2 - y^2 = (y + 2a + Bf)^2 - y^2 = 4a(y+a) + Cf,\ \ C = C(z) \text{ も整数係数多項式}$$

である. これに仮定 (i') を当てはめて $4a(y+a) \equiv Af \pmod 8$ を得て, 結論

$$a(z)\{y(z) + a(z)\} = D(z)f(z) \pmod 2$$

が導かれる; $D(z)$ は整数係数多項式. 素数の法 2 に戻した事に注意. 法 2 で $f(z)$ は既約だから, これは $a(z) = 2b(z) + E(z)f(z)$ 或いは $y(z) + a(z) = 2b(z) + E(z)f(z)$ の成立を意味し, 前者の場合 (7.28) から $x(z) = y(z) + 4b(z) + F(z)f(z)$, 後者の場合

$$\begin{aligned} x(z) &= y + 2a + Bf = 2(y+a) - y + Bf \\ &= 2(2b + Ef) - y + Bf = -y(z) + 4b(z) + F(z)f(z) \end{aligned}$$

が成り立つ. どちらにしてもこれらは (ii') の成立で (i')→(ii') が示された. 逆の (ii')→(i') は (a) によって明らか. ■

次の予備定理が Brent の結論の最大の鍵である:

定理 7.18.(Brent) $f(z)$ はモニックで法 2 で既約な $\boldsymbol{Z}/2^r$ 係数 n 次多項式, $n \geqq 2$ であるとする.
(a) $z^{2^n-1} \equiv 1$, 即ち $z^{2^n} \equiv z \pmod{2, f(z)}$ が成り立つ.
(b) この時 $z^{2^n-1} \equiv -1 \pmod{4, f(z)}$ となる必要十分条件は

$$f^2(z) + f^2(-z) \equiv 2f(z^2) \pmod 8 \tag{7.29a}$$

の成立である.
(c) またこの時 $z^{2^n-1} \equiv 1 \pmod{4, f(z)}$ となる必要十分条件は

$$f^2(z) + f^2(-z) \equiv 2(-1)^n f(-z^2) \pmod 8 \tag{7.29b}$$

の成立である.
(証明) (a) n 次多項式 $f(z)$ は法 2 で既約だから $\boldsymbol{Z}_2$1 次因数 z も $z-1$ も含めず, $f(z) = 0$ の根 $\alpha \neq 0, 1$ を $\boldsymbol{Z}_2$ に添加して有限体 $\mathrm{GF}(2^n)$ が作られる. $\mathrm{GF}(2^n)$ のすべての元, 特に α は $z^{2^n} - z = z(z^{2^n-1} - 1) = 0$ の根であり, $\alpha \neq 0$ の最小多項式である $f(z)$ は $z^{2^n} - z$, 特に $z^{2^n-1} - 1$ を割り切る.

以下 (b),(c) の証明のために $\boldsymbol{Z}_2$ 既約な n 次多項式 $f(z)$ を偶数次, 奇数次項に分けて常に次の様に置く:

$$f(z) = u(z^2) + zv(z^2). \tag{7.30}$$

(c) 法 2 では $-z \equiv z$ だから, (7.30) は $u(z^2) \equiv zv(z^2) \pmod{2, f(z)}$ を意味する. また任意の整数係数多項式 $a(z)$ について, 法 2 では 2 項係数の構造から $a(z^2) \equiv a^2(z)$ でもあった. 故に (a) と (7.30) とは次を与える:

$$u^2(z) \equiv u(z^2) \equiv z^{2^n} v(z^2) \equiv \{z^{2^{n-1}} v(z)\}^2 \pmod{2, f(z)}. \tag{7.31}$$

右辺は平方であり, Lemma 7.17.(b) によって $\boldsymbol{Z}_2$ 既約な n 次の任意の多項式 $f(z)$ について一般に次が成り立つ:

$$u^2(z) \equiv z^{2^n} v^2(z) \pmod{4, f(z)}. \tag{7.32}$$

また法 2 では $-z \equiv z$ と共に $u(-z) \equiv u(z)$, $v(-z) \equiv v(z)$ でもあるから, (7.31) から

$$u^2(-z) \equiv z^{2^n} v^2(-z) = \{z^{2^{n-1}} v(-z)\}^2 \pmod{2, f(z)},$$

も成り立ち, 再び Lemma 7.17.(b) によって

$$u^2(-z) \equiv z^{2^n} v^2(-z) \pmod{4, f(z)} \tag{7.33}$$

である. さらに (7.30) から $f^2(z) + f^2(-z)$ を作ると,

$$f^2(z) = \{u(z^2) + zv(z^2)\}^2 = u^2(z^2) + 2zu(z^2)v(z^2) + z^2v^2(z^2),$$
$$f^2(-z) = \{u(z^2) - zv(z^2)\}^2 = u^2(z^2) - 2zu(z^2)v(z^2) + z^2v^2(z^2),$$

であって,

$$f^2(z) + f^2(-z) = 2u^2(z^2) + 2z^2v^2(z^2) = 2f(z^2) + 8a(z^2), \tag{7.34}$$

となる. (7.31)-(7.34) は n 次 $\boldsymbol{Z}_2$ 既約多項式 $f(z)$ について一般に成り立つ事に注意する.

ここで仮定 $z^{2^n-1} \equiv -1 \pmod{4, f(z)}$, 即ち $z^{2^n} \equiv -z \pmod{4, f(z)}$ を置こう. そうすると (7.32) は

$$u^2(z) \equiv -zv^2(z), \;\; u^2(z) + zv^2(z) \equiv 0 \pmod{4, f(z)} \tag{7.35}$$

であり, 次の式が成立する:

$$u^2(z) + zv^2(z) - f(z) = u^2(z) + zv^2(z) - \{u(z^2) + zv(z^2)\} \equiv 0 \pmod{4, f(z)}.$$

$f(z)$ の次数 n が偶数の場合 $f(z)$ の最高次項 z^n は $u(z^2)$ にあり, $u(z)$ は $\dfrac{n}{2}$ 次である. $f(z)$ はモニックだから $u(z^2)$ も同じで, 上の式の中辺は z の $n-1$ 次以下の多項式である. また $f(z)$ の次数 n が奇数なら最高次項 z^n は $zv(z^2)$ にあり, $v(z)$ はモニックで, やはり上式中辺は $n-1$ 次以下の多項式である. 故にこの中辺は法 4 でも既約な $f(z)$ を含む事はできないから, これは法 4 での恒等式, 従って z の全ての冪の係数が法 4 で左右等しい下の式が成り立つ:

$$u^2(z) + zv^2(z) = f(z) + 4a(z). \tag{7.36}$$

$a(z)$ はある $n-1$ 次以下の整数係数多項式である. この結果で z を z^2 で置き換えれば,

$$u^2(z^2) + z^2v(z^2) = f(z^2) + 4a(z^2), \tag{7.37}$$

を得る. これを (7.34) に入れて

$$f^2(z) + f^2(-z) = 2f(z^2) + 8a(z^2) \tag{7.38}$$

即ち (7.29a) が成り立つ; (7.29a) は $z^{2^n-1} \equiv -1 \pmod{4, f(z)}$ からの帰結であり, (7.29a) が $z^{2^n-1} \equiv -1 \pmod{4, f(z)}$ の必要条件である事が示された.

逆にモニックで法 2 で既約な n 次の $f(z)$ が (7.29a) を満たすとしよう. 常に成り立つ (7.34) を (7.29a) に入れて (7.37) が得られ, この場合も (7.37) の両端の辺の z の最高次数の項 z^{2n} から考えて $a(z^2)$ は $2n-1$ 次以下, 従って $a(z)$ は $n-1$ 次以下であり, (7.37) は法 4 での恒等式で, そのすべての z^2 を z で置き換えれば $u^2(z) + zv^2(z) = f(z) + 4a(z)$, 即ち $u^2(z) + zv^2(z) \equiv 0 \pmod{4, f(z)}$ が得られる.

一方 $f(z)$ は $\boldsymbol{Z}_2$ 上の n 次既約多項式だから $z = z^{2^n} \pmod{2, f(z)}$ である. 故に $u(z^2) \equiv zv(z^2) \pmod{2, f(z)}$ も用いて, 法 2 の計算で

$$u^2(z) \equiv u(z^2) \equiv z^{2^n}v(z^2) = z^{2^n}v^2(z) \pmod{2, f(z)} \tag{7.39}$$

が見られる. $f(z)$ の $\boldsymbol{Z}_2$ 既約性と Lemma 7.17.(b) によってこれは

$$u^2(z) = z^{2^n}v^2(z) \pmod{4, f(z)}$$

を意味し, (7.34) へ入れて

$$(z + z^{2^n})v^2(z) \equiv 0 \qquad \pmod{4, f(z)} \tag{7.40}$$

を得る. $f(z) = u(z^2) + zv(z^2)$ なのだから勿論 $v(z)$ の次数は $f(z)$ の次数 n より小で $\boldsymbol{Z}_2$ 既約な $f(z)$ は $v(z)$ の中にはない. また法 2 で $v(z) \equiv 0$ でもない; 仮に法 2 で $v(z) \equiv 0$ なら法 2 で $f(z) \equiv u(z^2) \equiv u^2(z)$, 即ち $f(z)$ が $\boldsymbol{Z}_2$ 可約, の矛盾が生じるからである. こうして $v(z)$ は法 $(2, f(z))$ の可逆元, 従って Hensel の lemma 7.6. によって $v(z)$ は法 $(4, f(z))$ でも可逆で, この逆元を 2 度 (7.40) に掛けて

$$z + z^{2^n} \equiv 0 \pmod{4, f(z)}, \text{即ち } z^{2^n} \equiv -z \pmod{4, f(z)}$$

を得る. 勿論 3 次以上の $\boldsymbol{Z}_2$ 既約な $f(z)$ と z は法 2 で素で z も法 4 で可逆, その逆元を掛けて

$$z^{2^n-1} \equiv -1 \pmod{4, f(z)}$$

が得られた. これで長かった (a) の証明を終了する.

(b) $z^{2^n-1} \equiv 1 \pmod{2, f(z)}$ であるモニックで n 次 $\boldsymbol{Z}_2$ 既約な $f(z)$ について $z^{2^n-1} \equiv 1 \pmod{4, f(z)}$ が成り立つと仮定しよう. 証明方法は (a) と同じだが所々で符号が変る. 再び $f(z)$ の (7.30) の分解, また任意の整数係数多項式 $u(z), v(z)$ についての法 2 での $v(z^2) \equiv v^2(z),\ v(z^2) \equiv v^2(z)$ の成立に注意すると:

$$u^2(z) \equiv u(z^2) \equiv -z^{2^n} v(z^2) + f(z) \equiv z^{2^n} v(z^2) \equiv z^{2^n} v^2(z) \pmod{2, f(z)}. \quad (7.31)$$

z^{2^n} は平方だから Lemma 7.17.(b) によって, $\boldsymbol{Z}_2$ 既約な n 次 $f(z)$ について一般に,

$$u^2(z) \equiv z^{2^n} v^2(z) \pmod{4, f(z)} \quad (7.32)$$

である. また法 2 では $-z \equiv z$, $u(-z) \equiv u(z)$, $v(-z) \equiv v(z)$ だから, (7.31) から $u^2(-z) \equiv z^{2^n} v^2(-z) \pmod{2, f(z)}$ も成り立つ. 再び Lemma 7.17.(b) によって, 故に, $\boldsymbol{Z}_2$ 既約である n 次 $f(z)$ について一般に,

$$u^2(-z) \equiv z^{2^n} v^2(-z) \pmod{4, f(z)} \quad (7.33)$$

が成立する. さてここで (a) と異なるのだが, $z^{2^n-1} \equiv 1 \pmod{2, f(z)}$ であって $z^{2^n-1} \equiv 1 \pmod{4, f(z)}$ にもなるとすると, (7.32) によって

$$u^2(-z) \equiv z v^2(-z),\ \ u^2(-z) - z v^2(-z) \equiv 0 \pmod{4, f(z)} \quad (7.41)$$

であり,

$$u^2(-z) - z v^2(-z) - (-1)^n f(z) \equiv u^2(-z) - z v^2(-z) - (-1)^n \{u(z^2) + z v(z^2)\}$$
$$\equiv 0 \pmod{4, f(z)}.$$

$f(z)$ が偶数 n 次で z^n が $u(z^2)$ に含まれれば中辺での z^n の係数は $(-1)^{2(n/2)} - (-1)^n = 0$, n が奇数で z^n が $z v(z^2)$ に入ればそれは $-(-1)^{2(n-1)/2} - (-1)^n = (-1)^{1+n-1} - (-1)^n = 0$, どちらにせよ上の式全体の次数は n 未満で, 法 4 でも既約な $f(z)$ を含む事はできないから, 法 4 で次の恒等式の成立が判る:

$$u^2(-z) - z v^2(-z) = (-1)^n f(z) + 4a(z). \quad (7.35')$$

$a(z)$ は再びある整数係数多項式である. この結果で z を $-z^2$ で置き換えれば,

$$u^2(z^2) + z^2 v^2(z^2) = (-1)^n f(-z^2) + 4a(-z^2). \quad (7.36')$$

勿論 $u(z), v(z)$ のもとの定義 (7.30) から,

$$f^2(z) = \{u(z^2) + z v(z^2)\}^2 = u^2(z^2) + 2z u(z^2) v(z^2) + z^2 v^2(z^2), \quad (7.42)$$

$$f^2(-z) = \{u(z^2) - z v(z^2)\}^2 = u^2(z^2) - 2z u(z^2) v(z^2) + z^2 v^2(z^2), \quad (7.43)$$

即ち (7.36') によって

$$f^2(z) + f^2(-z) = 2u^2(z^2) + 2z^2 v^2(z^2) = 2(-1)^n f(-z^2) + 8a(-z^2). \quad (7.44)$$

これで

$$f^2(z) + f^2(-z) \equiv 2(-1)^n f(-z^2) \pmod{8} \quad (7.29b)$$

が導かれた. (7.29b) は $z^{2^n-1} \equiv 1 \pmod{4, f(z)}$ の必要条件である.

さあ, 1 息入れて逆に $\boldsymbol{Z}_2$ 上モニックで n 次既約な $f(z)$ が (7.29b) を満たすとしよう. $f(z)$ の偶奇冪への分解 (7.30) から (7.37), (7.38) は成立し, これらを (7.29b) へ入れると

$$f^2(z) + f^2(-z) = 2u^2(z^2) + 2z^2v^2(z^2) = 2(-1)^n f(-z^2) \pmod 8,$$

即ち

$$u^2(z^2) + z^2v^2(z^2) = (-1)^n f(-z^2) + 4b(z^2) \equiv f(z^2) \pmod 4 \qquad (7.45)$$

となる z^2 の整数係数多項式 $b(z^2)$ があり, $b(z)$ の次数は $n-1$ 以下で (7.45) が法 4 での恒等式になる. すべての z^2 を $-z$ で置き換えれば

$$u^2(-z) - zv^2(-z) = (-1)^n f(z) + 4b(-z),$$
$$u^2(-z) \equiv zv^2(-z) \pmod{4, f(z)} \qquad (7.46)$$

が得られる. 一方 $f(z)$ が n 次 $\boldsymbol{Z}_2$ 既約多項式である事から $z \equiv z^{2^n} \pmod{2, f(z)}$ であり,

$$f(z) = u(z^2) + zv(z^2),$$
$$u^2(z) \equiv u(z^2) \equiv u^2(-z) \equiv -z^{2^n}v^2(-z) \equiv z^{2^n}v^2(-z) \pmod{2, f(z)}$$

となる事, 2^n が偶数である事, $f(z)$ の $\boldsymbol{Z}_2$ 既約性, そして Lemma 7.17.(b) とから

$$u^2(-z) = z^{2^n}v^2(-z) \pmod{4, f(z)}$$

が成り立つ事によって

$$z^{2^n}v^2(-z) \equiv zv^2(-z), \ \ (z^{2^n} - z)v^2(-z) \equiv 0, \qquad \pmod{4, f(z)} \qquad (7.47)$$

を得る. $f(z) = u(z^2) + zv(z^2)$ なのだから勿論 $v(-z)$ の次数は $f(z)$ の次数 n より小で $\boldsymbol{Z}_2$ 既約な $f(z)$ と $v(z)$ には $\boldsymbol{Z}_2[z]$ の意味で互いに素である. また法 2 で $v(-z) \equiv 0$ でもない; 仮に法 2 で $v(-z) \equiv 0$(定数) なら $v(z) \equiv 0, \ f(z) \equiv u(z^2) \equiv u^2(z)$ が法 2 で可約になる矛盾が生じるからである. こうして $v(z)$ は法 $(2, f(z))$ の可逆元, 従って Hensel の定理 7.6 によって $v(z)$ は法 $(4, f(z))$ でも可逆である. この逆元を 2 度 (7.47) に掛けて

$$z^{2^n} - z \equiv 0 \pmod{4, f(z)}, \text{ 即ち } z^{2^n} \equiv z \pmod{4, f(z)}.$$

勿論 $f(z)$ と z も法 2 で素だから z も法 $(4, f(z))$ で可逆で, その逆元を掛けて法 $(4, f(z))$ で $z^{2^n-1} \equiv 1$ が得られた. (7.29b) は $z^{2^n-1} \equiv 1 \pmod{4, f(z)}$ の十分条件である. これで (b) の証明を終る. ■

上で我々が調べたのは, n 次 $\boldsymbol{Z}_2$ 既約な多項式 $f(z)$ が法 2^r では最長周期を「与えない」場合, n 次 $\boldsymbol{Z}_2$ 原始多項式 $f(z)$ で言えば法 2^r で $2^{r-1}(2^n-1)$ にはならない場合である. Brent は一般の $\boldsymbol{Z}_2$ 既約多項式で定理 7.15 が成り立つ事を示したが, 我々には原始多項式の場合以外にあまり興味がないから, その場合についてこの節の最初に述べた Brent の定理 7.15. へ戻ろう. 少し形を変えて再記する.

定理 7.15.(a) $\boldsymbol{Z}_2$ の意味で n 次原始多項式である

$$f(z) = z^n - b_1z^{n-1} - \cdots - b_nz^0, \quad n \geqq 3, \qquad (7.5)$$

を特性多項式とする法 2^r での線形漸化式

$$x_k = b_1x_{k-1} + b_2x_{k-2} + \cdots + b_nx_{k-n} \pmod{2^r}),\ \ b_1, b_2, \cdots, b_n \in \boldsymbol{Z}/2^r, \qquad (7.2)$$

について, $\boldsymbol{Z}_2$ の意味の零ベクトル, 即ち偶数の n 連, ではない任意の出発値 $(x_0, x_1, \cdots, x_{n-1})$ を考える.
(i) もし $f^2(z) + f^2(-z) \equiv 2(-1)^n f(-z^2) \pmod 8$ が成り立てば, すべての $r = 2, 3, \cdots$ に対して漸化式の周期 T は $T \leqq 2^{r-2}(2^n - 1)$ であり, 最長周期より小さい.
(ii) もし $f^2(z) + f^2(-z) \equiv 2f(z^2) \pmod 8$ が成り立てば, すべての $r = 3, 4, \cdots$ に対して漸化式の周期 T は $T \leqq 2^{r-2}(2^n - 1)$ であり, 最長周期より小さい.
(iii) すべての $r = 2, 3, \cdots$ に対して漸化式の周期 T は $T \leqq 2^{r-1}(2^n - 1)$ であり, 最長周期である必要十分条件は $f(z)$ が

$$f^2(z) + f^2(-z) \not\equiv 2f(z^2) \pmod 8, \qquad (7.25)$$

$$f^2(z) + f^2(-z) \not\equiv 2(-1)^n f(-z^2) \pmod 8, \qquad (7.26)$$

の両方を満たす事である.
(証明) (i) 定理 7.18.(b) によって, 仮定から $z^{2^n-1} \equiv 1 \pmod{4, f(z)}$ が成り立つ. 故に定理 7.17.(a) によって, すべての整数 $r \geqq 2$ に対してこの両辺の 2 乗を $r-2$ 回繰り返して

$$z^{2^{r-2}(2^n-1)} \equiv 1 \pmod{2^r, f(z)}$$

を得る. 法 2^r での漸化式系列の周期 T は $z^T \equiv 1 \pmod{w^r, f(z)}$ となる最小の T だから, 上の式は $T \leqq 2^{r-2}(2^n - 1) <$ 最長周期 $2^{r-1}(2^n - 1)$ を $r \geqq 2$ に対して証明する.
(ii) 定理 7.18.(a) によって, 仮定から $z^{2^n-1} \equiv -1 \pmod{4, f(z)}$ が成り立つ. 故に定理 7.17.(a) によって, 両辺の 2 乗を $r-2$ 回繰り返すと

$$z^{2^{r-2}(2^n-1)} \equiv 1 \pmod{2^r, f(z)},\ \ r \geqq 3,$$

を得る. これは漸化式周期 $T \leqq 2^{r-2}(2^n - 1) <$ 最長周期 $2^{r-1}(2^n - 1)$ を証明する.
(iii) **[必要性]** 上の (i),(ii) によって, (7.29a) が成り立てば $r \geqq 3$ に対して, (7.29b) が成り立てば $r \geqq 2$ に対して, 漸化式系列は最長周期 $2^{r-1}(2^n - 1)$ を持たない. 故に対偶としてすべての $r \geqq 2$ に対して最長周期であるためには (7.29a,b) がどちらも成り立たない事が必要である.
[十分性] $\boldsymbol{Z}_2$ 原始多項式[79] $f(z)$ が (7.47a,b) を満たさないと仮定する. $\boldsymbol{Z}_2$ での漸化式系列周期は最長の $2^n - 1$ だから法 4 での漸化式周期はこれと同じか最長の $2(2^n - 1)$ か, の二者択一である. 定理 7.18.(b) によって, $z^{2^n-1} \equiv 1 \pmod{4, f(z)}$ は成り立たないから $2^n - 1$ は漸化式系列の法 4 での周期は最長の $2(2^n - 1)$ 以外はあり得ない. 法 8 での周期は従ってこれと同じか或いは最長の $2^2(2^n - 1)$ かの二者択一となる. 前者は $z^{2(2^n-1)} \equiv 1 \pmod{8, f(z)}$ を意味するが, Lemma 7.17.(b) によるとこれは $z^{2^n-1} \equiv \pm 1 \pmod{4, f(z)}$ と同値であり, それは仮定によって成立しない. 故に法 8 での漸化式周期も最長であり, Ward の定理 7.14.(b) によってすべての $r \geqq 2$ に対して法 2^r での漸化式系列の最長周期が保証される. ■

実際は Brent の上の十分性の証明は Ward の定理 7.14. にも頼る事なく簡明に帰納的に行われる. 可能なら是非原著の端的な証明を読み解いて頂きたい.

加算生成法の理論解析の最後である:

[79] $f(z)$ の $\boldsymbol{Z}_2$ 既約性だけを仮定しても $2^n - 1$ を $f(z)$ の指数に置き換えて以下の証明は成り立つ.

定理 7.15.(b) (Brent) 次数 $n \geqq 3$ の時, n 次原始 3 項式 $f(z)$ は任意の $r = 1, 2, \cdots$ に対して法 2^r の加算生成法の最長周期を保証する.

(証明) Brent の証明の通り述べる. $\boldsymbol{Z}_2$ 上の原始特性 3 項式を $f(z) = z^n + b_s z^{n-s} + b_n$ とする. 当然 b_n も b_s も奇数, 法 2 で 0 ではない, 即ち法 2^r での可逆元である. Brent の条件の第 1,

$$f^2(z) + f^2(-z) \not\equiv 2f(z^2) \pmod 8 \tag{7.29a}$$

の成立を見よう. 逆があり得ないと示せばよい. (7.29a) の左辺を $f(z)$ の場合に展開すると次が成り立つ:

$$\begin{aligned}&(z^n + b_s z^{n-s} + b_n)^2 + \{(-1)^n z^n + (-1)^{n-s} b_s z^{n-s} + b_n\}^2 \\ &\quad = 2z^{2n} + 4b_s\gamma_s z^{2n-s} + 2{b_s}^2 z^{2n-2s} + 4b_n\gamma_n z^n + 4b_n b_s \gamma_{n-s} z^{n-s} + 2{b_n}^2, \end{aligned} \tag{7.48}$$

但し $\gamma_k := \dfrac{1 + (-1)^k}{2}$, k が偶数なら 1, 奇数なら 0 である. 一方 $2f(z^2) = 2z^{2n} + 2b_s z^{2n-2s} + 2b_n$ である. これが (7.48) と法 8 で合同であるためには, $2n-s > n > n-s$ かつ $2n-s > 2n-2s > n-s$ だから,

$$4b_s\gamma_s \equiv 0 \pmod 8, \tag{7.49}$$

$$2({b_s}^2 z^{2n-2s} + 2b_n\gamma_n z^n) \equiv 2b_s z^{2n-2s} \pmod 8, \tag{7.50}$$

$$2b_n b_s \gamma_{n-s} \equiv 0 \pmod 8, \tag{7.51}$$

$$2b_n^2 = 2b_n \pmod 8 \tag{7.52}$$

が成り立たなければならない. b_s, b_n は奇数, γ_k も 0 か 1 かである. (7.49) は $\gamma_s = 0$, s は奇数と定める. (7.51) は $\gamma_{n-s} = 0$, $n-s$ は奇数, 従って n は偶数であり, $\gamma_n = 1$ でなければならない. こうして (7.51) は

(i) $n = 2s$ かつ $2(b_s^2 - b_s + 2b_n)z^n \equiv 0 \pmod 8$ が成り立つか, 或いは

(ii) $n \neq 2s$, $2b_s^2 \equiv 2b_s$ かつ $4b_n \equiv 0 \pmod 8$ がすべて成立するか,

のどちらかを要求する. しかし b_n は奇数だから $4b_n \not\equiv 0 \pmod 8$, (ii) はあり得ないので (i) の $n = 2s \geqq 3,\ \ s \geqq 2$ とその他の条件, 例えば (7.52) の成立の可能性だけが残る. しかしこれは法 2 で見て $f(z) \equiv z^{2s} + z^s + 1$ を意味し, この形の $f(z)$ は $s \geqq 2$ の場合 $\boldsymbol{Z}_2$ 原始多項式ではあり得ない. なぜなら, これは $f(z) = 0$ の $\mathrm{GF}(2^n)$ での根 α が $\alpha^{2s} \equiv \alpha^s + 1 \pmod 2$ を満たす事を意味し, 次が成り立つ:

$$\alpha^{3s} = \alpha^{2s} \cdot \alpha^s \equiv (\alpha^s + 1)\alpha^s = \alpha^{2s} + \alpha^s \equiv 1 \pmod 2.$$

故に $f(z) = 0$ の根 α の位数 h は $3s$ 或いはそれ以下の大きさのその約数だが, 一方それは $\mathrm{GF}(2^n)$ の生成元で $h = 2^n - 1 = 2^{2s} - 1$ でなければならない. 関数

$$\xi(s) = 2^{2s} - 1 - 3s = 4^s - 1 - 3s$$

を用いて言えば, 整数 $s \geqq 1$ は $\xi(s) \leqq 0$ を満たさなければならない. しかし

$$\xi'(s) = (e^{s\log 4})' - 3 = (\log 4)e^{2s\log 2} - 3 = (\log 4)4^s - 3$$

によって $\xi'(s)$ は s の増加関数, $\xi'(s) = 0$ となるのは $s = \dfrac{\log 3 - \log\log 4}{\log 4} = 0.55686\cdots$ だ

け, $\xi(s)$ は $s \geqq 1$ で狭義単調増加, $\xi(1) = 4-1-3 = 0$ だから $s > 1$ で $\xi(s) > 0$ であり, $s > 1$, 即ち特性多項式 $f(z)$ の次数 $n = 2s > 2$ では条件 $\xi(s) \leqq 0$ が成り立つ事, 即ち (7.48) が成り立つ事はない. 故に次数 $n \geqq 3$ の $\boldsymbol{Z}_2$ 原始 3 項式 $f(z)$ について (7.29a) の不成立はなく, 必ず成立する.

Brent の条件の今 1 つである (7.29b), $f^2(z) + f^2(-z) \not\equiv 2(-1)^n f(-z^2) \pmod 8$ が満たされる事を見よう. $f(z) = z^n + b_s z^{n-s} + b_n$ の最高次 z^n の係数を 1 に取る約束だから,

$$F(z) := (-1)^n f(-z) = z^n + (-1)^s b_s z^{n-s} + (-1)^n b_n$$

を考える; $f(z) \equiv F(z) \pmod 2$ で, $f(z)$ が $\boldsymbol{Z}_2$ 原始 3 項式なら $F(z)$ も同じである. Brent の $f(z)$ に対する条件 (7.29b) を $F(z)$ で表すと,

$$F^2(z) + F^2(-z) \not\equiv 2F(z^2),$$

これは原始 3 項式 $F(z)$ に対する条件 (7.29a) で, $n \geqq 3$ に対してこれが満たされない事は上で示されている. ■

勿論次数 $n = 2$ の $\boldsymbol{Z}_2$ 原始 3 項式では Brent の条件を満たさないものがある. 3 項式と限らない, 加算生成法最長周期を与えない $\boldsymbol{Z}_2$ 原始多項式については Brent の原論文に「例外的 exceptional$\boldsymbol{Z}_2$ 原始多項式」としていくつかの低次のものが記されている.

7.4. 演習問題

Brent の定理の強力さを簡単な演習問題で確認して最後の旅へ進む.

問題 7.19.(a) $\boldsymbol{Z}_2$ 上の 2 次多項式 $f(z) = z^2 - z + 1$ が原始多項式である事を示せ.
(解) 我々の学んだ所では, その証明にはこの $f(z)$ を特性多項式とする漸化式

$$x_k = x_{k-1} - x_{k-2} \pmod 2, \quad k = 2, 3, \cdots \tag{7.52}$$

が任意の出発 2 連(但し 0 連ではないとする)に対して作る系列の周期 T が最長の $T = 2^2 - 1 = 3$ である事を見てもよい. ここでは $2^2 - 1 = 3$ はメルセンヌ素数だから

$$z^{2^2} \equiv z \pmod{2, f(z)}$$

の成立を 2 度の 2 乗で調べよう. 実際

$$f(z) = z^2 - z + 1 \equiv 0 \pmod{2, f(z)} \text{ だから } z^2 \equiv z - 1 \pmod{2, f(z)}$$

であり, この関係を 2 乗して

$$z^4 = (z^2)^2 = (z-1)^2 = \equiv z^2 + 1 \equiv (z-1) + 1 = z \pmod{2, f(z)}.$$

従って $f(z)$ は $\boldsymbol{Z}_2$ 上の 2 次原始多項式である. ■

問題 7.19.(b) しかし $f(z) = z^2 - z + 1$ は法 $2^r,\ r \geqq 3$ で加算生成法の最長周期を与えない. それをまず,
(i) $f(z)$ が Brent の条件

$$f^2(z) + f^2(-z) \not\equiv 2f(z^2) \pmod 8 \tag{7.29a}$$

$$f^2(z) + f^2(-z) \not\equiv 2(-1)^n f(-z^2) \pmod 8 \tag{7.29b}$$

の 2 つを満たすかどうかによって調べなさい.
(ii) 次に初期条件 $(x_0 = 1, x_1 = 1)$ で法 2,4,8 の加算生成法系列を作り, それらの周期を Brent の定理 7.18. の証明に基づいて説明しなさい.
(解) (i) 条件 (7.29a) については,

$$\begin{aligned} f^2(z) + f^2(-z) &= (z^2 - z + 1)^2 + (z^2 + z + 1)^2 \\ &= z^4 + z^2 + 1 - 2z^3 - 2z + 2z^2 + z^4 + z^2 + 1 + 2z^3 + 2z + 2z^2 \\ &= 2z^4 + 6z^2 + 2 \pmod 8, \\ 2f(z^2) &= 2z^4 - 2z^2 + 2 \equiv 2z^4 + 6z^2 + 2 \pmod 8. \end{aligned}$$

故に (7.29a) は破れている. (7.29b) については, $n = 2$ だから,

$$(-1)^n f(-z^2) = 2f(-z^2) = 2z^4 + 2z^2 + 2 \not\equiv 2z^4 + 6z^2 + 2 = f^2(z) + f^2(-z) \pmod 8.$$

だから (5.29b) は満たしている.
(ii) 法 2 では漸化式 (7.52), $x_k = x_{k-1} - x_{k-2}$ の解は次の通り:

k	0	1	2	3	4	5	6	7
x_k	1	1	0	1	1	0	1	1

法 $4 = 2^2$ では

k	0	1	2	3	4	5	6	7
x_k	1	1	0	-1	-1	0	1	1

法 $8 = 2^3$ では

k	0	1	2	3	4	5	6	7
x_k	1	1	0	-1	-1	0	1	1

法 $4 = 2^2$ での周期は $6 = 2^{2-1} \times (2^2 - 1)$, 最長である. 定理 7.18.(a) によれば, (7.29b) の成立は $z^3 \equiv -1 \pmod{4, f(z)}$ となる事, それは法 4 で漸化式の周期が最長の 6 である事だが, が法 $(8, f(z))$ でも $z^6 \equiv 1$, となる条件で, 上に見る通りそうなっている. 法 8 での周期は $6 = 2(2^2 - 1)$, 理論的最長の $2^{3-1}(2^2 - 1) = 4(2^2 - 1) = 12$ ではない. この周期の理由は上に見た (7.29a) の不成立にある. **(問題 7.19.(b) 終り)**

上で見た $\boldsymbol{Z}_2$ 上の 2 次原始 3 項式 $f(z) = z^2 - z + 1$ は Brent の所謂例外的原始多項式の 1 つである.

問題 7.19.(c) 2 次多項式 $g(z) = z^2 + z + 1$ は法 2 では問題 7.19.(a,b) の $f(z) = z^2 - z + 1$ と同じだから $\boldsymbol{Z}_2$ 上の 2 次原始多項式であるが法 4 或いは法 8 では $f(z)$ とは異なる. $g(z)$ を特性多項式とする線形漸化式

$$x_k = -x_{k-1} - x_{k-2} \pmod{2^r}, \quad k = 2, 3, \cdots, \quad r = 1, 2, \cdots \qquad (7.53)$$

も法 $2^r,\ r \geqq 3$ で加算生成法の最長周期を与えない. それをまず,
(i) $f(z)$ が Brent の条件

$$g^2(z) + g^2(-z) \not\equiv 2g(z^2) \pmod 8 \qquad (7.29a)$$

$$g^2(z) + g^2(-z) \not\equiv 2(-1)^n g(-z^2) \pmod 8 \qquad (7.29b)$$

を満たすかどうかによって調べなさい.
(ii) 次に初期条件 $(x_0 = 1, x_1 = 1)$ で法 2,4,8 の加算生成法系列を作り, それらの周期を Brent の定理 7.18. の証明に基づいて説明しなさい.
(解) (i) 条件 (7.29a) については,

$$\begin{aligned} g^2(z) + g^2(-z) &= (z^2 + z + 1)^2 + (z^2 - z + 1)^2 \\ &= z^4 + z^2 + 1 + 2z^3 + 2z + 2z^2 + z^4 + z^2 + 1 - 2z^3 - 2z + 2z^2 \\ &= 2z^4 + 6z^2 + 2 \pmod 8, \\ 2g(z^2) &= 2z^4 + 2z^2 + 2 \not\equiv 2z^4 + 6z^2 + 2 \pmod 8. \end{aligned}$$

故に (7.29a) は満たされている. (7.29b) については, $n = 2$ だから,

$$(-1)^n g(-z^2) = 2g(-z^2) = 2z^4 - 2z^2 + 2 \equiv 2z^4 + 6z^2 + 2 = f^2(z) + f^2(-z) \pmod 8.$$

だから (7.29b) は満たされない. 故に最長周期を与えない.
(ii) 法 2 では漸化式 (7.53), $x_k = -x_{k-1} - x_{k-2} \equiv x_{k-1} + x_{k-2} \pmod 2$ の解は次の通り:

k	0	1	2	3	4	5	6	7
x_k	1	1	0	1	1	0	1	1

法 $4 = 2^2$ では $x_k = -x_{k-1} - x_{k-2} \pmod 4$ でなければならず,

k	0	1	2	3	4	5	6	7
x_k	1	1	2	1	1	2	1	1

これは周期 3 である. 法 $8 = 2^3$ では

k	0	1	2	3	4	5	6	7
x_k	1	1	6	1	1	6	1	1

これも周期 3 である. 法 $4 = 2^2$ での最長周期は $6 = 2^{2-1} \times (2^2 - 1)$ だからこれよりは短い. (7.29a) が成り立たつから Brent の予備定理 7.18.(b) によって法 $(4, g(z))$ で $z^{2^n-1} = z^{2^2-1} \equiv -1$ **ではなく**, (7.29b) が成り立たないために同じ法で $z^{2^2-1} \equiv 1$ となって法 4 で線形漸化式周期は法 2 の時のままの $2^n - 1 = 2^2 - 1$ に留るのである. 実際線形漸化式 (7.53) は任意の整数 $r \geqq 2$ に対して法 2^r での解が

$$1 \quad 1 \quad -2 \quad 1 \quad 1 \quad -2 \quad \cdots$$

の繰返しとなって周期はすべて 3 である. **(問題 7.19.(c). 終り)**

問題 7.19.(d) $h(z) = z^2 - z + 3$ も $\boldsymbol{Z}_2$ 上原始的な $f(z) = z^2 - z + 1$ と「$\boldsymbol{Z}_2$ で係数を見れば」同じで, それ自身 $\boldsymbol{Z}_2$ 原始 $n = 2$ 次多項式である. これについて $h^2(z) + h^2(-z)$ と $2h(z^2)$ とを法 8 で計算し, Brent の条件

$$h^2(z) + h^2(-z) \not\equiv 2h(z^2) \pmod 8, \qquad \text{(7.29a)}$$

$$h^2(z) + h^2(-z) \not\equiv 2(-1)^2 h(-z^2) \pmod 8 \qquad \text{(7.29b)}$$

が満たされている事を示せ.
(証明) $h^2(z) \equiv z^4 - 2z^3 + 7z^2 - 6z + 1 \pmod 8,$

$$h^2(-z) = (z2 + z + 3) \equiv z^4 + 2z^3 + 7z^2 + 6z + 1 \pmod 8.$$

加え合せて

$$h^2(z) + h^2(-z) \equiv 2z^4 + 14z^2 + 2 \equiv 2z^4 + 6z^2 + 2 \pmod 8.$$

一方

$$2h(z^2) \equiv 2(z^4 - z^2 + 3) \equiv 2z^4 + 6z^2 + 6 \not\equiv 2z^4 + 6z^2 + 2 \pmod 8.$$

よって (7.29a) は示された. さらに,

$$\begin{aligned} 2(-1)^2 h(-z^2) &= 2(z^4 - z^2 + 3) \equiv 2z^4 - 2z^2 + 6 \\ &\not\equiv 2z^4 + 6z^2 + 2 = h^2(z) + h^2(-z) \pmod 8. \end{aligned}$$

よって示された. ■

問題 7.19.(e) $h(z) = z^2 - z + 3$ は漸化式

$$x_k = x_{k-1} - 3x_{k-2} \tag{7.54}$$

の特性多項式である. $(x_0, x_1) = (1, 1)$ から出発する法 4 の漸化式 (6) の解を下の表に x_9 まで計算し, その周期 T_4 を求めよ.

(解) 次の通り:

k	0	1	2	3	4	5	6	7	8	9
x_k	1	1	2	3	1	0	1	1	2	3

故に法 4 での $\{x_k\}$ の周期 $T_4 = 6 = 2^{2-1}(2^2 - 1)$, 最長周期である. **(問題 7.19(e) 終り)**

問題 7.19.(f) 同じ $h(z) = z^2 - z + 3$ が特性多項式である「法 8 の」漸化式

$$x_k = x_{k-1} - 3x_{k-2} \pmod 8 \tag{7.55}$$

を同じ出発値 $(x_0, x_1) = (1, 1)$ で解いて x_{17} まで計算し, その周期 T_8 を求めよ.
(解) 次の通り:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
x_k	1	1	6	3	1	0	5	5	6	7	5	0	1	1	6	3	1	0

故に法 8 での $\{x_k\}$ の周期は $T_8 = 12 = 2^{3-1}(2^2 - 1)$, 最長である. **(問題 7.19.(f) 終り)**

問題 7.19(b,c) の $g(z) = z^2 + z + 1,\ h(z) = z^2 - z + 3$ 等は法 2 で見れば Brent の「例外的」$\boldsymbol{Z}_2$ 原始多項式 $f(z) = z^2 - z + 1$ と同じである. $f(z), g(z)$ は問題 7.19.(a,b) で見た様に Brent の条件の 1 つを満たさず, 加算生成法の最長周期を与えない. しかし上の通り $h(z)$ はそうではない. この事がちゃんと, 法 4 及び法 8 での $h(z)$ が生起する加算生成法漸化式の解に反映し, 従って全ての法 $2^r,\ r \geqq 1$ で最長周期を与える. ややこしい状況をきちんと捌いている Brent の判定条件の強力さは見事である.

問題 7.20.(a) $\boldsymbol{Z}_2$ 上の 4 次多項式 $f(z) = z^4 + z^3 + 1$ が原始多項式である事を示そう. それにはこの $f(z)$ を特性多項式とする漸化式

$$x_k = x_{k-1} + x_{k-4} \pmod 2, \quad k = 4, 5, 6, \cdots \tag{7.56}$$

が任意の (但し 0 ばかりではない) 出発 5 連に対して作る系列の周期 T が最長の $2^4 - 1 = 15$

である, と見ればよい. 出発値 $(x_0, x_1, x_2, x_3,) = (1, 0, 0, 0)$ に対して, $\{x_0, x_1, x_2, x_3, \cdots, x_{18}\}$ までを (1) に従って計算して周期 15 であり, $f(z)$ が $\boldsymbol{Z}_2$ 上の原始多項式である事を証明せよ.
(証明) 次の通り:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
x_k	1	0	0	0	1	1	1	1	0	1	0	1	1	0	0	1	0	0	0

周期は最長の $2^4 - 1 = 15$ であり, $\{x_k\}$ は M 系列で $f(z)$ は $\boldsymbol{Z}_2$ 上の 4 次原始多項式である.
■

問題 7.20.(b) $f(z) = z^4 + z^3 + 1$ が $\boldsymbol{Z}_2$ 原始多項式である事が判ったから, この上での法 $2^2 = 4$ の加算生成法

$$x_k = x_{k-1} + x_{k-4} \pmod 4, \quad k = 4, 5, 6, \cdots \tag{7.57}$$

を行って見よう. 3 次以上の $\boldsymbol{Z}_2$3 項 M 系列漸化式についての Brent の定理から 周期は可能な最長周期, $2^{2-1}(2^4 - 1) = 30$ だと判る. 出発値は問題 7.20.(a) と同じ $(x_0, x_1, x_2, x_3) = (1, 0, 0, 0)$ に取り, $\{x_0, x_1, x_2, x_3, \cdots, x_{35}\}$ までを (7.55) に従って計算してこの周期を確かめよ.
(解) 次の通り:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
x_k	1	0	0	0	1	1	1	1	2	3	0	1	3	2	2	3	2	0	2

k	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
x_k	1	3	3	1	2	1	0	1	3	0	0	1	0	0	0	1	1

(問題 7.20.(b) 終り)

問題 7.20.(c) 法 $2^2 = 4$ の加算生成法,

$$x_k = x_{k-1} + x_{k-4} \pmod 4, \quad k = 4, 5, 6, \cdots \tag{7.58}$$

で得られた系列の Marsaglia 図は, 値に重複があるので描きにくい. 下の表に問題 7.20.(b) の解から $0 \leqq k \leqq 29$ に対する (x_k, x_{k+1}) の 30 点の出現頻度を集計せよ.
(解)

3	0	3	2	1
2	1	2	1	2
1	4	3	2	1
0	3	2	1	2
x_{k+1} / x_k	0	1	2	3

(問題 7.20.(c) 終り)

問題 7.20.(d) 同じ法 $2^2 = 4$ の 4 次加算生成法

$$x_k = x_{k-1} - x_{k-4} \pmod 4, \quad k = 4, 5, 6, \cdots \tag{7.59}$$

はこれを法 2 で見れば $x_k = x_{k-1} + x_{k-4}$ と同じ事だから特性多項式は $\boldsymbol{Z}_2$ 上の 4 次原始 3 項式で, これも Brent の定理によって任意の $r = 1, 2, \cdots$ に対する法 2^r での加算生成法として最長周期を保証され, 現在の $r = 2$, 法 4 の場合の (7.59) の解の周期は $2^{2-1}(2^4 - 1) = 30$ で

ある. 出発値を再び $(x_0, x_1, x_2, x_3) = (1, 0, 0, 0)$ に取り, $\{x_0, x_1, x_2, x_3, \cdots, x_35\}$ までを (4) に従って計算しせよ. 但し -1 は 3 で表し, $0, 1, 2, 3$ だけを用いる事とする. また $0 \leqq k \leqq 29$ に対する 30 点 (x_k, x_{k+1}) の出現頻度の結果を下の表に集計せよ.

(解) 法 4 の加算生成列は次の通り:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
x_k	1	0	0	0	3	3	3	3	0	1	2	3	3	2	0	1	2	0	0

k	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
x_k	3	1	1	1	2	1	0	3	1	0	0	1	0	0	0	3	3

Marsaglia 図については:

3	3	0	1	4
2	0	3	0	1
1	3	2	1	2
0	4	3	2	1
x_{k+1} / x_k	0	1	2	3

(問題 7.20.(d) 終り)

問題 7.20.(e) 今度はさらに大きい法 $2^3 = 8$ の 4 次加算生成法

$$x_k = x_{k-1} + x_{k-4} \pmod 8, \quad k = 4, 5, 6, \cdots \tag{7.58}$$

でどの様になるかを見よう. 周期は最長の $2^{3-1}(2^4 - 1) = 60$ のはずである. 出発値をまた $(x_0, x_1, x_2, x_3) = (1, 0, 0, 1)$ に取り, $\{x_0, x_1, x_2, x_3, \cdots, x_{65}\}$ までを (2') に従って計算せよ. また $0 \leqq k \leqq 59$ に対する 60 点 (x_k, x_{k+1}) の出現頻度の結果を (0 は記入せず) 下に集計せよ.

(解) 法 8 では加算生成列は次の様になる:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
x_k	1	0	0	0	1	1	1	1	2	3	4	5	7	2	6	3	2

k	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
x_k	4	2	5	7	3	5	2	1	4	1	3	4	0	1	4	0	0

k	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
x_k	1	5	5	5	6	3	0	5	3	6	6	3	6	4	2	5	3

k	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65
x_k	7	1	6	1	0	1	7	0	0	1	0	0	0	1	1

Marsaglia 図については:

7		1		1		2		
6		1	1	2		1	1	
5	1	1	2	1		2		
4		2	1	1	1		1	
3		1		1		2		1
2		1	1	1	2	1	3	1
1	5	3	1		1		1	1
0	4	2		1	2			1
$x_{k+1}\,/\,x_k$	0	1	2	3	4	5	6	7

(問題 7.20.(e) 終り)

法 8 の場合の集計から, 法を大きくすると周期は確かに長くなるが, 系列 $\{x_k\}$ の数の出方に「癖」が生じる様に感じられる. 低次の漸化式で大きな r に対する法 2^r の加算生法を行うのは良くないと注意される. この様な実際使用は避けよう.

上の問題 7.20. と共に, 次は加算生成法の問題点を多少とも示す例である.

問題 7.21.(a) $\boldsymbol{Z}_2$ 上の 5 次多項式 $f(z)=z^5+z^3+1$ は原始多項式である. これは $2^5-1=31$ が素数, 5 が Mersenne 指数である事から, $z^{2^5}\equiv z \pmod{2, f(z)}$ の成立を調べればわかる. 実際 $f(z)\equiv 0 \pmod{2, f(z)}$ だから同じ法で

$$z^5\equiv z^3+1,\quad z^6\equiv z^4+z,$$

$$z^8\equiv z^3z^5\equiv z^3(z^3+1)\equiv z^6+z^3\equiv z^4+z^3+z,$$

$$z^{16}=(z^8)^2\equiv (z^4+z^3+z)^2\equiv z^8+z^6+z^2\equiv (z^4+z^3+z)+(z^4+z)+z^2\equiv z^3+z^2,$$

$$z^{32}\equiv (z^3+z^2)^2\equiv z^6+z^4=(z^4+z)+z^4\equiv z.$$ ■

問題 7.21.(b) Brent の定理 7.15.(b) によって, $\boldsymbol{Z}_2$ 上の $5(\geq 3)$ 次原始 3 項式 $f(z)=z^5+z^3+1$ を特性多項式とする線形漸化式は任意の法 2^r, $r=1,2,3,\cdots$ で最長周期 $2^{r-1}(2^5-1)$ を持つと知れる. 余り周期が長いと計算が大変だから, 法 $2^2=4$ の加算生成法,

$$x_k=x_{k-2}+x_{k-5} \pmod 4,\quad k=5,6,\cdots \tag{7.60}$$

を行って見よう. 周期は $2^{2-1}(2^5-1)=62$ である. 出発値は $(x_0,x_1,x_2,x_3,x_4)=(1,0,0,0,0)$ に取り, $(x_0,x_1,x_2,\cdots,x_{70}\}$ までを計算してこの周期を確かめよ.

(証明) 長いけれど単純な計算である:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
x_k	1	0	0	0	0	1	0	1	0	1	1	1	2	1	3	2	0	0

k	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
x_k	1	3	3	3	3	0	2	3	1	2	1	0	0	1	2	2	2	2

k	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
x_k	3	0	1	2	3	1	3	2	1	1	2	0	0	1	1	3	1	3

k	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70
x_k	2	0	1	1	0	3	0	0	1	0	0	0	0	1	0	1	0

確かに, 周期は 62 である. ■

問題 7.21.(c) 法 $2^2 = 4$ の加算生成法 $x_k = x_{k-2} + x_{k-5} \pmod 4,\ \ k = 5, 6, \cdots$ で得られた (c) の系列の Marsaglia 図は, 値に重複があるので描きにくい. 次の表に問 (b) の解から $0 \leqq k \leqq 61$ に対する 62 点 (x_k, x_{k+1}) の出現頻度を集計せよ.

(解)

3	1	5	3	3
2	1	5	3	3
1	9	5	3	3
0	7	5	3	3
x_{k+1} / x_k	0	1	2	3

結果は, 表の右半分は大変良いが, 左半分の性能がよくわからない. **(問題 7.21.(c) 終り)**

問題 7.21.(d) 同じ法 4 の 5 次加算生成法 $x_k = x_{k-2} + x_{k-5} \pmod 4,\ \ k = 5, 6, \cdots$ で出発値として取り得る 5 連は, 最長周期 $T = 2^{2-1}(2^5 - 1) = 62$ を確保するため法 2 での 0 の 5 連, 即ち法 4 での偶数ばかりの 5 連 2^5 個を除く $4^5 - 2^5 = 2^5(2^5 - 1) = 16T$ 個で, 異なる加算生成法最長周期系列解が 16 個ある事になる. これら異なる初期値に対する系列の性質は互いに大いに異なり得る. 出発値を (c) と異なる $(x_0, x_1, x_2, x_3, x_4) = (1, 0, 0, 0, 2)$ に取り, $\{x_0, x_1, x_2, \cdots, x_{70}\}$ までを計算せよ. また $0 \leqq k \leqq 61$ に対する 62 点 (x_k, x_{k+1}) の出現頻度の結果を下の表に集計せよ. (c) と (d) とどちらの出発値が乱数として好ましいか.

(解) 再び長い単純な計算である:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
x_k	1	0	0	0	2	1	2	1	2	3	3	1	0	3	3	2	0	2

k	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
x_k	3	1	1	1	3	0	0	1	1	0	1	0	2	1	2	2	2	0

k	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
x_k	3	2	1	0	1	3	3	0	3	1	2	0	2	3	3	1	3	3

k	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70
x_k	2	2	3	1	2	3	0	2	1	0	0	0	2	1	2	1	2

3	3	3	5	5
2	5	5	3	3
1	3	3	5	5
0	3	5	3	3
x_{k+1} / x_k	0	1	2	3

出現頻度表からは (d) の結果の方が均等らしく好ましく見える. **(問題 7.21.(d) 終り)**

確かな事として, 加算生成法乱数の 1 周期での性格も上の 2 例の様に初期条件の選択に依存すると言う事はできる. これは連結 M 系列乱数についても同じである.[45] しかし「どの様に依存するか」について, 或いは「大した違いは生じないのか」について, 何分にも上の例では乱数としては出現する場合の総数が小さ過ぎ, 法 2^2 に対する乱数値の 2^{-2} 毎の刻み幅

も大き過ぎるので確定的な事が何も言えない. 現在の計算機では系列全体を到底計算し尽くせない 500 次の漸化式で法 2^{32} の加算生成法の 1 周期を想起しよう. この時 2^{500} 程度の点が 2^{32} 個の値の一様乱数として 2 次元平面の 1 辺の長さ 1 の正方形内で $(2^{32})^2 = 2^{64}$ 個の点に散布され, 各点には平均頻度 $2^{500}/2^{64} = 2^{436} \approx 10^{3\times 43.6} \approx 10^{130}$ で出現する. この数は膨大だから少々の不均等では $\cdots$ とも感じられるが, しかしこれも本当と言えるだろうか. 特に 1 周期ではなく, 実際に用いられる遥かに短い長さの範囲で実際はどれくらいの不均等になるか, 独立乱数列と見做すのに問題はないか. さらに大きな問題, 漸化式あるいは原始多項式の選択, と共に「よくわからない」と言うべきであり, 加算生成法のそのままの使用には問題が感じられる.

繰り返しにはなるが, 幸い加算生成法乱数出力列から性質のよりよい部分列を抽き出すアイデアが Lüscher[13] によって提案されている事を再度指摘する. Knuth[52] の p.35 及び Sec. 3.6. も参照. 簡単だが実際に効果が高いと思われるこの改善案は, 乱数生成速度の多少の犠牲を伴う [53] にしても, 加算生成法でシミュレーションを行う立場では十分考慮されるべき重要な指針と思われる.

8. 2つの展望

8.1. イデアル, ユークリッドの互除法と素 (既約) 因数分解

整数の合同算法から始めて, 我々は群, 体そして環の入り口まで進んだ. 議論の困難の中の1つの共通事項は, 多項式の既約因数分解の一意性の問題に関わっている. 最終の段階に立って振り返ると, もう1つの重要な共通事項, 整数で言えば最大公約数をどう算出するか, 素数と限らない法 m での数体系で或いは一般に多項式の環でどの様に可逆元とその「逆数」とを発見するか, についての一般の議論の欠落も指摘しなければならない. 関連する多少の記述は余り大きな努力なしに可能だし, それはまたこれからの発展, もっと進んだ教科書に目を向ける時容易な移行を見出すかどうかに大いに関わると思われる. そこで我々が今まで主として「群」の世界に安住できて触れる機会がなかったこれらの重要な構造, ユークリッドの互除 (算) 法と環のイデアル, にこの最終章の第1段として少し立ち入る.

群で部分群が全体構造に大切な役割を持っていた様に, 群にはない2種類の演算に関係する環特有のある種の部分集合の役割がある. この部分集合がイデアルである. これを考える事はまた, 懸案の, 体の元或いは整数を係数とする多項式の既約因数分解の一意性の理解への鍵でもある. まず, 次の定義から始める:

定義 8.1. 環 R の部分集合 J が次の性質を満たすとき「イデアル ideal」と呼ぶ:
(公理 1) J は環 R の加法について R の部分群である. 即ち $x, y \in J$ なら $x - y \in J$ が成り立つ.
(公理 2) 環 R の任意の元 $x \in R$ について $xJ \subset J$ を満たす, 即ち任意の $y \in J$ に対して $xy \in J$ となる. xJ は集合 $\{xy|\ y \in J\}$ の略記である. **(定義 8.1. 終り)**

イデアルの具体例は容易に見られる:

例 8.2. (a) 環 R の零元だけの集合 $J = \{0\} = 0R = \{0x|\ x \in R\}$, 及び R 自体もイデアルである. これらを環 R の自明なイデアルと呼ぶ.
(b) (0 でない) 整数 a の倍数全体を

$$(a) := a\boldsymbol{Z} = \{ak|\ k = 0, \pm 1, \pm 2, \cdots\}$$

と記す.[80] $a\boldsymbol{Z}$ は整数環 $\boldsymbol{Z}$ のイデアルである.
(c) 例 7.2.(d) によれば, 整数環 $\boldsymbol{Z}$ を係数とする文字 z の多項式の全体 $\boldsymbol{Z}[z]$ は環である. この中の任意の多項式を $f(z) \in \boldsymbol{Z}[z]$ とすれば, $f(z)$ を因数に持つ $\boldsymbol{Z}[z]$ の全体, 即ち $\boldsymbol{Z}[z]$ の中の $f(z)$ の倍数全体,

$$f(z)\boldsymbol{Z}[z] := \{f(z)g(z)|\ g(z) \in \boldsymbol{Z}[z]\}$$

[80] 記法 (a) は我々には少し紛らわしいので以後は $a\boldsymbol{Z}$, 一般の環 R なら aR を主に用いる.

は $\boldsymbol{Z}[z]$ のイデアルである.

(証明) (a) $J = \{0\}$ は加法の群 R の自明な部分群である. 任意の $x \in R$ に対して $x0 = 0 \in J$ も明らかで $\{0\}$ はイデアルには違いない. R 自体も同様に R の加法の部分群と考える事はでき, $xR \subset R$ も確かだからイデアルではある.

(b) $a\boldsymbol{Z} = (a)$ は自明に環 $\boldsymbol{Z}$ の部分集合である. $ak, am \in a\boldsymbol{Z}$ を任意に取ると, k, m は整数だから $ak - am = a(k - m)$ は再び a の倍数で $a\boldsymbol{Z}$ の元になる. 故に J は加法に関して $\boldsymbol{Z}$ の部分群の条件 Lemma 2.14.(a) を満たし, イデアルの公理 1 は成り立っている. 任意の整数 x について, $xa\boldsymbol{Z} = a(x\boldsymbol{Z}) \subset a\boldsymbol{Z}$ も明らかで, $a\boldsymbol{Z}$ に対してイデアルの公理 2 も成立する.

(c) 任意の整数係数多項式 $g(z),\ h(z) \in f(z)\boldsymbol{Z}[z]$ は $g(z) = f(z)u(z)$, $h(z) = f(z)v(z)$ の様に整数係数多項式 $u(z), v(z)$ で表される. 故に $g(z) - h(z) = f(z)\{u(z) - v(z)\}$ であり, $f(z)$ の倍数であって, $g(z) - h(z) \in f(z)\boldsymbol{Z}[z]$ が成り立つ. $f(z)\boldsymbol{Z}[z]$ は加法に関して $\boldsymbol{Z}[z]$ の部分群である. また任意の $w(z) \in \boldsymbol{Z}[z]$ を取ると $w(z)\{f(z)u(z)\} = f(z)\{w(z)u(z)\} \in f(z)\boldsymbol{Z}[z]$ も明らかで, $f(z)R$ はイデアルの公理を満たす. ■

これらの例の $a\boldsymbol{Z}$ や $f(z)\boldsymbol{Z}[z]$ の様に, 環 R のただ 1 つの元 a の倍数の全体 aR であるイデアルを単項イデアルまたは主イデアル principal ideal と呼ぶ. 実は例 8.2.(b),(c) は整数の環 $\boldsymbol{Z}$ や「体 F」係数の多項式の環 $F[z]$ のイデアルの一般の重要な事情を表している:

定理 8.3. (a) 整数の部分集合 S が加法に関して群なら, それは正の最小元 a の倍数の全体 $a\boldsymbol{Z}$ である. 特に整数環 $\boldsymbol{Z}$ のイデアルはすべて単項イデアルである.

(b) 体 F 係数の 1 変数 z の多項式全体の環 $F[z]$ のイデアルもすべて単項イデアルである.

(証明) (a) 整数の加法に関する部分群 S の正の最小数を a と置く. S の任意の数 x を a で整数の範囲で割って $x = aq + r$, 商 q と余り $0 \leqq r < a$ は整数とする. x も $qa = a + a + \cdots + a$ も共に加法の群 S の数であり, $x - qa = r$ も S に属す. S の正の最小数は a なのだから $r = 0$ でなければならず, S のすべての数は a で割り切れる; $S \subset a\boldsymbol{Z}$. 逆に a の任意の倍数 $ka = a + a + \cdots + a$, $k \in \boldsymbol{Z}$ が加法の群 S の元であるから $a\boldsymbol{Z} \subset S$. 故に $S = a\boldsymbol{Z}$ が成り立ち, S は a の整数倍 (a の倍数) の全体だと判明した. 特に整数環 $\boldsymbol{Z}$ の任意のイデアル J は $\boldsymbol{Z}$ の部分集合で加法について群なのだから, その正の最小の数を a とすれば $J = (a) = a\boldsymbol{Z}$ であり, J は必ず単項イデアルである.

(b) 体 F の係数を持つ任意の多項式 $f(z)$ の最高次の項を $a_k z^k$ として $f(z)$ の次数を k で定義する事は普通の通りだが定数 0 だけは次数を普通 $-\infty$ と便宜上定義する.[81] F は体だからその元 $a_k \neq 0$ は必ず逆元を持つ. 故に一般に $F[z]$ の任意の 2 つの多項式, 次数 $\geqq 0$, の間では次数の高くない方で他方を F 係数で割る事ができる. 今 $F[z]$ の部分集合であるイデアル J の中から定数 0 以外 のもの, 次数 $\geqq 0$ のもの, で最小の次数を持つものの 1 つ $f(z) \in J$ を取る. J の 0 以外の任意の多項式 $g(z)$ の次数は $f(z)$ 以上だから, $f(z)$ で割り算して $g(z) = f(z)q(z) + r(z)$, 余り $r(z)$ は 0 か, さもなければその次数は $f(z)$ より低い, と分解する.[82] $-q(z)f(z) \in J$ だから $r(z) = g(z) - q(z)f(z)$ も加法の群 J の多項式だが, $f(z)$ が J の 0 以外の元の中の最小次数なのだから $r(z) = 0$ でなければならない. 故に J の 0 ではないすべての多項式は $f(z)$ の倍数に限り $J \subset f(z)F[z]$. しかし J は $F[z]$ のイデアルだから

[81] 簡単に考えれば, 定数関数 $f(z) = 0$ では係数に 0 でないものがないから 0 次とはしない方が便利で, 多項式の積の次数を考えるために $-\infty \times 0 = -\infty$ の規約で次数 $-\infty$ を採用すると具合がよい.

[82] 第 1 章 Corollary 1.10. の様な除法の等式の成立は, 本来は証明が必要だが, 有理数係数での多項式同士の割り算の経験からは自明としてよかろう.

$f(z) \in J$ に対して $f(z)F[z] \subset J$ でもある. 故に $J = f(z)F[z]$. ■

現在の問題に関係の深い重要なイデアルが次である.

Lemma 8.4. (a) 2 つの 0 ではない整数 m, n を固定し, a, b はすべての整数を動くとして整数の集合

$$S = \{am + bn |\ a, b \in \boldsymbol{Z}\}$$

を考える. m, n の最大公約数を $d = (m, n)$ と記すと, 次の集合等式が成り立つ:

$$S = \{kd |\ k = 0, \pm 1, \pm 2, \cdots\}. \tag{8.1}$$

即ち, 集合 S は m, n の最大公約数 d の整数倍の全体から成る.
(b) 特に, 任意の整数 m, n とその最大公約数 d に対して,

$$d = am + bn$$

の成り立つ整数 a, b が必ず存在する.
(c) 任意の正の整数 m に対して整数 x が m と素である事が, $xy = 1 \pmod m$ となる法 m での x の逆数 y が存在する必要十分条件である.
(証明) (a) この命題は既に定理 4.4. として p.55 で証明されているが, 次の別証明は十分それだけの価値がある. 集合 $S \subset \boldsymbol{Z}$ は上に定義された通りとして, S の任意の 2 元 $x = am+bn,\ y = a'm + b'n$ を取る. $x - y = (a - a')m + (b - b')n \in S$ であり,[83] 任意の $c \in \boldsymbol{Z}$ に対して $cx = (ca)m + (cb)n \in S$ も明らかで S は $\boldsymbol{Z}$ のイデアルである. 故にそれは単項イデアル, S の正の最小数 $h = a_0m + b_0n$ の倍数の全体 (h) である. 特に $m = 1m + 0n$ や $n = 0m + 1n$ は h の倍数であり, h は m, n の公約数であって, m, n の最大公約数 d に対して $h \leqq d$ が成り立つ. 一方 $h = a_0m + b_0n$ の構成によって h が d で割り切れることは明らかで, $h \geqq d$ でもあり, $h = d$ と (8.1) 式とが得られる.
(b) 上の (a) の証明の通り, $d = h = am + bn$ となる整数 $a = a_0,\ b = b_0$ が存在する.
(c) 事柄は Lemma 7.3.(b) と同じで, 以下はその別証明である. x が m と素, $d = (x, m) = 1$ なら (b) によって $ax + bm = d = 1$ となる整数 a, b が存在する. 即ち $ax = 1 - bm \equiv 1 \pmod m$ が成り立ち, $a = x^{-1} \pmod m$ である. 逆に法 m で x が可逆で逆数 x^{-1} を持てば, $x^{-1}x = 1 + bm$ となる整数 b がある. 故に $x^{-1}x - bm = 1$ であり, 最大公約数 $(x, m) = 1$ でなければならず, x は m と素である. ■

整数 m, n の最大公約数 $d = (m, n)$ はユークリッドの互除法で必ず有限回の手数で求められる事を我々は学んだ.[84] $d = am + bn$ となる整数 a, b を求めるには同じ方法で d を求め, その手順を逆に辿ればよい. 特に法 m での整数の環 $\boldsymbol{Z}/m$ の可逆元 $x \in \boldsymbol{Z}_m^*$ の逆数も, 上の (c) の証明が示す様に, この (m, x) を求める手順で得る事ができる. 計算上でユークリッドの互除法は手続きが特に小さく, 有力な数値的算出方法である. 例で見よう.

問題 8.5. 最大公約数 $d = (112973, 7927) = 1$ である事を示し, 法 112973 での 7927 の逆数, 法 7927 での 112973 の逆数をそれぞれ求めなさい.
(解) ユークリッドの互除法を行う. まず小さい 7927 で大きい 112973 を割って

[83] これまでだけで S は加法に関する群である整数全体 $\boldsymbol{Z}$ の部分群である事がわかり, 定理 4.4. の通り命題は示されている. 以下は S が $\boldsymbol{Z}$ のイデアルである事を言うためのものである.
[84] 下の問題 8.5. 参照.

$$112973 = 14 \times 7927 + 1995, \quad 112973 - 14 \times 7927 = 1995,$$

を得る. 112973 と 7927 の公約数の全体を S_1 と置く. 第 2 式によれば S_1 の任意の数は 1995 も割り切る. 故に S_1 は 7927 と 1995 の公約数の全体 S_2 に含まれてしまう. 逆に第 1 式から S_2 の任意の数, 7927 と 1995 の公約数, は 112973 も割り切り, S_2 の全体は S_1 に含まれてしまう. これは集合の等式 $S_1 = S_2$ を意味し, 特にそれらの最大のもの, 最大公約数は同じで, $(112973, 7927) = (7927, 1995)$ が成り立つ. 従って数のより小さい組の最大公約数 $(7927, 1995)$ を求めればよい. この様に得られた余りでの割り算を続けて

$$112973 = 14 \times 7927 + 1995, \qquad 7927 = 3 \times 1995 + 1942,$$
$$1995 = 1 \times 1942 + 53, \qquad 1942 = 36 \times 53 + 34,$$
$$53 = 1 \times 34 + 19, \qquad 34 = 1 \times 19 + 15,$$
$$19 = 1 \times 15 + 4, \qquad 15 = 3 \times 4 + 3, \qquad 4 = 1 \times 3 + 1.$$

最後の余り 1 でもう 1 度割り算をすれば余りは 0 になる. 最大公約数 d は余り 0 の直前の余りで, この場合 $1 = (112973, 7927)$ であり, 112973 と 7927 とは互いに素である; 実は $112973 = 16139 \times 7$, 16139 と 7927 は素数である. これらの割り算の等式を逆に辿って順次記せば

$$\begin{aligned} d = 1 &= 4 - 1 \times 3 = 4 - (15 - 3 \times 4) = (1 + 3) \times 4 - 15 \\ &= -15 + 4 \times (19 - 1 \times 15) = (-1 - 4) \times 15 + 4 \times 19 \\ &= 4 \times 19 - 5 \times (34 - 19) = \cdots \\ &= 2094 \times 112973 - 29843 \times 7927. \end{aligned}$$

故に $2094 = 112973^{-1} \pmod{7927}$, $-29843 \equiv 83130 = 7927^{-1} \pmod{112973}$ と逆数が得られる. **(問題 8.5. 終り)**

体 F 上の 1 変数 z の多項式の環 $F[z]$ にも Lemma 8.4. と同様の重要な構造がある. 体係数の任意の 2 つの多項式の間では割る多項式より低次の余りが出るまで続ける除法が常に可能である事に注意する.

Lemma 8.6. 任意の体 F と, F を係数とする文字 z の任意多項式 $m(z), n(z) \in F[z]$ を取り, $F[z]$ の次の部分集合 S を定義する:

$$S = \{a(z)m(z) + b(z)n(z) |\ a(z), b(z) \in F[z]\}.$$

(a) $m(z), n(z)$ の最大公約数, 即ち $m(z), n(z)$ を共に F 係数で割り切る最大次数の $F[z]$ 多項式,[85] を $d(z) := (m(z), n(z))$ と記すと, 次の集合等式が成り立つ:

$$S = \{k(z)d(z) |\ k(z) \in F[z]\}. \tag{8.2}$$

即ち, 集合 S は $m(z), n(z)$ の最大公約数 $d(z)$ の倍数全体から成る環 $F[z]$ のイデアルである.
(b) 任意の $m(z), n(z) \in F[z]$ とその最大公約数 $d(z)$ に対して,

$$d(z) = a(z)m(z) + b(z)n(z)$$

[85] $f(z)$ が $m(z)$ を F 係数で割り切る, $f(z)|m(z)$, なら 0 ではない任意定数 $c \in F$ について $cf(z)|m(z)$ も成り立つ; 商を c^{-1} 倍に取ればよい. だから公約数或いは最大公約数の多項式としては係数 F の 0 でない定数倍の違いは無視或いは同一視する.

の成り立つ多項式 $a(z), b(z) \in F[z]$ が必ず存在する.
(c) 特に任意の多項式 $m(z) \in F[z]$ に対し, $f(z) \in F[z]$ が $m(z)$ と素, 最大公約数 $(m(z), f(z)) = 1$, である事と $f(z)g(z) = 1 + a(z)m(z)$ となる「法 $m(z)$ での $f(z)$ の逆数 $g(z)$」の存在とが同値である.
(証明) (a) 集合 $S \subset F[z]$ は上に定義された通りとして, S の任意の 2 元 $x = a(z)m(z) + b(z)n(z),\ y = a'(z)m(z) + b'(z)n(z)$ を取る. $x - y = (a - a')m + (b - b')n \in S$ であり, $0 = 0m(z) + 0n(z) \in S$ も明らかで, 環 $F[z]$ の中で S は加法に関する部分群である. また任意の $c(z) \in F[z]$ について

$$c(z)\{a(z)m(z) + b(z)n(z)\} = \{c(z)a(z)\}m(z) + \{c(z)b(z)\}n(z) \in S$$

から $c(z)S \subset S$ も明らかで S は環 $F[z]$ のイデアルである. 定理 8.3.(b) によって S は単項イデアルで, $S = h(z)F[z]$ となる $h(z) \in F[z]$ がある. 即ち任意の $a(z)m(z)+b(z)n(z) \in S$ をある $f(z) \in F[z]$ によって $f(z)h(z)$ と表す事ができ, 逆に任意の $g(z) \in F[z]$ に対して $g(z)h(z)$ は必ず S に入る. 特に $g(z) = 1$ として $h(z) \in S$ は S の中の 最小次数 $\geqq 0$ の元で S はこの倍数の全体である. 故に $m(z) = 1m(z)+0n(z)$ や $n(z) = 0m(z)+1n(z)$ は $h(z)$ の倍数, $h(z)$ は $m(z), n(z)$ の公約数であり, $m(z), n(z)$ の最大公約数 $d(z)$ に対して $h(z)|d(z)$ が成り立つ. 一方 S の元 $h(z)$ を $h(z) = a_0(z)m(z) + b_0(z)n(z)$ と表す $a_0(z), b_0(z) \in F[z]$ は存在するから $d(z)|h(z)$ は明らかで, $h(z)$ は $d(z)$ の F 定数倍, S は $d(z)$ の倍数の全体である.
(b) 上の (a) の証明で見た通り, $d(z) = h(z) = a(z)m(z) + b(z)n(z)$ となる多項式 $a(z) = a_0(z),\ b(z) = b_0(z)$ が存在する.
(c) $f(z)$ が $m(z)$ と素, $d(z) = (f(z), m(z)) = 1$ なら (b) によって $a(z)f(z) + b(z)m(z) = d(z) = 1$ となる多項式 $a(z), b(z) \in F[z]$ が存在し, 逆に $a(z)f(z) + b(z)m(z) = d(z) = 1$ となる多項式 $a(z), b(z) \in F[z]$ が存在すれば $f(z)$ と $m(z)$ のすべての公約数, 従って最大公約数は 1 の約数 1 であり $f(z)$ と $m(z)$ とは互いに素である. $a(z)f(z) + b(z)m(z) = d(z) = 1$ は $a(z)f(z) = 1 - b(z)m(z) \equiv 1 \pmod{m(z)}$, 即ち法 $m(z)$ での $f(z)$ の逆数としての $a(z)$ の存在, と同値だから命題通りである. ■

体 F 係数の 2 つの多項式 $m(z), n(z)$ が与えられた時, その最大公約数 $d(z)$ は整数の場合と同様にユークリッドの互除法で求められる事は明らかである. 特に上の Lemma 8.6.(c) の「法 $m(z)$ での $f(z)$ の逆数」がある場合にそれを求めるアルゴリズムとしてユークリッド互除法の逆算が大切な手段となる.

遠い道のりだったが, 漸く体 F の元を係数とする多項式の因数分解の一意性を透視する手段, Lemmas 8.4. と 8.6. との応用である次の系, に我々は達した:

Corollary 8.7. (a) 整数 a, b, c について最大公約数 $(a, b) = (a, c) = 1$ なら, $(a, bc) = 1$ も成り立つ.
(b) 任意の体 F 係数の多項式 $a(z), b(z), c(z)$ について最大公約数 $(a(z), b(z)) = 1$, $(a(z), c(z)) = 1$ なら $(a(z), b(z)c(z)) = 1$ である.
(証明) (a) 仮定 $(a, b) = (a, c) = 1$ から整数 m, n, m', n' があって

$$ma + nb = 1, \quad m'a + n'c = 1$$

が成り立つ. 第 2 式を第 1 式へ入れて $1 = ma + nb(m'a + n'c) = \{m + (nm'b)\}a + nn'bc$, 故に $(a, bc) = 1$ でなければならない.

(b) 仮定 $(a(z),b(z))=(a(z),c(z))=1$ から F 係数多項式 $m(z),n(z),m'(z),n'(z)$ があって

$$m(z)a(z)+n(z)b(z)=1,\quad m'(z)a(z)+n'(z)c(z)=1$$

が成り立つ. 第 2 式を第 1 式へ入れて

$$\begin{aligned}1&=m(z)a(z)+n(z)b(z)\{m'(z)a(z)+n'(z)c(z)\}\\&=(m+nm'b)a(z)+(nn')\{b(z)c(z)\}.\end{aligned}$$

故に $(a(z),b(z)c(z))=1$ でなければならない. ■

上の Corollary 8.7. の重要さは強調し過ぎる事はない. 以前考えられた例,

$$z^2-1\equiv(z-1)(z-7)\equiv(z-3)(z-5)\pmod 8$$

を想起しよう: 係数を環 $R=\boldsymbol{Z}/8$ に取って $R[z]$ は環である, $R[z]$ で $z-3$ は $z-1$ も $z-7$ も割り切る事はできない, それにも関わらず $z-3$ は積 $(z-1)(z-7)\equiv z^2-1$ を割り切る, 一般の環の世界は誠に複雑である. 対比してそのような事は, モニックな 1 次式での割り算の制限等もなく一般に, 係数が体の場合には起きないと Corollary 8.7. は保証するのである.

懸案の 1 つがこれで解決する:

定理 8.8. (a) 整数の素因数分解は一意である.
(b) 任意の体 F 係数の 1 次以上の多項式 $f(z)\in F[z]$ の既約因数への分解は, 体 F の 0 でない定数倍の任意性を除いて一意である.
(証明) どちらも全く同様に証明されるから, (b) の場合で変数 z の表記を省いて簡単に書く; 以下は「F 係数多項式 $f(z)$」を「整数 f」と, 「F 既約因数」を「素因数」とそれぞれ読み換えれば, (我々が常識として疑った事もない) 整数 $\boldsymbol{Z}$ の素因数分解の一意性の証明にもそのままなる. F 係数で $f(z)=f$ に 2 通りの既約因数分解があると仮定する:

$$f=aa'a''\cdots=bb'b''\cdots.$$

第 1 の表現の第 1 既約因数 a について $(a,f)=(a,aa'a''\cdots)=a$ である. 仮に a と $b,b',b''\cdots$ の全てとが素だとすれば, Corollary 8.7.(a),(b) によって $1=(a,b)=(a,bb')=(a,bb'b''\cdots)=(a,f)$ となって矛盾である. 故に F 既約な a は同様に F 既約な $b,b',b'',\cdots$ のどれか, それを b だとする, を割り切り, F の定数倍を除いて等しい. 故に F の 0 ではない定数を適当に掛けて $b=a$ としてよい. 残る a' も $b',b'',\cdots$ のどれかと等しくなければならない事は同様に示される. この手続きは f のすべての F 既約 a 因数について続けられ, 証明が完成する. ■

乱数問題が (有限) 体係数多項式の既約因数分解問題の理解だけを求めたことは幸いだった. しかし我々が殆ど気にも留めず暗黙に仮定している一般の整数 $\boldsymbol{Z}$ 係数多項式の既約因数分解の一意性の証明はもうほとんど終っている. 最後の 1 段の準備に立ち向かって, 数学の一般構造への入門の旅の終りしよう.

Lemma 8.9.(Gauss) 文字 z の整数係数多項式 $f(z)$ の係数の最大公約数が 1 の場合, $f(z)$ は原始多項式であると言う.[86] 原始多項式 $f(z),g(z)$ の積は原始多項式である.
(証明) 原始多項式 $f(z),g(z)$ に対して素数 p を任意に取り, 積 $f(z)g(z)$ の係数のすべてが p で割り切れる事はない, と示す. 法 p で考えれば, $f(z),g(z)$ は原始多項式でそれぞれの係数

[86] 有限体 $\mathrm{GF}(p^n)$ の乗法群の生成元を根に持つ $\boldsymbol{Z}_p$ 係数既約多項式である原始多項式と同じ名前が用いられるが, 登場する場が異なるので混乱はないだろう.

のすべてが p で割り切れる事はないから,

$$f(z) \equiv a_j z^j + \text{より低次の項}, \quad g(z) \equiv b_k z^k + \text{より低次の項} \pmod{p}$$

となる法 p での係数 $a_j, b_k \not\equiv 0$ と次数 $j, k \geqq 0$ とがあって

$$f(z)g(z) \equiv a_j b_k z^{j+k} + \text{低次項} \not\equiv 0 \pmod{p}$$

である. 故に積 $f(z)g(z)$ は必ず p では割り切れない係数を持つ. ■

定理 8.10. 整数係数多項式の既約因数分解は定数倍を除いて一意である. 特に既約原始多項式への因数分解は一意である.

(証明) 有理数 (分数) の全体を $\boldsymbol{Q}$ と記す. 整数係数多項式 $f(z)$ は必ずその整数係数の最大公約数 G で割って原始多項式にする事ができるから, はじめから $f(z)$ は原始多項式だと仮定する. 原始多項式 $f(z)$ は $\boldsymbol{Q}$ 係数多項式と見る事ができる. $\boldsymbol{Q}$ は体だから定理 8.8.(b) によって $\boldsymbol{Q}$ での $f(z)$ の既約因数分解は $\boldsymbol{Q}$ 定数倍を除いて一意である. その分解を

$$f(z) = \prod_{k=1}^{m} f_k(z)$$

と置く. ここで $f_k(z)$ は $\boldsymbol{Q}$ 係数の既約多項式である. $f_k(z)$ の係数である有理数のすべての分母の最小公倍数を L_k とすれば $L_k f_k(z)$ は整数係数多項式であり, この整数係数全体の最大公約数を G_k として

$$L_k f_k(z) = G_k g_k(z), \quad g_k(z) \text{ は原始多項式},$$

となる. 勿論 $f_k(z)$ は $\boldsymbol{Q}$ 係数で定数倍を除いて一意だから, その原始多項式成分 $g_k(z)$ も $\boldsymbol{Q}$ 係数で既約でありかつ原始多項式として一意である. こうして $f(z)$ の $\boldsymbol{Q}$ 既約な原始多項式の積への一意な因数分解

$$Lf(z) = Gg(z), \quad g(z) = \prod_{k=1}^{m} g_k(z), \quad L = \prod_{k=1}^{m} L_k, \quad G = \prod_{k=1}^{m} G_k,$$

が得られた. Lemma 8.9. によって $g(z)$ は原始多項式である. そうすると等式 $Lf(z) = Gg(z)$ の左辺の係数の最大公約数は L, 右辺の係数の最大公約数は G であって, これらは等しくなければならない. 即ち全体を $L = G$ で割る事ができて, $\boldsymbol{Q}$ 既約, 従って $\boldsymbol{Z}$ 既約な一意な因数分解

$$f(z) = g(z) = \prod_{k=1}^{m} g_k(z)$$

が成り立つ事が示された. ■

8.2. 行列表現での M 系列乱数と MT19937[87]

1 つの優れた新展望を乱数の旅の最後に議論できる事は幸いである. 最近 MT19937 と呼ばれる 19937 次の $\boldsymbol{Z}_2$ 上の M 系列乱数が Matsumoto-Nishimura[44] によって提案された. 19937 は Mersenne 指数であり, Matsumoto-Nishimura はこのような高次の 100 項以上を持つ $\boldsymbol{Z}_2$ 原始多項式 $f(z)$ を発見し, 4 バイト $= 32$ ビット 実数として $19937/32 \approx 623$ 次の目

[87] MT19937 は Matsumoto-Nishimura[44] による乱数発生ルーチンで MT は Mersenne Twister の略という.

覚しい均等分布を実現し, 実装では 3 項漸化式の様に高速計算させる工夫を与えたのである. 方法の基本構造は複雑だが Marsaglia-Tsay[14] が主として加算生成法の解析のために導入した行列に基づく定式化を経由すると最も容易に見通されると思われる. 今まで触れる事のなかったこの強力な行列表現の考察の良い機会でもあるので, 共に棹尾を飾るものとしよう.

一般に $\boldsymbol{Z}_p$ 上の n 次元列ベクトルの列 $\{\boldsymbol{X}_k|\, k=0,1,2,\cdots\}$ を考え, 次の様に成分を記す:[88]

$$ {}^t\boldsymbol{X}_{\boldsymbol{k}} = (x_k^{(1)}, x_k^{(2)}, \cdots, x_k^{(n)}). $$

以下 k は専ら系列のベクトルの番号に用いる. このベクトル列の乗算合同法的な漸化式

$$ \boldsymbol{X}_{k+1} = B\boldsymbol{X}_k, \quad B \text{ は} \boldsymbol{Z}_p \text{上の } n\times n \text{ 行列}, \tag{8.3} $$

を考えよう. まず次の一般的な事柄に注意する:

Corollary 8.11. 任意の素数 p に対する $\boldsymbol{Z}_p$ 上の任意のモニックな n 次多項式 $f(z)$ に対して, $\boldsymbol{Z}_p$ 成分を持つ $n\times n$ 行列 B でその固有多項式 $|zE-B| = f(z)$ となるものがある.

(証明) 具体的に $f(z)\in\boldsymbol{Z}_p$ を

$$ f(z) = z^n + b_1 z^{n-1} + b_2 z^{n-2} + \cdots + b_n \tag{8.4} $$

と置く. Lemma 6.5. の別証と同様に次の行列 ($f(z)$ の companion matrix) を導入する:

$$ T = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -b_n & -b_{n-1} & -b_{n-2} & \cdots & -b_2 & -b_1 \end{pmatrix}. $$

この行列の固有多項式 $|zE-T|$ を作る; E は $n\times n$ 単位行列である:

$$ |zE-T| = \begin{vmatrix} z & -1 & 0 & \cdots & 0 & 0 \\ 0 & z & -1 & \cdots & 0 & 0 \\ 0 & 0 & z & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & z & -1 \\ b_n & b_{n-1} & b_{n-2} & \cdots & b_2 & b_1+z \end{vmatrix}. $$

この $|zE-T|$ の第 2 列に z を, 第 3 列に z^2 を, $\cdots$, 第 n 列に z^{n-1} を, それぞれ掛けてすべて第 1 列に加えると,

$$ |zE-T| = \begin{vmatrix} z-z & -1 & 0 & \cdots & 0 & 0 \\ z^2-z^2 & z & -1 & \cdots & 0 & 0 \\ z^3-z^3 & 0 & z & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ z^{n-1}-z^{n-1} & 0 & 0 & \cdots & z & -1 \\ f(z) & b_{n-1} & b_{n-2} & \cdots & b_2 & b_1+z \end{vmatrix}. $$

この行列式の第 1 列についての展開から $|zE-T| = (-1)^{n+1} f(z)\times(-1)^{n-1} = f(z)$ が得ら

[88] 我々の規約, 太文字で列 (縦) ベクトルを表す, ${}^t\boldsymbol{X}_k$ は転置の行ベクトル, を思い出そう.

れる. T は存在を示すべき行列 B の 1 つである. もっと一般には $\boldsymbol{Z}_p$ 上の任意の $n\times n$ 正則行列 $U^{(\prime)}, V^{(\prime)}$ による変換 $B=UTV,\ B'=U'BV'$ も, そして転置行列 ${}^tB$ も同じ固有多項式を共有するものとして存在する. ■

以後任意の行列 B の固有多項式を $|zE-B|=f_B(z)$ と記し, さらに $f_B(z)$ が $\boldsymbol{Z}_p$ 上の n 次原始多項式 (8.4) となる様に $n\times n$ 行列 B を取ろう; Corollary 8.11. によってこれは可能である. 有名な Hamilton-Cayley の定理は次を知らせる:

定理 8.12. $\boldsymbol{Z}_p$ の意味で $f_B(B)=0$ である. 即ち $\boldsymbol{Z}_p$ 係数多項式 $f_B(z)$ の z に行列 B を入れた $n\times n$ 行列は $\boldsymbol{Z}_p$ で見て成分がすべて 0 の零行列である.

(証明) 多種類の証明[59),60),34),61)] が任意の体上の行列と固有多項式について成立するが, 特に我々には見やすいと思われるもの[59)] を $\boldsymbol{Z}_p$ を目的に記して紹介する. 行列式 $|zE-B|$ の第 i,j 余因子[89]を Δ_{ij} と記せば, Δ_{ij} は z の $n-1$ 次以下の多項式である. これを

$$\Delta_{ij}(z)=c_{ij}^{(1)}z^{n-1}+c_{ij}^{(2)}z^{n-2}+\cdots+c_{ij}^{(n-1)}z^1+c_{ij}^{(n)}$$

と記そう. 行列 $zE-B$ の「adjunct」$D(z)$ を $\Big(D(z)\Big)_{ij}=\Delta_{ji}(z)$ で定義し, それを文字 z で展開した係数である定数行列 C_l を $(C_l)_{ij}=(c_{ji}^{(l)}),\ 1\leqq l\leqq n$ で導入する:

$$D(z)=C_1z^{n-1}+C_2z^{n-2}+\cdots+C_{n-1}z+C_n. \tag{8.5}$$

通常の実数, 複素数上の線形代数, 行列式論で逆行列への関係としてよく知られる等式

$$(zE-B)D(z)=|zE-B|E$$

は和, 差と積だけで示されるから任意の環, 特に任意の体, 当然 $\boldsymbol{Z}_p$ での計算として成り立つ.[90] これと (8.5) は次の z の恒等式を与える:

$$\begin{aligned}f_B(z)E=|zE-B|E&=(zE-B)(C_1z^{n-1}+C_2z^{n-2}+\cdots+C_{n-1}z+C_n)\\&=z^nC_1+z^{n-1}(C_2-BC_1)+z^{n-2}(C_3-BC_2)+\cdots+z(C_n-BC_{n-1})-BC_n.\end{aligned}$$

体 K 上の行列 B に対し $f_B(z)$ の展開形が $z^n+b_1z^{n-1}+\cdots+b_{n-1}z+b_n$ なら左辺は:

$$\begin{aligned}f_B(z)E&=z^nE+b_1z^{n-1}E+\cdots+b_{n-1}zE+b_nE\\&=z^nC_1+z^{n-1}(C_2-BC_1)+z^{n-2}(C_3-BC_2)+\end{aligned}$$

[89]任意の $n\times n$ 行列 $A=(a_{ij})$ の行列式は加減法と乗法だけで, 従って任意の環 R の成分を持つ行列上で定義される. 第 i 行と第 j 列を除いた $(n-1)\times(n-1)$ 行列の行列式に $(-1)^{i+j}$ を掛けたものを行列式 $|A|$ の第 i,j 余因子 cofactor と言う. これを Δ_{ij} と記すと, 行列式 $|A|$ の第 i 行或いは第 j 列についての展開

$$|A|=\sum_{k=1}^{n}a_{ik}\Delta_{ik}=\sum_{l=1}^{n}a_{lj}\Delta_{lj}$$

が成り立つ. 環 R は勿論体, 特に $\boldsymbol{Z}_p$ でもよい.

[90]3 行 3 列の行列式までの知識でも, 前脚注で述べた行列式の行或いは列についての展開での余因子の役割からこれは容易に見られる. 実際 $A:=zE-B=(a_{ij})$ と置くと,

$$\sum_{k=1}^{n}a_{ik}\Delta_{jk}=\Big((zE-B)C\Big)_{ij}$$

は行列式 $|A|=|zE-B|$ の第 j 行を $(a_{i1}\,a_{i2}\,\cdots\,a_{in})$ で, つまり行列式の第 i 行で置き換えた行列式の第 j 行に関する展開計算である. $i=j$ ならこれは行列式 $|A|=|zE-B|$ そのものの展開だから i に関係なくすべて同じ数 $|zE-B|$ になり, $i\neq j$ なら「i と j 行が同一である行列式」の展開として常に 0, 故に $(zE-B)C=|zE-B|E$ が成り立つ.

$$\cdots + z(C_n - BC_{n-1}) - BC_n. \qquad (8.6)$$

行列成分毎に見て (8.6) は $K[z]$ の多項式の恒等式であり, z のすべての次数の係数は左右両辺で等しくなければならない.[91] 故に (8.6) の左右の z の各次数の係数行列は成分毎に, 従って行列として等しく, 次が成り立つ:

$$\begin{aligned}
&E = C_1,\\
&b_1E = C_2 - BC_1,\\
&b_2E = C_3 - BC_2,\\
&\cdots\cdots\cdots\cdots\\
&b_{n-2}E = C_{n-1} - BC_{n-2},\\
&b_{n-1}E = C_n - BC_{n-1},\\
&b_nE = -BC_n.
\end{aligned}$$

これらの上から順にそれぞれ行列 $B^n, B^{n-1}, \cdots, B^2, B^1, B^0 = E$ を左から (実はどちらからでもよいのだが) 掛けて足し合わせると, (8.6) の z に行列 B を入れた式が作られる:

$$\begin{aligned}
f_B(B) &= B^n + b_1B^{n-1} + b_2B^{n-2} + \cdots + b_{n-1}B + b_nE\\
&= B^nC_1 + (B^{n-1}C_2 - B^nC_1) + (B^{n-2}C_3 - B^{n-1}C_2) + \cdots\\
&\qquad +(B^2C_{n-1} - B^3C_{n-2}) + (BC_n - B^2C_{n-1}) - BC_n.
\end{aligned}$$

明らかにこの右辺はすべて打ち消しあって 0 行列である. ■

$f_B(z)$ が $\boldsymbol{Z}_p$ 上の n 次原始多項式 (8.4) となる様に (Corollary 8.11.) 行列 B を取ろう. この時 $f_B(z)$ は $\boldsymbol{Z}_p$ 内の根 0 を持つ事はできないから $|B| = f_B(0) \not\equiv 0 \pmod p$ で行列 B は正則である. これは漸化式 (8.3) が逆行可能である, $\boldsymbol{X}_{k-1} = B^{-1}\boldsymbol{X}_k$ となる事を意味する. また漸化式 (8.3) と定理 8.12. から

$$B^l\boldsymbol{X}_k = \boldsymbol{X}_{k+l}, \qquad f_B(B)\boldsymbol{X}_k = \boldsymbol{0}$$

も成り立つ. 上の第 2 式は (8.4) によってベクトル $\boldsymbol{X}_k$ の線形漸化式

$$\boldsymbol{X}_{k+n} + b_1\boldsymbol{X}_{k+n-1} + b_2\boldsymbol{X}_{k+n-2} + \cdots + b_n\boldsymbol{X}_k = \boldsymbol{0} \qquad (8.7)$$

であり, その特性多項式は n 次原始多項式 $f_B(z)$ だから, ベクトル $\boldsymbol{X}_k$ の第 i 行成分が作る系列 $\{x_k^{(i)} |\ k = 0, 1, 2, \cdots\}$ は 0 系列でなければ M 系列である.

---

[91] 多項式 $f(z) = a_0z^n + a_1z^{n-1} + \cdots + a_n \in K[z]$ の恒等式 $f(z) = 0$ を考える; $f(z) = g(z)$ なら $f(z) - g(z) = 0$ を取ればよい. 恒等式の z に K の異なる $n+1$ 個の値 $\{z_0, z_1, \cdots, z_n\}$ を代入すれば $\{a_0, a_1, \cdots, a_n\}$ に対する次の同次連立 1 次方程式を得る:

$$\begin{aligned}
&a_0{z_0}^n + a_1{z_0}^{n-1} + \cdots + a_n = 0,\\
&a_0{z_1}^n + a_1{z_1}^{n-1} + \cdots + a_n = 0,\\
&\qquad\cdots\cdots\cdots\cdots\\
&a_0{z_n}^n + a_1{z_n}^{n-1} + \cdots + a_n = 0.
\end{aligned}$$

この係数行列式は $n+1$ 次の Vandermonde 行列式 $D(z_0, z_1, \cdots, z_n)$ で K の互いに異なる $\{z_0, z_1, \cdots, z_n\}$ の差の積であり, 0 ではない. 故にこの連立 1 次方程式の解 $\{a_0, a_1, \cdots, a_n\}$ はただ 1 組, すべて 0 の trivial な解だけを持つ. K が有限体 $\boldsymbol{Z}_p$ で標数 p が小さくて $n+1$ 個の異なる $\{z_0, z_1, \cdots, z_n\}$ を取れなくても, $\boldsymbol{Z}_p$ の拡大体 $\mathrm{GF}(p^k)$ を適当な拡大次数 k で考えてそこで $\{z_0, z_1, \cdots, z_n\}$ を選べるから同じ結論が成立する.

上に導入された行列表現でもその遷移行列 B を (8.4) 式の下の行列 T のような形に選んだ場合には, ベクトルを成分で書き表せば容易に見える様に, 漸化式 $\boldsymbol{X}_{k+1} = T\boldsymbol{X}_k$ で定義される系列は単一の M 系列の第 k 成分から始まる n 連を n 次元列ベクトル $\boldsymbol{X}_k$ とみなす定式化に当たる. 遷移行列 B の選択は同一の固有多項式にも T 以外に上に見た通り多くあるからこの描像は一般には成り立たない. しかし $\boldsymbol{X}_k$ の成分 (行) 番号を固定すれば同一の M 系列漸化式に従うのだから, 正則遷移行列 B に基づく系列 $\boldsymbol{X}_k = B^k\boldsymbol{X}_0$ は以前第 6 章で見た連結 M 系列乱数を一般に表している. ベクトル系列が初期ベクトル $\boldsymbol{X}_0$ だけで定まる事は Fushimi-Tezuka の定理の条件を満たす様な出発ベクトルの組の選択に苦労した目からは異質に見えるが, 実はこれら出発ベクトルの様相は正則行列 B の姿に反映しており, 正則遷移行列による定式化のそれぞれは連結 M 系列乱数のうちで Fushimi-Tezuka の定理の条件を満たすものそれぞれと 1 対 1 に対応している. これは後に明確に見られる. Marsaglia-Tsay が行列による定式化で示した関係は次にまとめられる:

定理 8.13. $\boldsymbol{Z}_p$ 上の n 次元ベクトルの空間を $V_n := \boldsymbol{Z}_p{}^n$ と記し, それから零ベクトルを除いたものを $V_n{}^*$ とする. $\boldsymbol{Z}_p$ 成分の $n \times n$ 正則行列 B について次の (a)-(d) は同値である:

(a) 固有多項式 $f_B(z)$ が $\boldsymbol{Z}_p$ 上の n 次原始多項式である.

(b) 出発ベクトル $\boldsymbol{X}_k = \boldsymbol{X}_0$ を $V_n{}^*$ のどの元に取っても, ベクトル系列 $\{\boldsymbol{X}_k = B^k\boldsymbol{X}_0 |\ k = 0, 1, 2, \cdots, p^n - 1\}$ は周期 $p^n - 1$ で $V_n{}^*$ のすべてのベクトルを 1 度ずつ遍歴する.[92]

(c) 体 $\boldsymbol{Z}_p$ 上で正則 $n \times n$ 行列の全体は行列積に関して (一般に非可換な) 群, 一般線形群 $GL(n, \boldsymbol{Z}_p)$ を作る. その中で行列 B の生成する行列巡回 (部分) 群 $\{B^1, B^2, \cdots, B^k, \cdots\}$ はベクトル空間 V_n 上に可移 transitive に作用する. 即ち任意の 2 ベクトル $\boldsymbol{X}, \boldsymbol{Y} \in V_n{}^*$ に対して $B^i\boldsymbol{X} \equiv \boldsymbol{Y}$ となる整数 i が存在する.

(d) 行列巡回群 $\{B^1, B^2, \cdots, B^k, \cdots\}$ は (最大) 位数 $p^n - 1$ を持つ. 即ち

$$B^{p^n-1} = E \text{ であり, } 1 \leqq k < p^n - 1 \text{ では } B^k \not\equiv E \pmod{p} \text{ である.}$$

(証明) [(a) から (b)] (a) を仮定すると, 上に見た様に, 任意の出発ベクトル $\boldsymbol{X}_0$ に対してベクトル系列 $\{B^k\boldsymbol{X}_0 |\ k = 0, 1, 2, \cdots\}$ の各行成分は $\boldsymbol{Z}_p$ 上の n 次 M 系列の線形漸化式に従う. 出発ベクトル $\boldsymbol{X}_0$ を $V_n{}^*$ から選べば, まず第 1 に $\boldsymbol{X}_k = B^k\boldsymbol{X}_0$ はすべての番号 k でも零ベクトルになれない.[93] そして $\boldsymbol{X}_0$ については, それが必ず持つ 0 ではない行成分, それを第 i 列成分 $x_0^{(i)}$ としよう, から出発する系列 $\{x_k^{(i)} |\ k = 0, 1, 2, \cdots\}$ は 0 系列ではない n 次 $\boldsymbol{Z}_p$M 系列で周期は $p^n - 1$ である. ベクトル系列の (一般) 周期は各成分の系列の (一般) 周期の公倍数以外はあり得ない. だから $V_n{}^*$ の任意の出発ベクトル $\boldsymbol{X}_0$ に対するベクトル系列 $\{\boldsymbol{X}_k |\ k = 0, 1, 2, \cdots\}$ の一般周期, 特にその正の最小値である周期 T は必ず不等式 $T \geq p^n - 1$ を満たす. しかもベクトルの 1 段漸化式 $\boldsymbol{X}_{k+1} = B\boldsymbol{X}_k$ は同一のベクトルが実現すればそれからは繰り返し, と制限するから, どんな初期ベクトル $\boldsymbol{X}_0 \in V^*$ から出発してもベクトル系列 $\{\boldsymbol{X}_k |\ k = 0, 1, 2, \cdots\}$ は $p^n - 1$ 個以上の異なった $V_n{}^*$ のベクトルを経由しなければならない. しかし $V_n{}^*$ のベクトルの総数が $p^n - 1$ なのだから, ベクトル系列の周期は $p^n - 1$ 以外はあり得ないし, 脚注に記した様に $\boldsymbol{X}_k$ のどの成分系列も 0 系列ではない M 系列でなけ

[92] 従って $\boldsymbol{X}_k$ のすべての成分系列はすべて (同一漸化式に従う)0 系列ではない M 系列である. またこのベクトル系列の出現順は遷移行列 B で定まって本質的に一意で, 初期ベクトル $\boldsymbol{X}_0$ の選択はその出発位置を変えるだけである.

[93] もし $\boldsymbol{X}_k = \boldsymbol{0}$ なら, 行列 B は可逆だから, $\boldsymbol{X}_0 = B^{-k}\boldsymbol{0} = \boldsymbol{0}$ で仮定 $\boldsymbol{X}_0 \in V_n{}^*$ に矛盾する.

ればならない. またこのベクトル M 系列での各ベクトルの出現順が一意である事は漸化式 $\boldsymbol{X}_{k+1} = B\boldsymbol{X}_k$ から明らかである.

[(b) から (c)] (b) によって $\boldsymbol{X}_0 \in {V_n}^*$ を 1 つ固定すると, 任意の $\boldsymbol{X}, \boldsymbol{Y} \in {V_n}^*$ に $\boldsymbol{X} = B^k\boldsymbol{X}_0,\ \boldsymbol{Y} = B^l\boldsymbol{X}_0$ となる整数 k, l が定まる. 故に $\boldsymbol{Y} = B^{l-k}B^k\boldsymbol{X}_0 = B^{l-k}\boldsymbol{X}$ であり, 題意の整数 $i = l - k$ が必ず存在する.

[(c) から (d)] 行列 B の位数 $h < p^n - 1$ と仮定して (c) と矛盾する事を導き, (d) でなければ (c) が成り立たない, 即ち対偶として (c) ならば (d) が成り立つ事を導く (背理法). $h < p^n - 1$ なら (行列 B が生成する巡回部分群が $\boldsymbol{X}_0$ に作用して作る) ベクトルの集合 (軌道)$S := \{\boldsymbol{X}_k = B^k\boldsymbol{X}_0 |\ k = 1, \cdots, h\}$ は ${V_n}^*$ の真の部分集合になり, 任意の $\boldsymbol{Y} \in {V_n}^* - S$ を任意に取れば $\boldsymbol{Y} = B^k\boldsymbol{X}_0$ となる番号 k は存在せず (c) が成り立たない. 故に (c) ならば (d) が成り立つ.

[(d) から (a)] Marsaglia-Tsay の議論を紹介する. 行列 B の位数が $p^n - 1$ で (d) が成り立つとして巡回群で一般に見た様に $B^1, \cdots, B^{p^n-1} = E$ は $\boldsymbol{Z}_p$ ですべて異なる事を記憶する. 行列 B の $\boldsymbol{Z}_p$ 係数の多項式の全体を $\mathcal{P}$ と置く; $\mathcal{P}$ には行列としては B の冪とそれらの和しか含まれないからすべて可換で, $\mathcal{P}$ は $\boldsymbol{Z}_p$ 係数の文字 z の多項式の全体の環 $\boldsymbol{Z}_p[z]$ と同じ (同型) である. $\boldsymbol{Z}_p[z]$ で行った様に最小多項式 $\phi(B),\ \phi(B) \equiv 0$ (零行列) となる最小次数 m のもの, を考える. $\phi(B)$ は勿論 $\boldsymbol{Z}_p$ 既約である. $\boldsymbol{Z}_p$ 係数の任意多項式 $g(z)$ を $\phi(z)$ で割って

$$g(z) = q(z)\phi(z) + r(z), \qquad q(z) \text{は商}, r(z) \text{は余りで次数が} m \text{より小},$$

とすれば, $\phi(B) \equiv 0$(零行列) だから $g(B) \equiv r(B) \pmod{p}$ である. 故に行列 B の $\boldsymbol{Z}_p$ 係数多項式の全体 $\mathcal{P}$ は法 $(p, \phi(z))$ での整数係数多項式の全体と同じ (同型) で, その元で異なるものの総数は

$$m - 1 \text{次以下の多項式の} \boldsymbol{Z}_p \text{係数のすべての取り方の総数} = p^m$$

である. (d) の仮定から $B, B^2, \cdots, B^{p^n-1} = E$ そして零行列は法 $(p, \phi(B))$ で考えてもすべて異なり, 全体として p^n 個あるから $n \leqq m$ でなければならない. 一方 Hamilton-Cayley の定理は $f_B(B) \equiv 0$(零行列) を保証し, $f_B(B)$ は最小多項式 $\phi(B)$ で割り切れるから $m \leqq n$ である. これから $m = n$ が確定し, $f_B(B)$ は $\phi(B)$ の定数倍, 共にモニックだから $\phi(B) = f_B(B)$ である. 言い換えると $f_B(z)$ は $\boldsymbol{Z}_p$ 既約で, $z^h \equiv 1 \pmod{p, f_B(z)}$ となる最小の h は $h = p^n - 1$ である. 故に $f_B(z)$ は $\boldsymbol{Z}_p$ 上の n 次原始多項式である. ■

上の (d)→(a) の証明を見た機会に, 後のための注意を記す.

Corollary 8.14. $\boldsymbol{Z}_p$ 上の $n \times n$ 行列 B の固有多項式 $f_B(z)$ は n 次 $\boldsymbol{Z}_p$ 原始多項式で, $\boldsymbol{Z}_p$ 上の n 次元ベクトル $\boldsymbol{X}_0$ は 0 連ではない (V_n^* に属す) 任意のものとする.

(a) 系列 $\{\boldsymbol{X}_k := B^k\boldsymbol{X}_0 |\ k = 0, 1, 2, \cdots\}$ の相続く n ベクトル $\{\boldsymbol{X}_k, \boldsymbol{X}_{k+1}, \boldsymbol{X}_{k+2}, \cdots, \boldsymbol{X}_{k+n-1}\}$ は番号 k に関係なく 1 次独立である.

(b) 行列表現 $\boldsymbol{X}_{k+1} = B\boldsymbol{X}_k$ で定義されるベクトル系列 $\{\boldsymbol{X}_k |\ k = 0, 1, 2, \cdots\}$ の成分 M 系列の全体は, 連結 M 系列としては Fushimi-Tezuka の定理の要件を満たすクラスに属している.

(証明) (a) ある番号 k に対する相続く m 個 $\{\boldsymbol{X}_k, \boldsymbol{X}_{k+1}, \boldsymbol{X}_{k+2}, \cdots, \boldsymbol{X}_{k+m-1}\}$ の 1 次従属関係

$$c_0\boldsymbol{X}_k + c_1\boldsymbol{X}_{k+1} + \cdots + c_{m-1}\boldsymbol{X}_{k+m-1} = 0$$

を考える. $\boldsymbol{X}_{k+j} := B^{k+j}\boldsymbol{X}_0$ だから上は

$$g(B)\boldsymbol{X}_k = B^k g(B)\boldsymbol{X}_0 = \boldsymbol{0}, \quad g(z) = c_0 z^0 + c_1 z^1 + \cdots + c_{m-1} z^{m-1},$$

を意味し, 正則行列 B^k の逆行列を掛けて $g(B)\boldsymbol{X}_0 = \boldsymbol{0}$ でなければならず, $g(B)\boldsymbol{X}_k = \boldsymbol{0}$ が**すべての** k で成り立つ. ベクトル $\boldsymbol{X}_k$ は $V_n{}^*$ の全ベクトルを巡回するから, これは $g(B) =$ 零行列 を意味して $g(B)$ は B の $\boldsymbol{Z}_p$ 係数の最小多項式 $f_B(B)$ で割り切れる. $f_B(B)$ は n 次だから $g(B)$ の次数 $m-1$ は $m-1 \geqq n,\ m \geqq n+1$ を満たす. 故に $m \leqq n$ の 1 次従属関係はどの番号 k でもあり得ない.
(b) $\boldsymbol{X}_k$ の成分系列がすべて 0 系列ではない M 系列で同一漸化式に従う事, 連結 M 系列である事, は定理 8.13.(a)→(b) の証明で触れた. 上の (a) によってこの連結 M 系列は Fushimi-Tezuka の定理の要件を (初期ベクトル $\boldsymbol{X}_0$ さえ 0 ベクトルではない様に選べば) 満たしている. ■

上の (b) の逆の事柄, Fushimi-Tezuka の定理の条件を満たす連結 M 系列が適当な正則行列 B に基づく行列漸化式表現を持つ事は後に触れられる.

Marsaglia-Tsay は上の定理 8.13.(d) を原始性の判定に用いる事を提案した. B が例えば 500 以上の大きい次元を持つ行列の時, 特に MT19937 の $n = 19937$ の様に巨大な行列である場合にはこれは実際的ではないが, Matsumoto-Nishimura[44] は次の簡明な判定法を提案し実際に用いた:

定理 8.15. $\boldsymbol{Z}_p$ 成分 $n \times n$ 正則行列 B について, 次の (a) と (e) は同値である:
(a) 行列 B の固有多項式 $f_B(z)$ は $\boldsymbol{Z}_p$ 上の n 次原始多項式である.
(e) ベクトル系列 $\{\boldsymbol{X}_k = B^k\boldsymbol{X}_0 |\ k = 1, 2, \cdots\}$ の成分系列の中に周期 $p^n - 1$ の $\boldsymbol{Z}_p$M 系列が 1 つ存在する.

(証明) 定理 8.13. の証明でも見た通り, (a) はベクトル系列の**すべての**成分系列は M 系列である事を保証し, (a)→(e) が成り立つ. 逆に (e) の成立を仮定する. ベクトル系列の周期はその各成分系列の周期の公倍数である. 故に第 i 成分が M 系列ならベクトル系列の周期は $p^n - 1$ の倍数である. また漸化式 $\boldsymbol{X}_{k+1} = B\boldsymbol{X}_k$ と B の正則性から, 系列に 0 ベクトルは含まれてはならず, 同じベクトルが出現すればそこからは同じベクトル系列の繰返しだから 1 周期にはすべて異なる 0 ベクトルではないベクトルを経由しなければならず, (e) は $\boldsymbol{X}_k$ が $V_n{}^*$ の異なる $p^n - 1$ の倍数個のベクトルを経由する事を要求する. $p^n - 1$ は $V_n{}^*$ の異なるベクトルの総数だから, ベクトル系列の周期は実際 $p^n - 1$ であり, 定理 8.13.(b) が, 従って (a) も成立し, 実はベクトル系列のすべての成分は M 系列である. ■

今や MT19937 構造の理解は容易である. Matsumoto-Nishimura の戦略は素数 $p = 2$ の特殊性を利用した漸化式次数 n の指定, 漸化式構造の簡素化等, 現段階で極限的な多くの精巧な工夫で成り立つが, 基本は上の定理のベクトル系列 $\{\boldsymbol{X}_k = B^k\boldsymbol{X}_0 |\ k = 0, 1, 2, \cdots, p^n - 1\}$ から適当な長さの部分を切り取って乱数として用いる構造にある. 即ち, 固有多項式 $f_B(z)$ が $\boldsymbol{Z}_2$ 上の n 次原始多項式になる $\boldsymbol{Z}_2$ 成分の**ある特殊な形の** $n \times n$ 行列 B と $\boldsymbol{Z}_p$ **上で零ベクトルではない任意の出発ベクトル** (n 連)$\boldsymbol{X}_0$ とを取る. 得られる n 次元ベクトル M 系列 $\{\boldsymbol{X}_k = B^k\boldsymbol{X}_0 |\ k = 0, 1, 2, \cdots\}$ は, B の特殊形から, 次数 m の小ベクトル $\boldsymbol{x}_k$ の d 個と半端な次数のベクトルに (スペースの節約のため行ベクトルで書いて) 次の形に切り分ける事がで

きる:

$$ {}^t\boldsymbol{X_k} = (\cdots, {}^t\boldsymbol{x}_{k-d+1}, {}^t\boldsymbol{x}_{k-d+2}, \cdots, {}^t\boldsymbol{x}_k), \quad d := [n/m], \quad [a] \text{ は } a > 0 \text{ の整数部分.} $$

この先頭の$\cdots$の成分は ${}^t\boldsymbol{x}_{k-d}$ の前半部の $m' = n - md$ 次元の部分からなり,[94] 切り分けを含む $\boldsymbol{X}_k$ の全体は「欠いた配列」と呼ばれている.[53] これから例えば m「ビット」の「一様乱数列」は $\{\boldsymbol{x}_k | \, k = 0, 1, 2, \cdots\}$ を 2 進 m 桁の小数と見做して, 即ち 2 進整数 $\boldsymbol{x}_k$ を整数 2^m で割って, 得る事ができる.[95] Fushimi-Tezuka の定理 6.7., 特に (6.24) 式の行列の行成分と比べれば直ちにわかる様に, 行ベクトル ${}^t\boldsymbol{X}_k$, ${}^t\boldsymbol{X}_{k+1}$, $\cdots$, ${}^t\boldsymbol{X}_{k+n-1}$ が Corollary 8.14. によって 1 次独立である事はまさしくこれら小ベクトル $\{\boldsymbol{x}_k | \, k = 0, 1, 2, \cdots\}$ が d 次均等分布を持つ事と同値である.[96] 従って行列 B の固有多項式 $f_B(z)$ が $\boldsymbol{Z}_2$ 上の n 次原始多項式である, と示す事さえできれば, MT19937 の生成する M 系列乱数は最大次数 $d = [n/m]$ の均等分布を ($\boldsymbol{Z}_p$ 上の出発ベクトル $\boldsymbol{X}_0 \neq \boldsymbol{0}$ の任意の選択で) 自動的に保証される.

漸化式の特性多項式 $f_B(z)$ が原始多項式である事は

$$ z^{2^{19937}} \equiv z \pmod{2, f_B(z)} $$

を確かめて示されるが, z の 2 乗の 19937 回の繰返しの計算ではこれには現在の大きなコンピュータでも数年掛かるという. Matsumoto-Nishimura の多くの素晴らしい工夫のうちの 2 つは, 定理 8.15. の利用, 線形漸化式の解ベクトルのある第 i 成分の作る系列 $\{x_k^{(i)} | \, k = 0, 1, 2, \cdots\}$ の周期が $2^{19937} - 1$ である, と示す事を選び, 彼らの漸化式の選択が可能にするその大きな高速計算方法を与えた所にある. 即ちまず n をメルセンヌ指数 19937 に取り周期 $2^{19937} - 1$ を素数に設定したので, Corollary 7.6.(c) により**系列の途中の値に注意する必要なく**

$$ x_{2^{19937}} \equiv x_1 \pmod{2} \tag{8.8} $$

だけを示せばよい. さらに Matsumoto-Nishimura の遷移行列 B は 100 項以上を持つ漸化式に対応するが, ベクトル形で 3 項漸化式に類似の形にまとめられ, それに基づく $f_B(z)$ の原始性の証明は $1 \leqq j \leqq 19937$ の j に対する $\{x_{2^j} | \, j = 1, 2, \cdots\}$ の算出の 1 週間程度の計算機稼働で可能だったと 1998 年の段階 [44] で報告されている.

4 バイト = 32 ビット 乱数として原理的に保証された $[19937/32] = 623$ 次均等分布性は誠に素晴らしい. 乱数の性質改善のため付加されたいくつかの手だて [53] も考えれば, 広く一般に使用の公開された [44),53)] この MT19937 は現在我々が使用可能な最も優れた一様乱数ルーチンと言えよう.

8.3. おわりに

乗算合同法, M 系列法, 加算生成法など乱数生成の構造原理を求める船旅も終った. 各方法

[94] Matsumoto-Nishimura[44)] の MT19937 での選択は $n = 19937$, $m = 32$, $d = 623$, $m' = 1$ である.

[95] MT19937 ではベクトル $\boldsymbol{x}_k$ にさらに定 $m \times m$ 行列を掛けたものを出力ベクトルとしている.

[96] Marsaglia-Tsay の行列表現の眼目は連結 M 系列乱数での出発ベクトルに対する Fushimi-Tezuka の条件の考察の必要を除く所にあるが, 上に見た様に, M 系列乱数構造での Fushimi-Tezuka の定理が与える規制は大変 far-reaching で, 群の構造でのラグランジュの定理の姿を思わせる所がある. 最も豊かな結果を得る道は, 多分, 一方の表現だけに頼らない自由な使い分けにあるのだろう. 後の p.161 とその脚注 [95] 参照.

の素晴らしい着想や可能性と共に, 直面した多くの厳しい限界には失望もあったが, 新しい展望にも勇気付けられた事は喜びである. 数理構造としての岩礁や原理的限界は動かし難いから嘆くには当らず迂回の一手であり, 人間の側にできるのは解析理解をさらに深める事, そして「計算可能性」の厳しい限界を (コンピュータが何千何万倍も高速になるのを待つのではなく) 新しい原理や方法を見出して乗り越える事である, と自らを励ますべきだろうか.

一般的に回顧すれば, 一様独立乱数列の様に「見える」と言っても 10 個以上の相続く数列がそれを実現する事さえどんなに難しいか, それを越えて例えば 100 個の乱数が独立と見える様にするのが数値計算的にどれほど高価になり得るか, を知らされた. 現在開かれた 623 次の均等分布の原理的保証の貴重さ大切さは明らかである. 歴史を振り返れば, しかし, 間を置かずにこの限界さえも窮屈と感じる応用は現れるだろうし, 対応して乱数生成方式の発展もコンピュータの速度の増大と共に迫られようが. ただどのようなルーチンにも道具にも機能的限界は常にある.

大切なのはそれら限界内でいかに使いこなすかの工夫だと思われる. 乱数生成機構も物理工学的シミュレーションも論評する立場にはないから, ここでは Knuth[2),52)] に記されている通り, どんな擬似乱数でもその欠点を暴くテストは必ず存在する事にだけ注意する. 例えば生成方法を典型的に $x_{k+1} = f(x_k)$ とすれば, テスト系列 $y_{k+1} := x_{k+1} - f(x_k)$ はランダムでもなんでもない $\{0, 0, 0, \cdots\}$ になって x_{k+1} と x_k が独立な場合とは掛け離れる. 或いは連結 M 系列乱数でも Marsaglia-Tsay の行列表現についても

$$B\,(\boldsymbol{X}_k\,\boldsymbol{X}_{k+1}\,\cdots\,\boldsymbol{X}_{k+n-1}) = (\boldsymbol{X}_{k+1}\,\boldsymbol{X}_{k+2}\,\cdots\,\boldsymbol{X}_{k+n})$$

がすべての番号 k で成り立つ事, 従って $n \times n$ 行列 $M_k := (\boldsymbol{X}_k\,\boldsymbol{X}_{k+1}\,\cdots\,\boldsymbol{X}_{k+n-1})$ と M_{k+1} とを知れば乱数発生方式を遷移行列 $B = M_{k+1}{M_k}^{-1}$ で特定できる事, は容易にわかる;[97] テスト系列 $M_{k+1}{M_k}^{-1}$ を調べれば, たとえ何次の均等分布を持とうと, 独立乱数列とは掛け離れた定行列 B になってしまう. だからこれらによってランダムではない, と棄却する事もできるがこれは苛酷に過ぎるし, (擬似) 乱数列の正しい使用方法ではない. 非常な高純度の試薬, 超高価高精度の装置を用いないと正しい結果が得られない実験も大切だが, 程々の精度の材料, 機器から精度の高い結果を robust に得る実験の工夫の価値は大きく, それが擬似乱数を用いる応用には求められているのではないだろうか.

また, 今迄の乱数事情を考えると, 乱数専門家からは乱数生成機構自体の, そして利点と欠点の分かりやすい速やかな周知が強く望まれる. それによって利用する側も擬似乱数にできる事, できない事をより早く深く理解し, 欠点を巧みに避ける実験努力, 工夫が可能になる. いつの時代でも高精度乱数は数値計算としては大変高価であり, 実験予算は限られているし, 乱数生成方式自体も開発者と使用者の実効ある相互作用によって最も大きく育つだろうから.

一様乱数生成の理論と実際に関しては Tezuka[55)] の教科書がこの先にある. 殆ど数の幾何学から始まる高度な内容だが, M 系列を基礎体である $\boldsymbol{Z}_p$ の中だけを動くものに限らず, その n 次拡大体である $K = \mathrm{GF}(p^n)$ の任意の生成元に基づく謂わば乗算合同法の拡張として統一的に捉え, K の乗法群 K^* 全体を動く系列 $\{x_k\}$ として得られる出力乱数構造について

[97] 従って Fushimi-Tezuka の条件を満たす連結 M 系列と Marsaglia-Tsay の行列表現とは同値である. また暗号理論的には Fushimi-Tezuka の条件を満たす連結 M 系列乱数の「解読」は容易である.[8),9)]

の理論的透視, 特に高精度乱数を目指す場合選ぶべき漸化式の項数,[98] コンピュータ上の暗号理論 [7),8),9)] で問題となる「暗号理論的に安全な」乱数, 或いは非線型漸化式即ち有限体の置換多項式 [56)] を用いるものや漸化式前項の $\boldsymbol{Z}_p$ での逆数を用いる inversive method その他,[99] さらに我々が単に直観的に考えた乱数系列の精度をどの様に定量的に定義し検定するか, 結果はどの様になるか, 2 つ以上の乱数を組合わせるとその精度がどの様に向上できるか等, 多くの専門的情報を与えている. 著者達が開発して性質を詳しく調べた

複数の M 系列乱数の exclusive-or を取って相互に shuffle した乱数列

の高性能も実際使用からは注目される.

この機会に紹介すると, 2 つ以上の乱数列を交ぜ合わせて或いは一方で他方を shuffle してよりよい性能の乱数を目指す事は自然だが, それは検定を経ないと危険であるとも注意される. これについては専門家による評論 review, L'Ecuyer[57)], Niederreiter[58)] 等もぜひ参照して頂きたい. L'Ecuyer には 2 つ以上の乱数を混ぜ合わせて検定もせずによい性能だろうと考えて使う事は, ある人の言として,

better the unknown than the devil we know
「知らない方が知っている悪魔よりはまし」

と考える態度だ, と記され, さらに Niederreiter の指摘, 例えば乱数系列 $\{x_k, y_k\}$ の exclusive-or を取って $z_k := x_k \oplus y_k$ を作れば (いつも) 性質が良くなる, と考えるのはおかしい, なぜならそれが正しければ同じ議論で $x_k = y_k \oplus z_k$ が $\{z_k\}$ より性質が良いと言えようから, も付記されている. 教訓は, 「直感や思い付きで良かろうと考えて作っても乱数の良さは検定しない事にはわからない」, に尽きる.

これらすべての事柄について, 乱数に限らない計算理論や関連する数論等多くの事柄について, 今やクヌース [2)] が参照すべき第 1 の重要な参考書である. まえおきでも触れたように, 我々の旅は実際この教科書を読む困難をなくすためだったし, 現時点ではそれはまた伏見 [4)], L'Ecuyer[57)], Niederreiter[58)], Tezuka[55)] そして松本 [53)] への容易な導入を目指していたとも言える. これらの理解の上にさらに優れた応用が開かれる事を願う. このクヌースの優れた教科書は最近改訂された. ぜひ原書 [52)] も繙いて頂きたい.

またこの終点は現在の多くの代数学の教科書の出発点である. 有限体だけに限れば大変詳しい成書 [56)] も存在する. 我々のこの随分長い彷徨が「どうしてこんな抽象的な議論をするのだろう」という数学, 特に代数学を学ぶ際の最初の大きな barrier の低減, 必要性への透視や興味の喚起にも役立つなら幸いこの上ない.

[98] さらに根源的に言えば, 3 項漸化式と限らない最良の漸化式形の選択と共に連結 M 系列乱数の出発ベクトルの選択も, 困難は大きいが, 考えなければならないと思われる.[45)]

[99] これらは計算的には負荷が大きく最速ではないだろうしシミュレーションのための長周期の生成は容易ではないかもしれないが, スペクトル検定で言う格子構造は存在しない.

付録 A: T-及び LP-型乱数の不均等分布

我々は伏見[46]が示し, 第 6 章で再確認した「T 型系列と LP 型系列の相反性」から両方式が美点も欠点も共有すると知った. 連結 M 系列乱数として Tausworthe 乱数系列一般が理論的に可能な均等分布の性質を実現するとは限らない事は, Tootill et al.[47]が既に 1971 年に文献[10]の証明論理の不備として指摘し, また同じ方式で均等分布を確保するある判別法を記した. この事情は Fushimi and Tezuka[12]にも「Tausworthe 系列は, もしパラメータが適当に選ばれれば, 均等分布をする」, と婉曲に指摘されている所である. これらの記述だけでは状況の理解は難しいから, T 及び LP 系列が共に, 一般には理論的に可能な均等分布の性質を持たない 事を明確にし, 伏見-手塚の定理の重要さを得心しよう. 幸いにしてそれは簡単な例で可能である.

伏見-手塚の論文[12]の大変見やすい例を引用する. $\boldsymbol{Z}_2$ 係数の 6 次多項式

$$f(z) = z^6 + z^3 + 1 \tag{A1}$$

は原始多項式である. 即ち $f(z) = 0$ を特性方程式とする線形漸化式

$$x_k = x_{k-3} + x_{k-6} \pmod 2 \tag{A2}$$

の解は, 「すべて 0」ではない任意の出発 6 連 $\{x_0, x_1, \cdots . x_4, x_5\}$ に対して理論的に最長の周期 $2^6 - 1 = 63$ を与える. 証明は簡単で, 実際出発 6 連として識別しやすい $\{1, 1, 1, 1, 1, 1\}$ を取って線形漸化式の解を計算すれば (手でも容易だし, パソコンならもっと簡単きれいに打ち出し印刷させる事ができるが):

$x \setminus j$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
x_j	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	0
x_{10+j}	0	1	0	0	0	0	1	1	0	0	0	1	0	1	0	0
x_{20+j}	0	1	0	1	0	0	1	1	1	1	0	1	0	0	0	1
x_{30+j}	0	1	0	0	0	1	1	1	0	0	1	0	0	1	0	1
x_{40+j}	1	0	0	1	0	1	1	0	1	1	1	0	1	1	0	0
x_{50+j}	1	0	1	1	0	0	1	1	0	1	0	1	0	1	1	1
x_{60+j}	0	1	0	1	1	1	1	1	1	0	0	0	0	0	1	0
x_{70+j}	0	0	0	0	1	0	0	0	0	1	1	0	0	0	1	0

(A3)

確かに, 1 ばかりの 6 連は x_{63} から x_{68} に始めて再登場するから, 漸化式系列の 1 周期分は x_0 から x_{62} であり, 周期は 63 である.

この M 系列を $m = 3$ 連結して T 型系列を作る. M 系列の周期 $63 = 3^2 \times 7$ は 10 とは素だから, $s = 10$ を取った

$$u_k := x_{10k} x_{10k+1} x_{10k+2}, \quad k = 0, 1, 2, \cdots, \tag{A4}$$

は確かに T 型系列である. 我々は 1 周期にわたる分布の均等性だけを議論したいのだから一様乱数目的の実用は無視して, u_k を整数と考え $2^3 = 8$ 個の値

$$(000)_{(2)} = 0,\ (001)_{(2)} = 1,\ (010)_{(2)} = 2,\ (011)_{(2)} = 3,$$

$$(100)_{(2)} = 4,\ (101)_{(2)} = 5,\ (110)_{(2)} = 6,\ (111)_{(2)} = 7$$

で分類される抽象的な系列と見て十分である. 系列 $\{u_k|\ k=0,1,2,\cdots 7\}$ は k を法 63 で考え, 上の表 (A3) の相続く 3 つの項に当てはめて列方向に (番号で 10 跳びに) 読み取りながら進んで容易に得られる. 結果をまとめると次の通り:

u_0	1	1	1	u_{13}	1	1	0	u_{26}	0	0	0	u_{39}	0	0	0	u_{52}	1	1	0
u_1	0	1	0	u_{14}	0	0	1	u_{27}	0	0	0	u_{40}	0	1	0	u_{53}	1	1	1
u_2	0	1	0	u_{15}	0	0	1	u_{28}	1	1	0	u_{41}	0	0	0	u_{54}	1	1	0
u_3	0	1	0	u_{16}	0	1	1	u_{29}	0	0	1	u_{42}	0	1	0	u_{55}	1	0	1
u_4	1	0	0	u_{17}	0	1	1	u_{30}	1	1	1	u_{43}	1	1	0	u_{56}	1	1	0
u_5	1	0	1	u_{18}	0	0	1	u_{31}	0	1	0	u_{44}	0	1	1	u_{57}	1	1	1
u_6	0	1	0	u_{19}	1	1	1	u_{32}	1	0	0	u_{45}	0	0	1	u_{58}	0	0	0
u_7	0	0	0	u_{20}	1	0	0	u_{33}	0	1	1	u_{46}	0	0	1	u_{59}	1	0	0
u_8	1	0	0	u_{21}	1	0	1	u_{34}	0	1	1	u_{47}	1	0	1	u_{60}	0	0	1
u_9	1	1	1	u_{22}	1	0	0	u_{35}	1	1	1	u_{48}	0	1	0	u_{61}	1	0	1
u_{10}	1	0	0	u_{23}	0	0	1	u_{36}	1	1	0	u_{49}	1	1	0	u_{62}	1	0	0
u_{11}	0	1	1	u_{24}	0	1	1	u_{37}	0	1	1	u_{50}	1	0	1	u_{63}	1	1	1
u_{12}	1	0	1	u_{25}	1	0	1	u_{38}	1	1	1	u_{51}	0	0	0	u_{64}	0	1	0

これの相続く対 $\{(u_k,u_{k+1})|\ k=0,1,\cdots,62\}$ が作る平面の点を可能な値の $8^2=64$ 個の升目へ集計する事は, 少々時間はかかるが全く容易である:

7		2		2	2		2	
6	2		2			2		2
5		2		2	2		2	
4	2		2			2		2
3		2		2	2		2	
2	2		2			2		2
1		2		2	2		2	
0	1		2			2		2
u_{k+1}/u_k	0	1	2	3	4	5	6	7

これは $m=3$ ビット (乱数) 系列 $\{u_k|\ k=0,1,2,\cdots\}$ が $n/m=2$ 次均等分布, 例えば今の場合 $u_k\neq 0$ が出たあと u_{k+1} として $\{0,1,2,\cdots,7\}$ がすべて 1 度ずつ出るが $u_k=0$ の後では $u_{k+1}=0$ だけは出ない, という性質, を満していないと証明している. T 型系列は一般に理論的に可能な n/m 次の均等分布はしない. 従って LP 系列も同様である.

Tootill et al.[47] の指摘した事は, この例に限定して言えば, T 型 $m=3$ 連結 M 系列乱数 $\{u_k|\ k=0,1,2,\cdots\}$ が上の通り $n/m=2$ 次均等分布をしないという判定[100]と, 今一つ, T 型 $m'=2$ 連結乱数列 $\{v_k:=x_{10k}x_{10k+1}|\ k=0,1,2,\cdots\}$ を選べば $n/m'=6/2=3$ 次均等分布を得るだろう, という判定[101]とである. この後者の結論の正しさは $\{v_j\}$ を

$$v_k=(00)_2=0,\quad (01)_2=1,\quad (10)_2=2,\quad (11)_2=3$$

[100] それは $sm=30$ が周期 $2^6-1=63$ と 素ではない から, である.
[101] それは $sm'=20$ が周期 63 と素である事に基づく.

の 4 つの値を取る系列, 但し番号 k は法 63 で考える, と見て表 (A3) から読み取り, 3 次元のプロットは手では無理だから相続く 3 連系列

$$\{(v_k, v_{k+1}, v_{k+2})|\ k = 0, 1, 2, \cdots, 62\}$$

が $0, 1, 2, 3$ の 4 値 3 連のあらゆる可能な組み合わせ, 具体的に記せば

$$\begin{array}{cccccccc}
(0,0,0) & (0,0,1) & (0,0,2) & (0,0,3) & (0,1,0) & (0,1,1) & (0,1,2) & (0,1,3) \\
(0,2,0) & (0,2,1) & (0,2,2) & (0,2,3) & (0,3,0) & (0,3,1) & (0,3,2) & (0,3,3) \\
(1,0,0) & (1,0,1) & (1,0,2) & (1,0,3) & (1,1,0) & (1,1,1) & (1,1,2) & (1,1,3) \\
(1,2,0) & (1,2,1) & (1,2,2) & (1,2,3) & (1,3,0) & (1,3,1) & (1,3,2) & (1,3,3) \\
(2,0,0) & (2,0,1) & (2,0,2) & (2,0,3) & (2,1,0) & (2,1,1) & (2,1,2) & (2,1,3) \\
(2,2,0) & (2,2,1) & (2,2,2) & (2,2,3) & (2,3,0) & (2,3,1) & (2,3,2) & (2,3,3) \\
(3,0,0) & (3,0,1) & (3,0,2) & (3,0,3) & (3,1,0) & (3,1,1) & (3,1,2) & (3,1,3) \\
(3,2,0) & (3,2,1) & (3,2,2) & (3,2,3) & (3,3,0) & (3,3,1) & (3,3,2) & (3,3,3)
\end{array}$$

の $4^3 = 8^2 = 64$ 個から 0 連 $(0,0,0)$ は除いた 63 個を 1 度ずつ取る事を, 例えば上の 64 個の組み合わせを (v_k, v_{k+1}, v_{k+2}) の実現と共に消去して, 確認すれば容易に確かめられる. 少し時間はかかるが, 丁度手頃な演習問題である. 手で試みて確認し, この様に文献 [47] では均等分布の十分条件は得られていたが, 必要十分の完全な判定には伏見-手塚の定理を待たなければならなかった状況を実感了解して頂きたい.

付録B. 一般の線形漸化式の周期

乱数生成方式として見ると, 素数の法 p での n 次M系列法は整数係数の n 次線形漸化式

$$x_k \equiv b_1 x_{k-1} + b_2 x_{k-2} + \cdots + b_n x_{k-n}, \quad b_n \neq 0 \pmod{p} \tag{5.1}$$

の利用の特殊な一例だった. その特殊性は (5.1) に付随する決定方程式或いは特性 (固有) 方程式

$$f(z) = z^n - b_1 z^{n-1} - b_2 z^{n-2} - \cdots - b_{n-1} z^1 - b_n = 0 \tag{5.2'}$$

が $\boldsymbol{Z}_p$ で既約で, さらに $\boldsymbol{Z}_p$ の n 次拡大体 $\mathrm{GF}(p^n)$ の乗法群 $K^* = \mathrm{GF}(p^n) - \{0\}$ の生成元を根に持つ n 次原始多項式である, という所にあった. $\boldsymbol{Z}_p$ 既約多項式 (一般に任意の有限体係数の既約多項式でも同じ) の特性根 $\{a_1, a_2, \cdots, a_n\}$ は個数十分で, 線形漸化式の一般解はこれらによる

$$x_k = c_1 (a_1)^k + c_2 (a_2)^k + \cdots + c_n (a_n)^k \tag{5.3}$$

の表現を任意の初期条件 $\{x_0, x_1, \cdots, x_{n-1}\}$ に対して常に持った. 特性根 $\{a_1, a_2, \cdots, a_n\}$ は共通の位数 h(h は $p^n - 1$ を割り切る, $h | p^n - 1$) を持ち, $f(z)$ の指数とも呼ばれ, 0 連を除くすべての初期値 $\{x_0, x_1, \cdots, x_{n-1}\}$ に対して (5.1) の解系列 $\{x_k\}$ に同じ周期 h を与えた.

数理構造としてもっと一般の線形漸化式ではどうなるか, は自然な疑問である. 結論的には, 特性多項式が $\boldsymbol{Z}_p$ 既約ではない線形漸化式の解の周期の姿は外見的には非常にややこしい. 例えば周期が理論的な最長の $p^n - 1$ にはならないのは当然として, 初期条件によってこの解の周期が一般に変ってしまう. 長くもない周期の上に初期条件への複雑な配慮を必要とする乱数ルーチンでは明らかに実用には適さない. しかしどうしてそうなのか, を考える事は有限体だけの議論を越えて, 多項式 (環) による問題の拡張定式化の必然と力強さとを理解し, 理論全体の構造のよりよい見通しを得る道でもある. もはやその議論は難しくはないのだから, この付録で演習形式も交えて是非触れておこう.

再び p は素数を表すとする. $\boldsymbol{Z}_p$ 係数の n 次特性多項式 $f(z)$ が $\boldsymbol{Z}_p$ 可約で, モニックな F 既約多項式への因数分解

$$f(z) = g(z) h(z) \cdots \tag{B1}$$

を持つがこれら $\boldsymbol{Z}_p$ 既約因数に重複がない, $f(z)$ が square-free である, 場合を最初に考える. $f(z)$ の $\boldsymbol{Z}_p$ 既約因数 $g(z),\ h(z),\ \cdots$ には共通根はない事に注意する.[102] $g(z)$ が i 次, $h(z)$ が j 次, $\cdots$ で $i + j + \cdots = n$ だとしよう. $\boldsymbol{Z}_p$ 既約な i 次多項式 $g(z)$ を 1 次因数に分解するには $\mathrm{GF}(p^i)$ の拡大体である有限体, 即ち p^i の何乗かを位数を持つ $\mathrm{GF}((p^i)^l) = \mathrm{GF}(p^{il}),\ l \geqq 1$ に限られる, を取ればよい. 同様に $h(z)$ は $\mathrm{GF}(p^j)$ を含む有限体 $\mathrm{GF}(p^{jl'}),\ l' \geqq 1$, で 1 次因数に分解される. だから n 次で $\boldsymbol{Z}_p$ 可約だが square-free な特性多項式 $f(z)$ は $\mathrm{GF}(p^N)$, N は既約因数の次数 $i, j, \cdots$ の最小公倍数, で完全に 1 次因数に分解される. 有限体 $\mathrm{GF}(p^n)$ と

[102] 以前の議論, 任意の有限体 F を係数とする既約多項式 $g(z)$ が根 α を F の拡大体 K に持てば, $g(z)$ は α を根とする F 係数多項式の中で最小次数 (α の F 係数最小多項式) であり, 同じ F 係数の多項式 $h(z)$ も α を根とするなら $g(z)$ は $h(z)$ を F 係数で割り切る事を思い出そう; 実際 $g(z)$ で $h(z)$ を F 係数で割って $h(z) = q(z)g(z) + r(z)$ として $r(\alpha) = 0$ だから, $g(z)$ より低次の余り $r(z)$ は定数 0 以外あり得ない. $h(z)$ も F 既約なら, $h(z)$ は $g(z)$ と同次数で商 $q(z)$ は定数でなければならない. 故に任意有限体係数の 2 つの既約多項式は互いに他の F 定数倍であるか, 或いは共通根は全くなく互いに素であるか, の 2 者択一である.

は一般に異なる $\mathrm{GF}(p^N)$ がこの場合線形漸化式 (5.1) の解析の舞台である. しかしこの中での $f(z)$ の単根 $\{a_1, a_2, \cdots, a_n\}$ によって線形漸化式 (1) の任意の初期条件に対する解が (5.3) の形に表されることは第 5 章の始めに 0 ではない Vandermonde 行列式を用いて議論した通りで, 解系列の周期もこの構造から容易に透視される. i 次既約因数 $g(z)$ に属する根の位数 ($\boldsymbol{Z}_p$ 既約多項式 $g(z)$ の指数)h' は乗法群 $\mathrm{GF}(p^i) - \{0\}$ の位数 $p^i - 1$ の約数, j 次の $h(z)$ の根の位数 h'' は $p^j - 1$ の約数, $\cdots$ である. だから線形漸化式 (5.3) の形の解の周期は初期条件が $g(z)$ の根だけで表せるなら h' であり, 例えば $g(z)$ の根と $h(z)$ の根の両方が必要なら h' と h'' の最小公倍数になる. square-free な $\boldsymbol{Z}_p$ 既約因数の積である特性多項式の場合可能な最大周期は, 全既約因数の指数の最小公倍数 L である. 勿論この最大周期を実現する初期条件, 線形漸化式 (5.1) の出発 n 連 $x_0, x_1, \cdots, x_{n-1}$, を選ぶのは実際手続きとしては簡単ではないし, またたとえそれが可能でも周期 L は $\mathrm{GF}(p^n)$ 上のM系列の場合には及ばない:

$$L \leqq (p^i - 1)(p^j - 1) \cdots < p^{i+j+\cdots} - 1 = p^n - 1.$$

乱数生成方式としては, だから, 初期条件選択に依らずこの最大周期を得るために, (B1) の形の特性多項式を持つ線形漸化式ではなく n 次M系列を選ばなければならない.

$\boldsymbol{Z}_p$ 上の線形漸化式の数理構造の一般論は $f(z)$ が squre-free でなく重根を持つ場合で完成する. 既に記した様に, この場合を解剖するには有限体とその中での特性根の議論ばかりではなくより広い代数系である「環」, 具体的には $\boldsymbol{Z}_p$ 係数の 1 変数の多項式の四則演算の考察, と共に, それに基づく特殊な技法が要求される. 一様乱数の実用構造としてはM系列法がやはり最も将来有望と見えるから, 乱数問題のためだけならこの技法にこれ以上は立ち入らなくてもよいとも思われるが, 多くの応用分野で「環」は重要である. 今までに得た知識からはもはや困難は少なく, 行われる議論の底の構造も多く見える. だから第 7 章の議論の反芻消化も兼ねて, 以下簡単な演習問題で「多項式」を用いる方法の必要, 新しい考え, 展望を得て, 環の広い応用分野への我々の可能性を開いておこう.

具体的に $\boldsymbol{Z}_3$ 上の 4 次特性多項式

$$f(z) = (z-1)^4 = z^4 - 4z^3 + 6z^2 - 4z + 1 \equiv z^4 - z^3 - z + 1 \pmod 3 \qquad \text{(B2)}$$

を例に取る. 特性方程式 $f(z) = 0,\ z^4 = z^3 + z - 1$ が表す $\boldsymbol{Z}_3$ 上の 4 次線形漸化式は

$$x_k \equiv x_{k-1} + x_{k-3} - x_{k-4} \pmod 3 \qquad \text{(B3)}$$

である. これは x_{k-4} について逆に解く事もできて, 明らかに線形漸化式 (B3) は逆行可能である. 初期条件の 4 連 $\{x_0, x_1, x_2, x_3\}$ が 0 ばかりの 0 連なら以後もすべて 0 になり, 逆行系列も同様だから, 0 連以外の 4 連を任意に与えれば (B3) は以後のすべての $k \geqq 4$ に対して x_k を一意に決定し 0 連は決して出現せず, 同じ 4 連が出て系列は繰り返す. $\boldsymbol{Z}_3$ 上での 4 連の総数は 0 連を除いて $3^4 - 1 = 80$ と有限だから, (B3) の解系列は必ず周期を持ち, その原理的最大周期はM系列の場合のこの 80 である.[103] 勿論 (B2) の特性多項式 $f(z)$ は既約ではなく, この最大周期は実現しない. 周期は次の方法で見出される.

符号理論で符号それぞれを「多項式符号」と対応させて, 或いは「表現」して考えた様に, まず (B3) の線形漸化式の解 $\{x_k |\ k = 0, 1, 2, \cdots\}$ に伴われる母関数 $G(z)$ を導入する:

$$G(z) := x_0 + x_1 z + x_2 z^2 + \cdots + x_k z^k + \cdots.$$

[103] 逆に (B3) の解系列の周期がある初期条件に対して 80 なら, 実際それは $\boldsymbol{Z}_3$ M系列, $f(z)$ は 4 次原始的である事も Lemma 6.2.(b) で見られている.

上に述べた通り, どの様に初期条件を取っても解系列 $\{x_k\}$ は必ず有限の周期 $T \leqq 80$ を持ち, $x_{T+k} = x_k$ が成り立つから, $G(z)$ は実際は次の形になる:

$$G(z) = \sum_{j=0}^{\infty} \sum_{k=0}^{T-1} x_{jT+k} z^{jT+k} = \sum_{j=0}^{\infty} (z^T)^j R(z) = \frac{R(z)}{1-z^T}, \quad R(z) := \sum_{k=0}^{T-1} x_k z^k. \tag{B4}$$

ここではわかりやすいように x_k は $0 \leqq x_k \leqq p-1 = 2$ の整数, z は複素数で $|z| < 1$ だと仮定して $G(z)$ や $R(z)$ を頭の中で複素関数に固定した.[104] 次の計算が成り立つ:[105]

$$\begin{aligned} f(z)G(z) &= (z^4 - z^3 - z + 1)(x_0 + x_1 z + x_2 z^2 + \cdots + x_k z^k + \cdots) \\ &= x_0 + x_1 z + x_2 z^2 + x_3 z^3 + x_4 z^4 + \cdots \\ &\quad - x_0 z - x_1 z^2 - x_2 z^3 - x_3 z^4 + \cdots \\ &\quad - x_0 z^3 - x_1 z^4 + \cdots \\ &\quad + x_0 z^4 + \cdots \\ &= Q(z) + \sum_{k=4}^{\infty} z^k (x_k - x_{k-1} - x_{k-3} + x_{k-4}). \end{aligned}$$

ここで $Q(z)$ は次で定義される:

$$Q(z) = x_0 + (x_1 - x_0)z + (x_2 - x_1)z^2 + (x_3 - x_2 - x_0)z^3. \tag{B5}$$

$f(z)G(z)$ の右辺で $Q(z)$ 以外の和の項は $\{x_k\}$ が漸化式 (6) の解だから消えて:[106]

$$f(z)G(z) = Q(z) + 3S(z). \tag{B6}$$

これに (B4) の関係を用いよう. 両辺に $1 - z^T$ を掛ければ,

$$f(z)R(z) = (1 - z^T)\{Q(z) + 3S(z)\}.$$

即ち (B3) の解の周期 T は任意の $|z| < 1$ に対して次の恒等式を満たさなければならない:

$$\begin{aligned} &(z-1)^4 R(z) = (1 - z^T)\{Q(z) + 3S(s)\}, \quad R(z) := \sum_{k=0}^{T-1} x_k z^k, \\ &Q(z) = \Big\{x_0 + (x_1 - x_0)z + (x_2 - x_1)z^2 + (x_3 - x_2 - x_0)z^3\Big\}. \end{aligned}$$

係数を法 3 で考える問題ではこれは

$$(z^T - 1)Q(z) = -f(z)R(z) = -(z-1)^4 R(z) \pmod 3 \tag{B7}$$

である. この恒等式には T を与える大変精妙な構造がある. 具体的な問題にして考えよう.

問題 B.1.(1) 初期条件 $x_0 = 1, x_1 = 1, x_2 = 1, x_3 = 1$ を選ぶ. これに対する線形漸化式

---

[104] 本来は $G(z)$ や $R(z)$ を「$\boldsymbol{Z}_3$ 係数の形式的冪級数」と考える方が便利である. 脚注[107] 参照.

[105] この演習問題には少し工夫があって $g(z) := z^4 f(1/z) = f(z)$ が成り立つ様に作られている. 一般には $g(z) \neq f(z)$ であり, 下の式では $g(z)G(z)$ を計算しなくてはならない. 本文の p.122 を参照.

[106] $G(z)$ の中で我々は z を絶対値が 1 より小さい複素数と取り, その「係数 x_k は法 3 の数ではなく $0 \leqq x_k \leqq 2$ の整数」と考えたから, 本当は $x_k - x_{k-1} - x_{k-2} + x_{k-4}$ は一般には整数 0 ではなく k 毎に決まったある 3 の倍数 $3c_k$ だとしなければならない. 但し x_k は法 3 で周期的だから $\{c_k\}$ も周期的で絶対値はある定数で上限を押さえられ, $f(z)G(z) = Q(z) + 3S(z)$, $S(z) = \sum_{k=4}^{\infty} c_k z^k$. $S(z)$ は $|z| < 1$ で収束が保証された整数係数冪級数である. 以下必要な z の各冪の係数の法 3 での計算ではこの付加項の全体 $3S(z)$ は全く影響を与えないのでその存在は無視してよいが以下少しの間記す. $\boldsymbol{Z}_3$ 係数形式的冪級数の見方はこの煩雑な考察を不要にする.

$$x_k \equiv x_{k-1} + x_{k-3} - x_{k-4} \pmod 3 \qquad \text{(B3)}$$

の解系列を下に計算し, すべての $k = 0, 1, 2, \cdots$ に対して $x_{k+T} = x_k$ となる最小の正の T, すなわち周期 T を求めなさい.

(解)

k	0	1	2	3	4	5	6	7	8	9	10	11	12
x_k	1	1	1	1	1	1	1	1	1	1	1	1	1

故に周期 $T = 1$ である. **(問題 B.1.(1) 終り)**

線形漸化式 (B3) の解系列が未知, 従って周期 T と $R(z)$ が不明であっても, 出発 4 連 $x_0 = 1, x_1 = 1, x_2 = 1, x_3 = 1$ は $Q(z)$ を決定する:

$$Q(z) = x_0 + (x_1 - x_0)z + (x_2 - x_1)z^2 + (x_3 - x_2 - x_0)z^3 = 1 - z^3.$$

故に (B7) の恒等式は次の形を取る:

$$(z^T - 1)Q(z) = (z^T - 1)(1 - z^3) = -(z - 1)^4 R(z) \pmod 3.$$

法 3 では $(z-1)^3 = z^3 - 3z^2 + 3z - 1 \equiv z^3 - 1$ である事に注意しよう. そうすると法 3 での両辺の共通因数 $Q(z) = -(z-1)^3$ を除いて, 我々は次の恒等式を得る:

$$z^T - 1 = f_1(z)R(z) \pmod 3, \quad f_1(z) := z - 1 = \frac{-f(z)}{\mathrm{GCD}(f(z), Q(z))}.$$

これは $f_1(z) = z - 1$ が $z^T - 1$ の法 3 での因数であることを意味する. 即ち

$$z^T - 1 = f_1(z)R(z), \quad z^T = 1 + f_1(z)R(z). \qquad \text{(B8)}$$

これが大きな一般的構造の一端である. 文字 z の $\boldsymbol{Z}_3$ 係数の多項式の全体 $\boldsymbol{Z}_3[z]$ を考え, これらの多項式の間に「法 $(p, f_1(z))$ で等しい」という関係を

係数の $p = 3$ の倍数の違い, 2 つの多項式の間の定
まった (法) 多項式 $f_1(z)$ の倍数の違いは無視して

定める. 即ち任意の $u(z), v(z), f_1(z) \in \boldsymbol{Z}_p[z]$ に対しある $a(z) \in \boldsymbol{Z}_p[z]$ が存在し, 係数を法 p で同定するとき $u(z) \equiv v(z) + a(z)f_1(z)$ が成り立つ事を $u(z) \equiv v(z) \pmod{p, f_1(z)}$ と定義する. この言葉では上の (B8) 式は次を意味する:

$$z^T \equiv 1 \pmod{p, f_1(z)}, \quad p = 3,\ f_1(z) := z - 1 = \frac{-f(z)}{\mathrm{GCD}(f(z), Q(z))}. \qquad \text{(B8')}$$

Lemma. 任意に与えられた法 p と法多項式 $f_1(z) \in \boldsymbol{Z}_p[z]$ に対して $z^a \equiv 1 \pmod{p, f_1(z)}$ となる正または 0 の整数 a の全体を B とする. B の正の最小のもの (があるとしてそれ) を P とすれば, B は P の倍数の全体と等しい:

$$B = \{a \in \boldsymbol{Z} |\ a \geqq 0,\ \ z^a \equiv 1 \pmod{p, f_1(z)}\} = \{kP |\ k = 0, 1, 2, \cdots\}.$$

(証明) 任意の $a \in B$ を取り, B の中の正で最小のもの P で割って $a = qP + r$, q, r は整数の商と余り $0 \leqq r < P$ とする. $a, P \in B$ から $z^a \equiv 1 + s(z)f_1(z) \equiv 1,\ z^P \equiv 1 + S(z)f_1(z) \equiv 1 \pmod{p, f_1(z)}$ がある $s(z),\ S(z) \in \boldsymbol{Z}_p[z]$ について成り立ち,

$$1 \equiv z^a = z^{qP+r} = (z^P)^q z^r \equiv z^r \pmod{p, f_1(z)}.$$

故に $r \in B$ だが B の正の最小のものが P なのだからそれより小さい $r = 0$ でなければなら

ない. 即ち B の任意の数 a は P で割り切れる. 逆に P の任意の倍数 kP が B に入っている事は $z^{kP} = (z^P)^k \equiv 1^k = 1 \pmod{p, f_1(z)}$ から明らか. ■

こうして非常に一般に, 条件 (B8') 即ち (B8) を満たす T には正で最小のものがあり, 他のものはその倍数になっている事が知られた. 数学定理は頭に入りにくい. 例で確かめよう.

問題 B.1.(2) 実際に初期条件 $x_0 = 1, x_1 = 1, x_2 = 1, x_3 = 1$ と $T = 1$ とを (B8) に入れて, $T = 1$ はこの初期条件に対して恒等式 (B8) を満たす事を確かめなさい. また, すべての $T = 2, 3, \cdots$ に対しても恒等式 (11) が成り立つ事を示しなさい.

(証明) $T = 1$ として $R(z) = x_0 z^0 = 1$. 故に $f_1(z) = z - 1$ から

$$z^T - 1 = z - 1 = f_1(z)R(z).$$

確かに (11) は $T = 1$ で成り立つ恒等式である. 任意の正の整数 T を考えると, 今の場合すべての $x_k = 1$ だから $R(z) = 1 + z + z^2 + \cdots + z^{T-1}$ であり,

$$z^T - 1 = (z - 1)(z^{T-1} + z^{T-2} + \cdots + z + 1) = f_1(z)R(z).$$

再び確かに, 恒等式 (B8) はすべての正の整数 T でも成り立っている. ■

問題 B.2.(1) 今度は初期条件 $x_0 = 1, x_1 = 0, x_2 = 0, x_3 = 1$ を選ぶ. この初期条件に対する線形漸化式 (B3), $x_k \equiv x_{k-1} + x_{k-3} - x_{k-4} \pmod 3$, の解系列を下に計算しなさい:

(解)

k	0	1	2	3	4	5	6	7	8	9	10	11	12
x_k	1	0	0	1	0	0	1	0	0	1	0	0	1

故に周期 $T = 3$. **(問題 B.2.(1) 終り)**

問題 b.2.(2) 上で T は線形漸化式 (B3) の解系列から得られた. しかしこの解系列の知識を仮定せず, 周期 T と $R(z)$ が不明の場合でも, 出発 4 連は $Q(z) = 1 - z$ の形を与え, (B7) が $(z^T - 1)(1 - z) = -(z - 1)^4 R(z)$ でなければならないこと, 即ち次の形の恒等式になる事を我々に知らせる:

$$z^T - 1 = f_1(z)R(z) \pmod 3, \quad f_1(z) := \frac{-f(z)}{\mathrm{GCD}(f(z), Q(z))} = (z - 1)^3.$$

これは $f_1(z) = (z - 1)^3 \equiv z^3 - 1 \pmod 3$ が $z^T - 1$ を法 3 で割り切る (当然 $T \geqq 3$ である) 事を意味し, T が満たすべき次の (必要) 条件を与える:

$$z^T = 1 + (z - 1)^3 R(z) \equiv 1 \pmod{3, f_1(z)}. \qquad \text{(B9)}$$

$T = 3$ が実際に (B9) を満たす事を初期条件 $x_0 = 1, x_1 = 0, x_2 = 0, x_3 = 1$ と $T = 3$ とを (B9) に入れて確かめ, さらに 3 のすべての倍数も (B9) を満たす事を直接示しなさい.

(証明) $T = 3$ だから $R(z) = 1 + 0z + 0z^2 = 1$. 故に

$$(z - 1)^3 R(z) = (z - 1)^3 = z^3 - 3z^2 + 3z - 1 \equiv z^3 - 1,$$

従って $T = 3$ は恒等式 (12) を満たす. 3 の倍数の例えば $T = 3j$ の場合

$$R(z) = 1z^0 + 1z^3 + 1z^{3\cdot 2} + 1z^{3\cdot 3} + \cdots + 1z^{3(j-1)} = 1 + (z^3)^1 + \cdots + (z^3)^{j-1},$$
$$(z - 1)^3 R(z) \equiv (z^3 - 1)\Big\{1 + (z^3)^1 + (z^3)^2 + \cdots + (z^3)^{j-1}\Big\} = (z^3)^j - 1 = z^{3j} - 1.$$

故に 3 の倍数である $T = 3j,\ j = 1, 2, 3, \cdots$ はすべて, 恒等式 (12) を確かに満たす. ■

問題 B.3.(1) 初期条件 $x_0 = 1, x_1 = -1 \equiv 2, x_2 = 1, x_3 = -1 \equiv 2 \pmod 3$ を取る. 線形漸化式 (B3) の解系列が未知, 従って周期 T と $R(z)$ が不明であっても, 出発 4 連から

$$Q(z) = x_0 + (x_1 - x_0)z + (x_2 - x_1)z^2 + (x_3 - x_2 - x_0)z^3 \equiv 1 + z - z^2$$

であり, (B7) の恒等式が次の形になる事はわかる:

$$(z-1)^4 R(z) = (1 - z^T)(1 + z - z^2) \pmod 3. \qquad \text{(B10)}$$

法 3 で $z - 1$ は $1 + z - z^2 \equiv 2z^2 - 2z + 1$ を割り切らない (因数定理). だから (B10) 左辺の

$$(z-1)^4 = z^4 - 4z^3 + 6z^2 - 4z + 1 \equiv z^4 - z^3 - z + 1 \pmod 3$$

は法 3 で $1 - z^T$ を割り切る, T はそういう正の整数で

$$z^T \equiv 1 \pmod{p, f_1(z)}, \quad p = 3,\ f_1(z) = \frac{-f(z)}{\mathrm{GCD}(f(z), Q(z))} = -f(z)$$

が成り立たなければならない. $T = 4, 5, \cdots$ として試してもよいが, 有限体での多項式の根を含む数の計算と同様な $f_1(z) = -z^4 + 4z^3 - 6z^2 + 4z - 1 \equiv -z^4 + z^3 + z - 1 \equiv 0$ の規則で見た z の冪乗計算なのだから,

$$z^4 \equiv z^3 + z - 1$$

の規則で z^4 を 3 次以下の $z^3 + z - 1$ にいつも置き換えて $z^5, z^6, z^7, \cdots$ を計算し, 初めて $z^T \equiv 1$ になる T を求めてもよい. これを行い, 正で最小の T を求めなさい.

(解) $z^5 = z \cdot z^4 = z(z^3 + z - 1) = z^4 + z^2 - z = (z^3 + z - 1) + z^2 - z = z^3 + z^2 - 1,$

$z^6 = (z^3 + z - 1) + z^3 - z \equiv -z^3 - 1,$

$z^7 = -(z^3 + z - 1) - z = -z^3 + z + 1,$

$z^8 = -(z^3 + z - 1) + z^2 + z = -z^3 + z^2 + 1,$

$z^9 = -(z^3 + z - 1) + z^3 + z = 1.$

故に正で最小の T は 9 である. **(問題 B.3.(1) 終り)**

問題 B.3.(2) 上の問 (1) で求めた T は我々の提示した議論では周期の必要条件を満たしているに過ぎないが, この計算結果の T の正の最小値が必ず線形漸化式 (B3) の解の周期である事は示される.[107] 実際に初期条件 $x_0 = 1, x_1 = -1 \equiv 2, x_2 = 1, x_3 = -1 \equiv 2 \pmod 3$ から解系列を計算し, 周期が (1) で求めた正最小の T で与えられることを確認しなさい.

(証明)

k	0	1	2	3	4	5	6	7	8	9	10	11	12
x_k	1	−1	1	−1	0	−1	0	1	0	1	−1	1	−1

確かに周期 $T = 9$ である. ■

[107] 一般に任意の整数 $m > 0$ を取り, 特性多項式 $f(z)$ から初期条件で定まる $Q(z)$ との法 m での共通因数を除いた $f_1(z) = -f(z)/\{\mathrm{GCD}(f(z), Q(z))\}$ も法として, $z^T \equiv 1 \pmod{m, f_1(z)}$ となる最小の $T > 0$ が法 m での (B3) の解の周期である. 十分性も含めた証明はさらに幾つかの準備を要するので pp.118-126 の法 $m = p^r$ での一般の議論を参照.

付録C. 整数行列の単因子

C1. 行列の基本変形

行列の行或いは列の交換はその行列に別の行列を掛けることによって実現できる. 3×3 行列

$$S_{23}:=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix},\qquad A=\begin{pmatrix}a&b&c\\d&e&f\\g&h&i\end{pmatrix},$$

を考える. S_{23} を A に掛ける効果は次の計算で知られる:

$$S_{23}A=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}\begin{pmatrix}a&b&c\\d&e&f\\g&h&i\end{pmatrix}=\begin{pmatrix}a&b&c\\g&h&i\\d&e&f\end{pmatrix},$$

$$AS_{23}=\begin{pmatrix}a&b&c\\d&e&f\\g&h&i\end{pmatrix}\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}=\begin{pmatrix}a&c&b\\d&f&e\\g&i&h\end{pmatrix}.$$

一般に $n\times n$ 行列 $S_{kl}=S_{lk}$ ($k\neq l$) は $n\times n$ 単位行列 E で第 k 行と第 l 行 (第 k 列と第 l 列でもよい) を交換したものとする. 上の 3×3 行列の結果から, 任意の $n\times n$ 行列 A に対する S_{kl} の行列積の効果の記述として次が成り立つ事は明らかである:

$S_{kl}A$ は行列 A の第 k 行と第 l 行を交換した行列であり,

行列 AS_{kl} は行列 A の第 k 列と第 l 列を交換した行列であって,

行列式 $|S_{kl}|$ は $|E|$ の 2 行, 或いは 2 列を交換した行列式で -1 である.

行列 $T_2(\alpha):=\begin{pmatrix}1&0&0\\0&\alpha&0\\0&0&1\end{pmatrix}$ と $A=\begin{pmatrix}a&b&c\\d&e&f\\g&h&i\end{pmatrix}$ の次の積も計算をしよう:

$$T_2(\alpha)A=\begin{pmatrix}1&0&0\\0&\alpha&0\\0&0&1\end{pmatrix}\begin{pmatrix}a&b&c\\d&e&f\\g&h&i\end{pmatrix}=\begin{pmatrix}a&b&c\\\alpha d&\alpha e&\alpha f\\g&h&i\end{pmatrix},$$

$$AT_2(\alpha)=\begin{pmatrix}a&b&c\\d&e&f\\g&h&i\end{pmatrix}\begin{pmatrix}1&0&0\\0&\alpha&0\\0&0&1\end{pmatrix}=\begin{pmatrix}a&\alpha b&c\\d&\alpha e&f\\g&\alpha h&i\end{pmatrix}.$$

一般に $n\times n$ 単位行列 E の第 k 対角成分を α とした $T_k(\alpha)$ を $n\times n$ 行列 A に作用すると,

行列 $T_k(\alpha)A$ は行列 A の第 k 行を α 倍した行列であり,

行列 $AT_k(\alpha)$ は行列 A の第 k 列 α 倍した行列であって,

行列式 $|T_k(\alpha)|=\alpha$ である.

行列のある列を ξ 倍して他の列に加える操作も 3×3 行列の例で考えよう. 行列 $U_{13}(\xi)$

$:= \begin{pmatrix} 1 & 0 & \xi \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $U_{31}(\,\xi\,) := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \xi & 0 & 1 \end{pmatrix} = {}^tU_{13}(\,\xi\,)$ と $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ の積は:

$$AU_{13}(\,\xi\,) = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} 1 & 0 & \xi \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b & a\,\xi + c \\ d & e & d\,\xi + f \\ g & h & g\,\xi + i \end{pmatrix},$$

$$U_{31}(\,\xi\,)A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \xi & 0 & 1 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ g + \xi a & h + \xi b & i + \xi c \end{pmatrix}.$$

一般に行列 $U_{kl}(\,\xi\,)$ $(\,k \neq l\,)$ は $n \times n$ 単位行列 E の非対角成分である第 $(\,k, l\,)$ 成分 **0** を ξ に置き換えたものとする. $n \times n$ 行列 A との積について, 次が成り立つ:

行列 $AU_{kl}(\,\xi\,)$ は A の第 k 列の ξ 倍を第 l 列に加えた行列,

行列 $U_{lk}(\,\xi\,)A$ は A の第 k 行の ξ 倍を第 l 行に加えた行列で,

行列式 $|U_{kl}(\,\xi\,)| = |U_{lk}(\,\xi\,)| = 1$ である.

まとめると, 1 つの $n \times n$ 行列 A の「行基本変形」は

(a) 2 つの行 k, l を交換する事は正則行列 S_{kl} で $S_{kl}A$ を作って,

(b) k 行を定数 $\alpha \neq 0$ 倍する事は正則行列 $T_k(\alpha)$ で $T_k(\alpha)A$ を作って,

(c) k 行の定数 ξ 倍を l 行に加える事は $U_{lk}(\xi)A$ で,

それぞれ実現される. 行列 A の列の基本変形についも同様で:

(a) k, l 列を交換する事は正則行列 S_{kl} で AS_{kl} を作って,

(b) k 列を定数 $\alpha \neq 0$ 倍する事は正則行列 $T_k(\alpha)$ で $AT_k(\alpha)$ を作って,

(c) k 列の定数 ξ 倍を l 列に加える事は $AU_{kl}(\xi)$ で

それぞれ実現される.

行の基本変形の繰り返しは行列 A の左に次々に正則行列を掛けて実現されるから全体結果はある正則行列 X との積 XA $(|X| \neq 0)$ である. 同様に列の基本変形の繰り返しは行列 A の右に次々に正則行列を掛ける事で, やはり結果はある正則行列 Y との積 AY $(|Y| \neq 0)$ と等価である. この簡明な結論から次の構造がわかる:

(1) 行の相続く基本変形とその逆順とは一般に結果が異なる: $XX'A \neq X'XA$.

(2) 相続く列変形についても同様である.

(3) しかし行変形と列変形とは可換である: $(XA)Y = X(AY)$(結合法則).

C2. 整数基本変形による整数行列の対角化

実数或いは複素数成分の行列の基本変形を考えよう. 上の通り基本変形は行列 A に「正則行列」を掛けて実現され, 逆行列を掛けて必ず元へ戻す事ができる. 勿論この「可逆性」は基本変形操作を直接それぞれ考えても明らかではある. この場合行や列の基本変形で行

列を上 3 角形或いは対角形にできる事は連立 1 次方程式のガウスの消去法を想起すれば明らかである. 基本変形は行や列ベクトルの独立性を変えないので, この対角変形によって行列のランクは容易に得られた.

伏見-手塚の定理は $\boldsymbol{Z}_p$ 整数行列のランク計算を求めた. $\boldsymbol{Z}_p$ は体でその 0 ではない数はすべて逆数を持つから, 実数上と同様に消去法の手続きは遂行可能で, 基本変形による対角化がこの目的に大変有用であることも経験された.

この実用を少し離れて, ここでは「法 p を取らない単なる整数基本変形のうち, 同様な整数基本変形で元へ戻せるものだけを用いて行列を対角化できるか」という問題を考える. 答えは「可能」であり, 興味はその対角形の特徴付けにある. 基本変形のうち行, 列の交換は繰り返しによって数体系によらず自明に元へ戻せる. ある行の整数 ξ 倍を他の行に加えることも同じ行の $-\xi$ 倍を他の同じ行に加える事で相殺できて同様である. ただある行或いは列の α 倍は, これを整数 (の加減乗法) だけを用いた基本操作で元へ戻す事は $\alpha = \pm 1$ の場合しか可能ではない. だからここで扱う問題は

(a) 行或いは列の交換

(b') 行或いは列の符号を変える

(c') 行 (或いは列) の任意整数倍を他の行 (或いは列) に加える

だけで行列を対角化できるか, そしてその対角形はどのようになるか, である. 次の定理が結論を与え, その証明は実際に整数行列の対角化を行う具体的な手続きを明示している:

定理 C.1. 整数成分の行列 A は, 整数の範囲で可逆な基本変形 XAY で[108]対角形

$$XAY = \begin{pmatrix} a_1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & a_2 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & a_3 & \cdots & 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & a_r & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad 0 \leqq a_1 \leqq a_2 \leqq \cdots \leqq a_r,$$

に変形される. ここで $r = \mathrm{rank} A$ は行列 A のランクであり, 0 でない対角成分はすべて正の整数で整除関係 $a_1 \,|\, a_2$, $a_2 \,|\, a_3$, $\cdots$, $a_{r-1} \,|\, a_r$ が成り立つ. 因子 $a_1, a_2, \cdots, a_r$ は行列 A の単因子 proper divisor と呼ばれる.

(証明) 行列 $A = (\, a_{ij}\,)$ の整数成分で 0 でないものの絶対値最小のものは必ずあるから, それを含む行或いは列を ± 1 倍してプラスに変え, 行や列の第 1 行, 第 1 列との交換で $(1,1)$ 成分に持ってきて a_{11} とする. もし第 1 列が 0 ばかりではないなら, この a_{11} で第 1 列の数 a_{21}, $a_{31}, \cdots, a_{n1}$ を整数の範囲で割り算して余りを ${a_{21}}', {a_{31}}', \cdots, {a_{n1}}'$ と置く. 割り算の等式から

[108]正則行列 X とその逆行列 X^{-1} とは $XX^{-1} = E$ を満たし, $|XX^{-1}| = |X||X^{-1}| = 1$ となるのだから $|X^{-1}| = 1/|X|$ でなければならない. 故に X^{-1} が整数行列であるためには $|X| = \pm 1$ である事が必要である. $|X| = \pm 1$ が整数行列 X の整数成分逆行列 X^{-1} の存在のために十分でもある事は公式 $X^{-1} = (\text{余因子}/|X|)$ から明らか. 行列式 $|X| = \pm 1$ の行列はユニモジュラーと呼ばれる. ここでの問題は整数成分のユニモジュラー行列 X, Y による整数成分行列 A の変形 XAY で得られる標準形は何か, という事になる.

$$a_{i1} = a_{11}q + a_{i1}',\ \ q \text{は商},\ \ 0 \leqq a_{i1}' < a_{11},$$

だから, 第 1 行の整数 q 倍を第 i 行から引く基本変形を第 2–n 行のすべてに行う. 新しい第 1 列は「a_{11} 以外皆 0」か, 或いは 0 でないものがあってもそれらは皆正で必ず a_{11} より小さくなる. この変形の上で全く同様な列の基本変形を行い, 第 1 行成分をすべて a_{11} で割り算した余り, a_{11} 以外すべて 0 か或いは a_{11} より小さい正の数か, にする. この後再び行列全体を見渡す. a_{11} より小さい最小絶対値の成分があれば,[109] それをはじめの様に正に変えて $(1,1)$ へ移送し, 再度第 1 列, 第 1 行を新しい小さい a_{11} で割った余りに変える. この操作は a_{11} を毎回必ず 1 以上減らし, 第 1 列と第 1 行が a_{11} 以外すべて 0 でなければ続くから, 必ず有限回で a_{11} 以外の第 1 列, 第 1 行成分は 0 になって終る. 結果は次の形である:

$$A = \begin{pmatrix} a_1 & 0 & 0 & \cdots & 0 \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} \\ 0 & a_{32} & a_{33} & \cdots & a_{3n} \\ \cdots & \cdots & \cdots & \cdots & \\ 0 & a_{n2} & a_{n3} & \cdots & a_{nn} \end{pmatrix}. \tag{C1}$$

仮にここで第 2 行, 第 2 列以下に 0 ではなくしかも a_1 で割り切れないものが残っていて, 例えばそれが a_{ij} だとすると $a_{ij} = a_1 q + r,\ \ 0 < r < a_1$ と置く事ができるから, 第 1 行に q を掛けて第 i 行に加え, それで作られた第 1 列を第 j 列から引いて, $a_{ij}' = r$ と変えられる. 再びこの r を $(1,1)$ 成分に移してさらに a_1 を 1 以上小さくできる. だからこれも必ず有限回の後に a_1 が残るすべての行列成分を割り切る様になって終る. この後は残る第 2 行第 2 列以下の中の絶対値最小の成分を $(2,2)$ へ移して同じ手続きを繰り返せばよい. すべて a_1 で割り切れるものの加減乗法で作っていくのだから, 以後のどのような操作を経てもこの第 2 行以下, 第 2 列以下の成分は a_1 の倍数であり続ける. ■

構造や概念の重要性は措いて $\boldsymbol{Z}_p$ でのランク計算の実際から言うと始めから法 p で考える方が大きい整数が出ず計算は楽だが, 議論を消化するためにも次の例を上の証明方法で対角化して text の問題 6.10. と比べよう.

問題 C.2. $\boldsymbol{Z}$ 上の行列 $B = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & -2 & 3 & 5 \\ 1 & 3 & -1 & 2 \\ 2 & -2 & 1 & -1 \end{pmatrix}$ の単因子を求めなさい.

(解) 行や列の ± 1 倍, 符号変化, しか使わない事に注意して整数で基本変形すればよい:

$$B \to \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & -2 & 3 & 5 \\ 0 & 2 & -2 & 2 \\ 0 & -4 & -1 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 3 & -2 \\ 0 & 2 & -2 & 2 \\ 0 & -1 & -1 & -4 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & -4 \\ 0 & 2 & -2 & 2 \\ 0 & 5 & 3 & -2 \end{pmatrix}$$

$$\to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & -4 \\ 0 & 0 & -4 & -6 \\ 0 & 0 & -2 & -22 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & -4 \\ 0 & 0 & -2 & -22 \\ 0 & 0 & -4 & -6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & -4 \\ 0 & 0 & -2 & -22 \\ 0 & 0 & 0 & 38 \end{pmatrix}$$

[109] 第 1 行或いは第 1 列に a_{11} 以外に 0 ではないものが残っている限り, これは必ず存在する.

$$\to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 38 \end{pmatrix}.$$

この結果は問題 6.10. と本質的に同じである. また基本変形は XBY ともとの行列 B に左右から行列式 ± 1 の行列 X, Y を掛けて実現されるのだから, 結果の対角行列式 $2 \times 38 = 76 = \pm|B|$ であり, 実際 $|B| = -76$ である事は容易に見られる. **(問題 C.2. 終り)**

もっと一般化して言えば, 単因子を求める変形でもとの行列式の絶対値が変わらないのと同様に, もとの行列の k 次の 0 ではない任意の小行列式の最大公約数は変わらない. 実際,

(a) 行や列の交換は各小行列式を ± 1 倍するだけ,

(b) 行や列の $\alpha = \pm 1$ 倍も同じ

であり, 小行列式全体の最大公約数 g_k は変らない. 残る基本操作 (c), ある行或いは列の ξ 倍を他の行或いは列に加える, は一般に個々の小行列式を変えるが, その変え方は k 次の小行列式をそれと他の k 次の小行列式の整数倍との和或いは差に置き換えるだけのものだから, (c) 操作後の k 次小行列式の全体の最大公約数 $g_k{}'$ はもとの小行列式全体の最大公約数 g_k で割り切れる. これらの操作の逆を考えれば同じ理由で g_k も $g_k{}'$ で割り切れて $g_k{}' = g_k$ でなければならない.

この様に k 次小行列式の全体の最大公約数 g_k は単因子に分解された行列の $g_k{}'$ に等しい. これは a_1 から順に見て次を意味する:

定理 C.3. 整数行列 A の単因子 $a_1, a_2, \cdots, a_r > 0$ は関係

$$k \text{ 次小行列式の最大公約数 } g_k = a_1 a_2 \cdots a_k \quad (\, k \leqq r \,)$$

を満たして a_1 から $a_2, a_3, \cdots$ の順に一通りに定まる. 故にこれら単因子は一意である.[110]

整数行列の単因子の考え方は様々に, 特に任意の主イデアル整域の元を成分とする行列, 例えば体を係数とする文字 z の式を成分とする行列, の可逆行列による対角化, に一般化され, 一般化それぞれに応じて様々な応用を持つ. 我々の興味で言うと, 有限アーベル群を一般にした「有限生成アーベル群」の構造は単因子を考えて深く見通される. これについては例えば, 近藤 [20], 但し単因子を使わない議論としては酒井 [63], 等を参照.

[110] 整数行列 X の任意の行或いは列の成分の最大公約数は行列式 $|X|$ の因数になる. だから X がユニモジュラーならそのすべての行, 列の成分は互いに素で最大公約数は 1 でなければならない. $\alpha = \pm 1$ の $T_k(\alpha)$ も含めて, 整数上の可逆な基本変形は皆この様なユニモジュラー行列で実現され, この構造による変形が A のすべての小行列式の最大公約数を保存するのだと考えてもよい. ファンデルヴェルデン / 銀林浩訳「現代代数学 3」(東京図書) pp.147-158, 高木貞治「(改訂) 代数学講義」(岩波書店) pp.405–407 を参照.

関連図書

[1] 津田孝夫: 「モンテカルロ法とシミュレーション」 (培風館, 1969).

[2] D. E. Knuth / 渋谷政昭訳: *The Art of Computer Programming* Vol.II, 第 3 分冊 「準数値算法 / 乱数」 (サイエンス社, 1981; 原著第 2 版 1981).

[3] 宮武修, 脇本和昌: 「乱数とモンテカルロ法」(森北出版, 1978).

[4] 伏見正則: 「乱数」 (東大出版会, 1989).

[5] 例えば A. M. Ferrenberg, D. P. Landau and Y. J. Wong: ”Monte Carlo simulations: Hidden errors from ’good’ random number generators” Physical Review Letters **69** (1992), 3382–3384. これは G. Marsaglia and A. Zaman: ”A new class of random number generators” Annals of Applied Probability **1** (1991), 462–480 による乱数方式に関するものでその構造解析は手塚集: 京都大学数理解析研究所「確率数値解析における諸問題」研究集会 (1993 年 6 月) で与えられた. M. Lüscher[13] による別の発展も参照.

[6] Birger Jansson: *Random Number Generators* (Victor Pettersons, 1966).

[7] N. Koblitz: *A Course in Number Theory and Cryptography* (Springer, 初版 1987, 第 2 版 1994).

[8] 辻井重男, 笠原正雄: 「暗号と情報セキュリティ」 (昭晃堂, 1990).

[9] 岡本龍明, 山本博資: 「現代暗号」 (産業図書, 1997).

[10] R. Tausworthe: ”Random numbers generated by linear recurrence modulo two” Mathematics of Computation **19** (1965), 201–209.

[11] T. G. Lewis and W. H. Payne: ”Generalized feedback shift register pseudorandom number algorithms” Journal of the ACM **20** (1973), 456–468.

[12] M. Fushimi and S. Tezuka: ”The k-distribution of generalized feedback shift register pseudorandom numbers” Communications of the ACM **26** (1983), 516–523.

[13] M. Lüscher: ”A portable high-quality random number generator for lattice field theory simulations” Computer Physics Communications **79** (1994), 100–110.

[14] G. Marsaglia and L-H. Tsay: ”Matrices and the structures of random number sequences” Linear Algebra and its Applications **67** (1985), 147–156.

[15] S. C. Phatak and S. Suresh Rao: ”Logistic map: A possible random-number generator” Physical Review **E51** (1995), 3670–3678.

[16] 秋月康夫, 鈴木通夫: 「高等代数学 I」 (岩波, 1952).

[17] 山崎圭次郎: 「環と加群 I」 (岩波講座基礎数学, 1976).

[18] 渡辺敬一, 草場公邦: 「代数の世界」 (朝倉書店すうがくぶっくす **13**, 1994).

[19] 芹沢正三: 「C による初等整数論」 (森北出版, 1993).

[20] 近藤武: 「群論 I」 (岩波講座基礎数学, 1987).

[21] 銀林浩: 「初等整数論入門」 (国土社, 1966).

[22] S. L. Anderson: ”Random number generators on vector super computers and other advanced architectures” SIAM Review **32** (1990), 221–251.

[23] 中澤宏, 中澤直也: 「乱数生成の構造 I. 巡回群と乗算合同法」詫間電波高等専門学校研究紀要第 23 号 (1995), 25–36.

[24] S. K. Park and K. W. Miller: ”Good random number generators are hard to find” Communications of the ACM **31** (1988), 1192.

[25] G. Marsaglia: ”Random numbers fall mainly in the planes” Proceeding of the National Academy of Sciences of the U. S. A. **61** (1968), 25–28.

[26] U. Dieter: ”How to calculate shortest vectors in a lattice” Mathematics of Computation **29** (1975), 827–833.

[27] R. R. Coveyou and R. D. McPherson: ”Fourier analysis of uniform random number generators” Journal of the ACM **14** (1967), 100–119.

[28] W. A. Beyer, R. B. Roof and D. Williamson: ”The lattice structure of multiplicative congruential pseudo-random vectors” Mathematics of Computation **25** (1971), 345–363.

[29] G. S. Fishman and L. R. Moore: ”An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{31} - 1$” SIAM Journal on Scientific and Statistical Computing **7** (1986), 24–45; 素数の法 $m = 2^{31} - 1 = 2147483647$ の乗算合同法の場合のすべての原始根乗数のスペクトル検定結果の報告である.

[30] G. S. Fishman: ”Multiplicative congruential random number generators with modulus 2^{β}: An exhaustive analysis for $\beta = 32$ and a partial analysis for $\beta = 48$” Mathematics of Computation **54** (1990), 331–344. これは法 2^{32} の乗算合同法のすべ

ての最長周期乗数と, 法 2^{48} の場合の (約 3.51×10^{11} 個の最長周期乗数のすべては計算的に無理なのでそのうちの)67.1×10^{6} 個の乗数についての調査報告である.

[31] J. W. S. Cassels: *An Introduction to the Geometry of Numbers* (Springer, 1959); この pp.332–333, pp.6–7 そして pp.33–34.

[32] 杉山昌平: 「差分 · 微分方程式」 (共立出版, 1971).

[33] 笠原皓司: 「新微分方程式対話」 (現代数学社, 1970).

[34] 松阪和夫: 「線型代数入門」 (岩波書店, 1980).

[35] ファンデルヴェルデン / 銀林浩訳: 「現代代数学 1」 (東京図書, 1959).

[36] N. Zierler: ”Linear recurring sequences” Journal of the Society for Industrial and Applied Mathematics **7** (1959), 31–48.

[37] バーコフ, バーティー / 一松信, 睦子訳: 「現代応用代数 II」(新曜社, 原著 1970).

[38] 宮川洋, 岩垂好裕, 今井秀樹: 「符号理論」 (昭晃堂コンピュータ基礎講座 18, 1973).

[39] 奥川光太郎: 「応用抽象代数学」 (コロナ社, 1974).

[40] S. W. Golomb: *Shift Register Sequences* (Holden-Day, 1967).

[41] N. Zierler: ”On the theorem of Gleason and Marsh” Proceedings of the American Mathematical Society **9** (1959), 236–237.

[42] R. R. Varshamov: ”A general method of synthesizing irreducible polynomials over Galois fields” Soviet Mathematics Doklady **29** (1984), 334–336.

[43] V. Shoup: ”New algorithms for finding irreducible polynomials over finite fields” Mathematics of Computation **54** (1990), 435–447.

[44] M. Matsumoto and T. Nishimura: ”Mersenne Twister: A 623-dimensionally Equidistributed Uniform Pseudorandom Number Generator” ACM Transactions on Modelling and Computer Simulation **4** (1994), 254–266.

[45] 中澤宏: 「連結M系列乱数の「2 次均等分布元」次元について」 詫間電波高専研究紀要第 24 号 (1996), 31–36.

[46] 伏見正則: 「M 系列に基づく乱数発生法に関する相反定理とその応用」 情報処理学会論文 誌 **24** (1983), 576–579.

[47] J. P. Tootill, W. D. Robinson and A. G. Adams: ”The runs up-and-down performance of Tausworthe pseudo-random number generators” Journal of the ACM **18** (1971), 381-399.

[48] H. S. Bright and R. L. Enison: ”Quasi-random number sequences from a long-period generator with remarks on application to cryptography” Computing Surveys (the Survey and Tutorial Journal of the ACM) **11** (1979), 357–370.

[49] M. Ward: ”The arithmetical theory of linear recurring series” Transactions of the American Mathematical Society **35** (1933), 600–628.

[50] R. P. Brent: ”On the periods of generalized Fibonacci recurrences” Mathematics of Computation **63** (1994), 389–401.

[51] 上野健爾: 「代数入門 2」 (岩波講座現代数学への入門, 1996).

[52] D. E. Knuth: *The Art of Computer Programming* Vol.II, *Seminumerical Algorithms*, **3rd Edition** (Addison-Wesley, 1997).

[53] 松本眞:「コイン投げで一儲けする方法ー擬似乱数研究の現状ー」 情報処理 **39** (1998), 1166–1170.

[54] D. E. Knuth / 中川圭介訳: *The Art of Computer Programming* Vol.II, 第 4 分冊 「準数値算法 / 算術演算」(サイエンス社, 1986; 原著第 2 版 1981).

[55] S. Tezuka: *Uniform Random Numbers: Theory and Practice* (Kluwer Academic Publishers, 1995).

[56] R. Lidl and H. Niederreiter: *Finite Fields* (Addison-Wesley, 1983).

[57] P. L’Ecuyer: ”Random numbers for simulation” Communications of the ACM **33** (1990), 85–97.

[58] H. Niederreiter: ”Recent trends in random number and random vector generation” Annals of Operations Research **31** (1991), 323–346.

[59] 古屋茂: 「行列と行列式」(培風館, 1957).

[60] 佐武一郎: 「線形代数学」(裳華房, 1974).

[61] 笠原皓司: 「教養課程線形代数学」(サイエンス社, 1982).

[62] 中澤宏: 「Tausworthe と Lewis-Payne の連結 M 系列乱数の均等分布性」環瀬戸内応用数理研究集会 (2001 年 6 月 9 日, 愛媛大学) / 詫間電波高等専門学校研究紀要第 29 号 (2001), to appear.

[63] 酒井孝一: 「代数学談話室 (大学院への数学–加群の理論とその応用)」(現代数学社, 1974).