コンピュータ上の
優れた乱数とは何か

中澤 直也[1] / 中澤 宏[1]

(2022年7月-2024年8月24日)

(開示: 第4章まで)

[1]© 枚方乱数工房 / Hirakata Ransū Factory (HRF) / 573-0081 枚方市釈尊寺町 28-18-103

まえおき

伊藤清先生は晩年京都大学数理解析研究所の所長を勤められました。彼は周りの, どうも理解の速くない我々物理学徒や学生諸君に、大本の確率論、確率過程論、確率微分方程式やいわゆる Ito Cacukulus に直感的理解を得るように、と力を注がれました。中澤 宏 (HN) はある講義での先生の言葉を時折思い出します:

> …… 数学はどんな方程式でも扱う事はできます。けれど最も深くて最も多産な方程式は物理工学問題から生じるようです。だから数学は物理に興味を惹かれるのです ……

なにしろ 40 数年前の事柄ですから、HN の記憶も定かではなく、伊藤先生の言葉を正確に伝えているか、彼が単に物理の学生を元気付けようとされていたのか、も知れませんが、HN には彼の叡知経験からの深い言葉を口にされたと思われてなりません。我々は皆 Sir Isaac Newton が微積分を発見し、微分方程式を創始して物体の運動から天体の運行まで理解を開き、西欧の産業革命の道を啓いたこと、輝かしい物理の展開、を知っているのですから …。

乱数はコインの裏表も、サイコロの目も、カードも、古くから人類と共にありましたし、数学でも確率的な現象として多くの数学者の興味を惹いていた事でしょう。しかし現代的な乱数への興味はやはり、60 年余り前のコンピュータの利用の始まりによる、速い多量の生成に伴われる若い分野と思われます。HN は 1990 頃、国立高等専門学校の場で 20 歳位の学生諸君に乱数の諸理論を伝える必要に迫られました。当然彼は D. E. Knuth 先生の浩瀚な書物に懸命に分け入り、コンピュータ上の乱数は厳しい条件、『再現可能性と移転可能性』を満たさなければならない事を学びました。これらの条件は高度に発達した確率論、確率過程論とは相容れない、むしろ初等整数論に近いものです。再現可能性とは、乱数列の生成は与えられた初期乱数からは一意に、どんなに長い生成を続けても全桁変りのない乱数を与えなければならない、という事です。コンピュータ上で現象のシミュレーションを行うプログラムは複雑な構造を持つでしょうから、そのデバッグを進めるにはプログラムの変更がどの様な効果を持つか、『同一の乱数列の上で』変化を見得る様望まれるし、計算機種や計算言語を変えても同一の結果が与えられる必要があるからです。これらの要求は殆ど一意に『整数演算』の世界にプログラムを限定し、現在の確率論、確率過程論、巨人 Kolmogorov 教授の与えた『筒集合上の確率測度』や天才 Wiener 教授の名を冠した過程で議論される世界からは遠くにあります。

Knuth 教授が著された教科書も勿論この制限の結果でしょうし、それは伊藤先生の『予言』に沿うものでしょう。現在のこの本から読者が整数の精細な構

造への議論の限定方法と、孫子の定理の力とへの御理解を深められれば、それは著者達の喜びです。この理解は HN と中澤直也 NN 自身も長い苦闘の末得る事ができたものです。1990 年頃に HN が学び、厚顔にも教科書に編んだ当時の乱数諸理論は、枚方乱数工房 (Hirakata Ransu Laboratory HRF) の archive

http://www10.plala.or.jp/h-nkzw/indexarchivenew.html

に”rans1203.pdf”のファイル名で載せられています。2000 年当時の乱数諸理論を一瞥なさる事もできるでしょう。

学んだ事を学生諸君に伝える形でも学生諸君の受容は悪くはなく、HN 自身も次第に興味を深めましたが、定年退職となりました。その後の幸いは 3 つありました。第一は工科系の学校でコンピュータの使用に親しみ、例えば正方形の上に相続く乱数の 2 連 $(V_k.V_{k+1})$ を時系列の点として取って、乱数の分布の相関の発生を認識するソフトウエアを容易に使用できる様になりました。現在ではありふれた技術でしょうが、これが例えば法が奇素数と 2 の冪の積である乗算合同法乱数はきつい相関を持ち、相続く出力乱数が『独立性』を持つとはいえない事、を明確に視覚的に示します。結果の影響は広大で、乗算合同法乱数は互いに素な奇素数を部分法に持つ生成機構に限られる、だから $d = 10^n$ の様な法を取ってはいけない、という一般的教訓を与えます。この様な視覚的な認識はその後も検定方法の推進に大きな力となりました。

第 2 の幸運は中澤直也 (NN) の HRF での研究への参加を得た事です。彼は応用数論を研究し、学位を得、HRF で乱数問題に興味を抱きました。それは丁度 HRF で『近似定理』、つまり再現可能で移転可能なすべての乱数生成機構は乗算合同 (multiplicative congruential, MC) 法で近似てきる、という広範な構造定理が得られた時期でした。それから暫く、NN と HN の 2 人は『良い性能と見える 2 つの部分法 d_1 と d_2 の積 $d = d_1 d_2$ を法とする MC 法でどうしても良い一様独立と見える MC 生成機構を発見できない、という直感に反する難問に苦しみました。それは乱数生成機構が『高い性能である』と判断する『検定基準』の再検討に HRF を向わせ、MC 乱数の相続く出力 l 連が形成する『l 次元格子の作る単体はを正単体を単位胞とする l 次元正格子』を基準に取るべきだ、という認識を与えました。これは第 3 の幸運、HRF が誇る『正単体基準』の発見で、これに基づいて HRF は、長い検定の末に、#001 を 2018 年、#003 を 2020 年、2 つの優れた MC 乱数生成機構を『2 つの異なる奇素数の積を法として』発見する事ができました。これらは我々が導入した新しい検定基準で初めて発見する事ができた合格乱数生成機構で、さらに中澤直也が新しく見出した孫氏の定理の魔術的な力による生成で、2^{52} にも及ぶ長大な周期を高速に生成します。すべての意味で一頭地を現在遥かに抜く一様独立乱数生成機構として、HRF が喜びと共に、その構成と検定合格の詳細等を詳しく述べます。

現在つくづく思うのですが、古くからの乱数は大変難しい問題を提示してい

ました。むしろ『何が問題なのか分らなかった』と言うべきでしょうか。問題に参加してから 30 年以上経っているのですから HN に誇るべき所は何もありません。成功はそれまで専門とされる多くの人々が辛苦を払われたその数多くの不成功の消去法で漸く得られたものです。今まで携わってこられた方々に HRF は深い敬意を表します。そして HRF までの長い年月を支えて下さったすべての方々に心から感謝します。特に故伊藤清先生、故飛田武幸先生、渡辺新三先生そして John R. Klauder 先生、last but not least ですが、我々の深い謝辞を捧げたいと思います。 **（2019 年 5 月-2024 年 7 月）**

目次

第 1 章　基本的な諸概念と用語

1. 1. 見本過程としてのコンピュータ上の乱数

確率過程論はランダムな関数、典型的には連続な関数の集合の上に確率測度の概念を与える事から始まります。『確率』を与えるべき対象は典型的には連続な関数の集まりです。これは難しいテーマです。一般論なら対象はいろんな場合に応じて様々に姿を変える変化過程であり、その様な変化の数限りない場合の集まり、とても一筋縄では捉えられません。勿論『確率過程論』では『時間と共に変る関数の集まりを取る事、それら集まりに確率を与える事、と概念的に隙間なく出来上がっています。これは大コルモゴロフの偉業です。我々差し当っての手には負えません。離散的な (乱) 数の離散的な 1 本の列、とだけ考えて済む事柄に限って難を避けます。それは『離散確率過程の 1 つの見本過程 sample process』の考察です。さいころと投げ方とにインチキはないか、という問題は少し一般化して、『コンピュータ上に与えられる乱数は独立乱数系列の見本と見てよいか』とします。これより難しい事は必要ありませんがこれだけでも難しい！

数の神様（女神様かも知れません）は思いがけないプレゼントを我々に用意してくれていました。我々は漸く 21 世紀にもなってそれに気付きましたが。ごく特殊だが考え易い（そして実は最も一般的な）『離散一様乱数列』、長さ T の数の列、

$$\{u_0, u_1, u_2, \cdots, u_{T-1} |\quad 0 \leq u_k \leq 1, \quad 0 \leq k \leq T-1\}$$

で考えます。

命題 1. コンピュータ上の乱数系列の相続く 2 連 (u_k, u_{k+1}) の独立性は、統計的仮説として、これらの 2 次元平面の点としての 1 周期に亙るプロットが、平面で**方向性を持たない分布**を持てば最も弱く否定される。　　**（命題１終り）**

実例は話を早くします。次頁の第 1 図左は周期はたった $T = 250$ ですが、かなり独立に近い乱数列の相続く 2 連をプロットしたものです。右は少し後に説明する乗算合同法の 2 連の点の図で、左図を近似するもの[2]です。

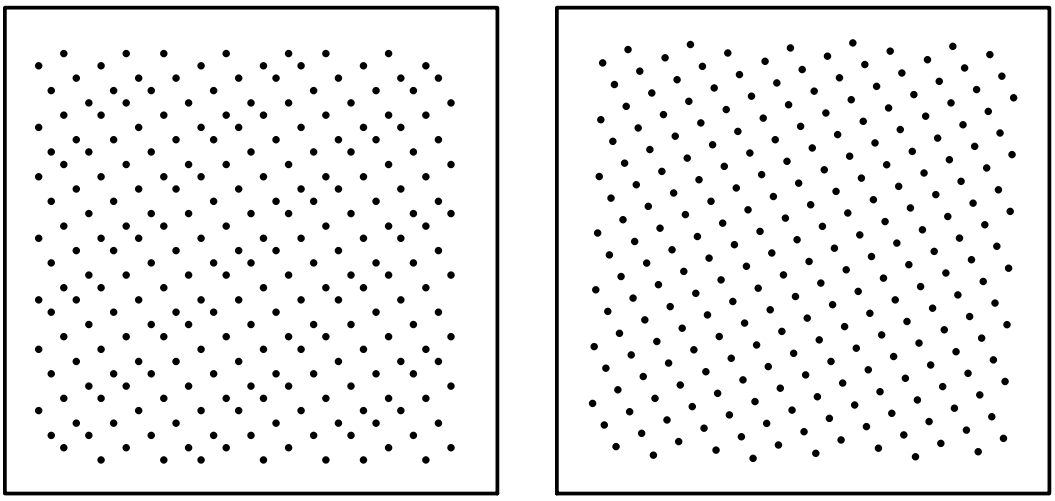
これらの図に描かれた 2 連の諸点を気長に勘定して頂くと分かりますが、左右とも 1 周期 $T = 250$ と同じ数の点が存在します。という事は 2 連の諸点には特殊性[3]があって、両図共に 1 度ずつ現れて重複する事はありません。左図は相続く乱数 u_k と u_{k+1} の（そして右図は関係する乗算合同法乱数の相続く 2 連の）相関を調べるプロットになっているのです。左図は多少でこぼこがありま

[2] あなたが 1990 年代のパソコンを持ち、この pdf ファイルをゆっくり表示させる事ができるなら、これら及び以下の図の上で点が乱数の発生順に現れる動画を御覧になれます。

[3] この言葉は不要、性質は実は**巡回列**というものの一般性だと後にわかります。

すが、まあ平面に均等に分布し、相続く乱数 u_k と u_{k+1} とはほぼ独立と見えます。

第 1 図　右は素数の法 251、原始根 34 の乗算合同法 2 連のプロット



(第 1 図終り)

図の威力、と言うか我々の視覚の威力は明らかです。そして数と幾何が我々に与えるプレゼントはもっと精妙多様で素晴らしいのです。

1. 2. 法 d の合同と合同算法

前に進むため、我々の小学校での算術の知識を少し磨きます。

定義 2.（素数、素因数分解、互いに素、法 $d > 0$ での合同）

$x, y, z, \cdots$ は整数[4]を表すとする。

(A) 整数 $x > 1$ が 1 と自分自身以外の約数を持たないとき、x は素数であると言う。1 は素数に含めない。

(B) 整数 $x \geq 2$ が素数 p で割り切られるとき、p は x の素因数であると言う。

(C) 任意の整数 $x \geq 2$ の素因数への分解は一意である (ユークリッド-ガウス)。

(D) 整数 x, y が共通な素因数を持たないとき、『互いに素』と言う。

(E) 整数 $d > 0$ に対し整数 x, y が d で割り切れる差 $x - y$ を持つとき、x と y は法 d で合同と言い、$x \equiv y \pmod{d}$ と記す（ガウスの記法)。　**（定義 2 終り）**

上の**補題 (C)** は小さい素数から或いは大きい素数からの順次割り算を考えると殆ど自明と思われますが、それは本当か、証明が要るのではないか、とガウス

[4]『整数 integers』は正、0、負すべて含む事を約束し、正の整数を『数 numbers』と言う用語は避けます。

が証明を与えました。証明にはユークリッドの互除法が必要なので、後に記します。1 は素数には入れませんでした。そうすると 1 と任意の整数とに共通素因数はないので、1 は自身も含めたすべての整数と互いに素、という定義になります。この場合を『互いに素』の定義から除外しない方が便利です。

補題 3.（法 d での合同関係の性質）

整数 $x, y, z, \cdots$ と整数の法 $d \geq 1$ について

(A) $x \equiv y \pmod{d}$ とは $y = x + kd$ となる整数 k の存在と同値である。

(B) $x \equiv y \pmod{d}$ とは x, y を d で割った余りが等しい事である。

(C) $xy \equiv xz \pmod{d}$ であり、x が d とは素ならば $y \equiv z \pmod{d}$ が成り立つ。即ち法 d とは素な整数 x を両辺に含む合同式は x で割る事ができる。

(D) $x, y, z, \cdots$ が法 d で $x', y', z', \cdots$ と合同なら、$x, y, z, \cdots$ から加減乗法で作られる任意の整数 $f(x, y, z, \cdots)$ について次が成り立つ：

$$\begin{aligned} f(x, y, z, \cdots) &\equiv f(x', y, z, \cdots) \equiv f(x, y', z, \cdots) \\ &\equiv \cdots \equiv f(x', y', z', \cdots) \pmod{d}. \end{aligned}$$

即ち整数の加減乗法では、演算の任意の段階で、任意の整数をそれと法 d で合同なものと置き換えても、結果は変らない。

（証明） **(A)** 明らかです。

(B) 上の **(A)** から自明。

(C) $xy \equiv xz \pmod{d}$ なら $xy - xz = x(y - z)$ が d の倍数です。x には d と共通の素因数はないから、これは $y - z$ が d の倍数である事、$y \equiv z \pmod{d}$ を意味します。

(D) 例えば仮定 $x' \equiv x \pmod{d}$ 等からある整数 $j, k, l, \cdots$ について、

$$x' = x + jd, \quad y' = y + kd, \quad z' = z + ld, \ \cdots$$

と**等式**が成り立ちます。$x'y = (x + jd)y = xy + (jy)d$、$jy$ は整数だから $x'y \equiv xy \pmod{d}$。議論は他のすべての場合で成り立ち、結論は自明です。 ■

法 $d = 1$ では整数 x, y の差は整数、法 $d = 1$ の倍数、となり、すべての整数 x, y について $x \equiv y \pmod{1}$ が成り立つ事に注意します。 また法 d での合同を **(B)** によってすべて『法 d で割った余りの算法』と言ってもよいので、FORTRAN 等の計算言語ではこの事を利用して関数 $\mathrm{mod}(x, d)$ を定義[5]します。**(D)** から『余り』での置換は計算のどの段階でも正しいのですが、置換すると整数を算出する式 $f(x, y, z, \cdots)$ の構造が見えなくなります。だからコンピュータではない我々は計算途中は式をそのまま残して、『法 d で割った余り』を取るのは最後にするのが得策です。

[5]関数 $\mathrm{mod}(x, d)$ では整数 x を $x \geq 0$ に限る方が安全です；負の x に対する $\mathrm{mod}(x, d)$ がどの様に定義されているかは計算言語毎に注意しなければならないと思います。

少し難しい考えになりますが、『整数達の間に、整数の法 $d \geq 1$ での合同関係を置く』事は、整数の法 $d \geq 1$ で合同な、つまり整数 $d \geq 1$ の整数倍異なるすべての整数を『同じものだ』と見る事です。それは整数達の乗る数直線を周の長さが d の円に巻き付け、円周上の 2 点 a, b が円周 d の整数倍の距離違うなら同じ点だ、とする考え方です。実はこれが我々非数学徒にとっては大問題の起りなのです。20 世紀中葉から発展した計算機と計算プログラムは、この難題に対して『関数』mod を携えて対応しました。それは非負の整数 A と法の整数 $d > 0$ に対して整数 $A \geq 0$ を法 d で整数の商 $Q \geq 0$ で割った余りの整数 $R \geq 0$ で定義する事です。確かにこれは余り $R = \mathrm{mod}(A, d) \geq 0$ を非負の整数 A に対して唯 1 つ確定し、『関数』の資格を持ちます。しかしその鈍重な定義は数学者の気に入るものではなく、『法 d の合同、同値類』の概念がガウスの記号 $\equiv$ と共に導入された様です。

我々にとって問題の元凶はこの合同算法ですが、それは暫く擱きます。

1. 3. コンピュータ上の乱数と概念的問題

話題が飛び跳ねて脈絡が見えないとの御不満は、全体として最短の記述を狙っていると推察頂き、暫く我慢をお願いします。コンピュータ上の乱数系列の利用を考えます。現在メモリーは安価で、1 テラバイト $= 10^{12}$ バイト $\simeq 2^{40}$ バイトのメモリーでも驚きませんが、それでも 8 バイト乱数なら 2^{37} 個しか収納[6]できません。十分な数の優れた乱数を記憶に置いてシミュレーションする事は現在も、そして将来も、諦めるべきです。

コンピュータ上の乱数は最も正統的には大規模シミュレーションに使いたいので、乱数を用いた大規模プログラムとなると間違い探し、デバッグ虫取り、が大問題です。乱数は全く同一のものを繰り返し使ってプログラムの手直し毎の計算の変化を見なければなりません。だからコンピュータ上の乱数は、やり直すと決まれば、前に出力した系列を完全に再現しなければなりません；これが reproducibility 再現可能性の要求[7]です。そして計算言語を FORTRAN や C 等々と変え、コンピュータを替えたとしても、出力乱数は同一でなければなりません。移植可能性 transportability の要求です。

記憶に蓄えられる量ではないなら計算生成しかありません。また再現可能性や移植可能性を保証したいならその計算は整数のみを用いなければなりません；乱数計算の回数は膨大で、実数計算では丸めや打ち切り誤差の集積が避けられず、さらに計算言語や計算機毎に実数の規格が異なるからです。整数計算ではどんな計算言語、どんなコンピュータでもそのような誤差の集積や規格の

[6] この個数の乱数なら、乗算合同法では卓上コンピュータを生成専一に動かしてほぼ 5 時間で生成を終えます。

[7] だからどんなに統計的性質がよくても、放射能カウンターの出力のように再現できない**自然乱数**は使えません。

違いはありません。

数式計算で生成される数列が果たして『でたらめな数』としての乱数と言えるかどうか、は古典的哲学的な大疑問でした。しかし現在の我々はコンピュータ上で『乱数の 1 つの見本過程』を実現したい、それで十分、と認識します。この立場を受け入れましょう。『決まった計算式で算出されるからでたらめではない』という事はなく、算出された見本列が仮説、『相続く出力が独立である乱数系列の見本過程だ』という事を最も弱く打ち消すなら十分、という統計的仮説検定の問題とするのです。

我々はこうして、概念的困難を越えて次の認識に達しました。コンピュータソフトウェアとしての我々の問題は

(A) 十分大きい整数 $z \gg 1$ を取り、整数列 $\{x_0, x_1, \cdots, x_{T-1}\}$ を

$$\{x_0, x_1, \cdots, x_{T-1} |\ 0 \leq x_k < z,\ \ k = 0, 1, \cdots, T-1\}$$

が十分大きい個数 T まで成り立つ様に生成し、

(B) 乱数としては有理数の列、

$$\{u_k := x_k/z |\ 0 \leq u_k \leq z,\quad k = 0, 1, \cdots, T-1\}$$

を出力して、

(C) 列 $\{u_k\}$ が独立乱数見本列だという仮説を最も弱く否定する生成機構を選ぶ、

という事です。現在漸く得られたこの安心立命を共有しましょう。この **(C)** に言う『検定で優れた生成機構を選ぶ』事は実現の難しい作業です。

乱数列は 0 と 1 の間の数を一様に、そして独立に出力する『一様独立乱数列』以外にも数多く存在します。しかし他の確率分布の乱数へは精度の保証された関数変換が十分に用意されていて、全て一様独立乱数から得る事ができます。最も困難なのは正確な一様独立性の保証された乱数の獲得です。だからここでは一様独立 uniform and independent 乱数の生成に話を限ります。

1. 4. 乗算合同法

整数の加減乗除の演算も、合同算法もすべて数からの贈り物ですが、我々は驚くべき多くの数学的事実を発見します。表記のため、まず乗算合同 (MC) 方法 multiplicative congruential method と呼ばれる最も古い一様独立乱数生成法の概念と表記を定めます。与えられた法の整数 $d > 0$ と任意の整数 $a > 0$ に対して定まる計算諸言語で標準的な関数 $\mathrm{mod}(a,\, d)$ を確認します。正の整数 a を法の整数 $d > 0$ と整数の q で割った整数の余りが $a' = \mathrm{mod}(a,\, d)$ です。前の第 1. 2. 節ではこの関係をガウスの記法、

$$a' \equiv a \ (\mathrm{mod}\ d)$$

でも記しました；a' は a と法 d で合同、同値なものなら何でもよい、とするの

です。『関数 $\mathrm{mod}(a,d)$ の方が簡単』とも思われますが、ガウスの記法の利点はすぐ分かります。

定義 4.（乗算合同法 multiplicative congruential method[8]）

法 modulus の整数 $d>0$ と、法 d とは素な整数の乗数 multiplier z との組 (d,z) は、次の様に乗算合同 (MC) 法一様乱数列 $\{r_0,r_1,\cdots\}$ を生成する：

$$\begin{aligned} &x_0 \equiv n \pmod d,\\ &x_k \equiv z x_{k-1} \equiv n z^{k-1} \pmod d, \quad k=1,2,\cdots,\\ &r_k = x_k/d, \quad 0 \le r_k < 1, \quad k=0,1,2,\cdots. \end{aligned}$$

ここで $n>0$ は法 d とは素な任意の整数で、種 seed と呼ばれる。

（定義 4 終り）

乗算合同法は 3 つ組 (d,z,n) で定まる、とすべきです。しかし seed 種 n は乱数出力列の出発値を定めるだけで統計的性質には関係がないので、多くの場合略記 (d,z) を用います。

法 d では整数は本質的には $0,1,\cdots,d-1$ だけですが、ガウスの見方では方 d で同値な整数 a と $a'=a+kd$, k は任意の整数とは同値だと見て、『法 d の同値類 Z/d』というもの』の全体、

$$Z/d = \{0,1,2,\cdots,d-1\}$$

というものを考えます。法 d の乗算合同法はこれと違って

> 法 d とは素な、即ち法の整数 d とは共通素因数のない整数の集合
> 即ち d との最大公約数 $\mathrm{GCD}(d,a)=1$ の整数の法 d での集合 $Z_d{}^*$

を考えるのです。互いに素な正の整数の組 (d,z,n) が定める乗算合同 MC 法乱数は $Z_d{}^*$ という整数の集まりだけの中を動き、それは次の群の概念と見事に調和しています。

1. 5. 既約剰余類群

群の概念は現代数学の始まりで、19 世紀ガロワによって発見された事は御存知の通りです。我々の応用には一般ではなく部分的な理解で十分なので、整数の特殊な集まり（既約剰余類）とその乗法だけに限って考えて話を易しくします。

興味は整数の法 $d>0$ が定められた整数の全体で法 d とは共通素因数のないものです。任意の整数 x を d で割った余りは $\{0,1,2,\cdots,d-1\}$ の d 個だけで、

[8] D. H. Lehmer: *Mathematical methods in large-scale computing units,* Annals Comp. Lab. Harvard **26** (1951) pp. 141-146.

それらが代表する法 d の同値類を Z/d と記し、その中の d とは共通素因数を持たないものを考えます。

定理 5.（既約剰余類群 reduced residue class groups）

任意の整数 $d > 0$ に対し、法 d の剰余類 Z/d、$\{0, 1, 2, \cdots .d-1\}$ で代表される『法 d で合同な整数の集合』から d とは素な (d と共通素因数を持たない) ものだけで定義された数の全体 ${Z_d}^* \subset Z/d$ を『法 d の既約剰余類 reduced residue class』と言う。${Z_d}^*$ は法 d での乗法 $*$ に[9]関して、次の群の公理 1 から公理 3 を満たす。

（公理 1） ${Z_d}^*$ の任意の整数 x, y, z には法 d の乗法 $*$ が定義されて、

(A) $x * y \in {Z_d}^*$ が成り立つ、即ち ${Z_d}^*$ は乗法 $*$ で閉じていて、

(B) $(x * y) * z = x * (y * z)$、即ち乗法 $*$ には結合法則が成り立ち、

(C) $x * y = y * x \in {Z_d}^*$、即ち乗法 $*$ は可換性を満たす。

（公理 2） ${Z_d}^*$ には単位元 $e \equiv 1 \pmod d$ が存在し、任意の $x \in Z_d^*$ に対して $x * e \equiv e * x \equiv x \pmod d$ が成り立つ。

（公理 3） 任意の $x \in {Z_d}^*$ にはその逆元 $x^{-1} \in {Z_d}^*$ が存在して、$x * x^{-1} \equiv x^{-1} * x \equiv e \equiv 1 \pmod d$ を満たす。

（証明） こんな簡単な事、こんな証明が何の役に立つのか、の疑問は抑えて、用語の納得のために議論をトレースして下さい。

（公理 1） d とは素な 2 整数 $x, y \in {Z_d}^*$ の普通の積 xy が再び d とは素である事は x, y 共に法 d と共通素因数を持たない事から明らかで、

$$x * y \equiv xy \pmod d \in {Z_d}^*$$

が成り立ちます。即ち ${Z_d}^*$ は法 d の乗法 $*$ で閉じています。交換結合法則は普通の数の乗法で成り立ち、そのまま引き継がれます。

（公理 2） 整数 1 に法 d で合同で d と素な元 e は任意の整数 k で $e = 1 + kd$ と表現されて存在し、次の成立は明らかです：

$$ex = (1 + kd)x = x + kxd \equiv x \pmod d,$$
$$xe = x(1 + kd) = x + xkd \equiv x \pmod d.$$

（公理 3） 任意の $x \in {Z_d}^*$ を取り、${Z_d}^*$ の有限個の元を 1 列に並べて $a, b, \cdots, f$ と記します。これらと x の積の列 $xa, xb, \cdots, xf$ は皆 d と素、共通素因数のない ${Z_d}^*$ の整数で、**補題 3** の **(C)** から $xa \equiv xb$ なら $a \equiv b \pmod d$、対偶として a と b が法 d で合同でなければ xa と xb とは法 d で異なります。言い換えるとこれらは ${Z_d}^*$ のすべての元の等しいもののない並べ替えであり、この中に必ず 1 に法 d で合同な単位元が 1 つあります。即ち $xx' = e$ となる $x' \in {Z_d}^*$ が必

[9]少しの間この法 d での乗法を $*$ と記します。

ず 1 つだけ存在し、これが x の逆元 $x' \equiv x^{-1} \in {Z_d}^*$、$x * x^{-1} = e$ です。法 d の乗法 $*$ は可換だから $x^{-1} * x \equiv 1 \pmod d$ も成り立ちます。[10] ■

かつて**補題 3** の **(B)** で、既約剰余類群 ${Z_d}^*$ について、その元（即ち d とは素な整数）a, b, c の間に関係 $ab \equiv ac \pmod d$ が成り立つのは $b \equiv c \pmod d$ の場合である事を見ました。群であると認識すると、『d と素である』事を使わずとも、任意の群 G の 3 つの元 a, b, c について一般的明解に、

$$\begin{aligned} a^{-1} * (a * b) &= (a^{-1} * a) * b = e * b = b \\ &= a^{-1} * (a * c) = (a^{-1} * a) * c = e * c = c \end{aligned}$$

と群乗法で知る事になります。

1. 6. 部分群とラグランジュLagrange の定理

群の 3 公理という何の変哲もないものだけで群一般の多様な性質が保証されるのは不思議です。我々の舞台乱数でのその様な有用な性質の主役は『部分群 subgroup』の概念、様々な群の元の総数の理解に重要なラグランジュの定理と、巡回部分群、巡回群の概念です。以下一般の有限群 G の元の総数を $\sharp G$ で表して『order 位数（いすう）』と呼びます；収まりのよい用語ではないが、慣習です。

補題 6.（部分群とその条件）

群乗法 $*$ を持つ（有限）群 G の部分集合 H が同じ乗法 $*$ に関して再び群であるとき、H は G の部分群 subgroup であると言う。H が G の部分群である必要十分条件は、

$$H \text{ の任意の 2 元 } x, y \text{ が } x^{-1} * y \in H \text{ を満たす事である.}$$

（証明） H が部分群ならその任意の 2 元 x, y について、

$$x^{-1} \in H, \quad x^{-1} * y \in H$$

は明らかで条件は必要です。逆に条件が満たされると、$y = x$ として部分集合 H には群 G の単位元 $e = x^{-1} * x$ が属すと分かります（群の**公理 2** の成立）。故に $y = e$ として H の任意の元 x に対して $x^{-1} * e = x^{-1} \in H$ も成り立ちます（群の**公理 3** の成立）。**公理 1** はもとの群 G の通り成り立つので H は群、G の部分集合で部分群です。 ■

すばらしいのは次の Lagrange の定理です。

[10] 法 d の乗法の可換性に頼らなくても（行列の様に乗法が非可換でも）乗法の結合法則だけから次の議論ができます：x^{-1} の逆元を y とすれば $1 = x^{-1}y = (x^{-1}e)y = x^{-1}(xx^{-1})y = (x^{-1}x)(x^{-1}y) = (x^{-1}x)e = x^{-1}x$、だから正方行列 A の逆行列 A^{-1} でも $AA^{-1} = A^{-1}A =$ 単位行列、が成り立ちます。

定理 7.（Lagrange の定理、部分群の位数）
群 G が位数 g を持ち、G の部分群 H の位数が h なら、g は h で割り切られる。
（証明） G の元を 1 列化して $G = \{a, b, \cdots, f\}$ と記し、部分群 H の元を 1 列化して $\{j, k, \cdots, m\}$ と記す事にします。次の集合、

$$aH := \{aj, ak, \cdots, am\}$$

を考えて『部分群 H の a 剰余類 residue class[11]』と呼びます。すでに見た様に剰余類 aH はすべて異なる G の元から成り、元の総数（位数）は $h = \sharp H$ です。次の補題が成り立ちます：
補題 8.（部分群による群の剰余類への分割）
群 G の任意の 2 元 a, b に対し G の部分群 H の剰余類 aH, bH は、集合として同一か、それとも共通元を持たない同数の元の集合か、の二者択一である。
（証明） 剰余類 aH と bH とは共通元を持つか持たないかの二者択一です。共通元があるなら、$a * h = b * h'$ となる部分群 H の元 h, h' があり、

$$a = b * (h' * h^{-1}), \quad h' * h^{-1} \in H$$

が得られ、$(h' * h^{-1})H$ は H の並べ替えで集合として H と同一ですから、2 つの剰余類 aH と bH は同一集合です。そうでなければ 2 つの剰余類は共通元を持ちません。 ■
（Lagrange の定理の証明続き） こうして部分群 H があれば、群 G の元で H に入っていないもの a を取って H とは共通元を持たない剰余類 aH が作られます。集合 H と aH とで G が尽きれば $\sharp G = 2\sharp H$ となります。そうでないなら H と aH とには属さない G の元 b がありますからそれで剰余類 bH を作り G は共通元のない H, aH, bH を含みます。これで G が尽きれば $\sharp G = 3\sharp H$ です。この手続きは部分群 H の剰余類には属さない G の元がなくなるまで続き、群の位数は部分群の位数の倍数です。 **（Lagrange の定理証明終り）**

1. 7. 巡回部分群と巡回群

以下群 G の 2 元 a, b の乗法を通常の積のような ab の記法に戻し、$a * b$ からは離れます。また単位元は記法 e ではなく 1 と記す事にします。部分群の中の特別なものが巡回部分群 cyclic subgroup です。我々は有限群 G で考えますから、群 G の元 a の冪の列 $H(a) = \{1, a, a^2, \cdots\}$ は必ず有限回で再帰します。仮に再帰が $a^i = a^j$ の形で整数 $i < j$ で成り立つなら、a の逆元 a^{-1} を i 回両辺に掛けて等式 $1 = a^{j-i}$ がある整数 $h = j - i > 0$ で成り立ち、a の冪の列は、

$$1, a, a^2, \cdots, a^{h-1}, a^h = 1, a, a^2, \cdots, a^h = 1, a, a^2, \cdots$$

[11] ここでは群乗法は可換だから左右の剰余類の区別はありません。

の形です。次の定義を置きます。

定義 9.（群の元の位数 order と巡回部分群 cyclic subgroup）

任意の有限群 G の元 a には $a^h = 1$ となる最小の正の整数 $h > 0$ が存在する。これを元 a の位数 order と[12]言う。また、

$$H(a) := \{1, a, a^2, \cdots, a^{h-1}\}$$

を『a が作る巡回列 cyclic sequence』と呼ぶ。 **（定義 9 終り）**

定理 10．(巡回部分群)

群 G の元 a が位数 h を持てば、a が作る巡回列 $H(a)$ は位数 h の部分群である。これを a が作る巡回部分群 cyclic subgroup と呼ぶ。

（証明）（可換な）群 G の部分集合 $H(a)$ には群と同じ乗法が定義され、乗法の結合法則を満たすから $H(a)$ では群の公理 1 が成り立ちます。単位元 1 は $a^h = 1$ で $H(a)$ 内に存在し、$H(a)$ の一般の元 a^j には a^{h-j} が $a^j a^{h-j} = a^h = 1$ を与える逆元として存在します。$H(a)$ は群の公理 2 及び 3 を満たし、G の部分群です。 ■

Lagrange の定理から、群 G の任意元 a の作る巡回部分群 $H(a)$ の位数 h は群 G の位数（元の総数）g の約数です。この事は乗算合同法乱数生成機構にとって最重要な知識の 1 つです。

定義 11.（巡回群 cyclic group）

群 G に元 a があってその巡回列 $H(a)$ が群 G 全体であれば、G は巡回群と呼ばれ、a はその生成元と名付けられる。 **（定義 11 終り）**

素数 prime $d = p$ を法とする既約剰余類群は巡回群で、生成元、法 p の原始根 primitive root の存在は周知ですが、簡単重要ながら証明の難しい理解なので後に再び触れます。

1. 8. コンピュータ上の乗算合同法乱数の表現力

コンピュータ上の乱数列のより深い理解に向かいます。シミュレーション計算の技術的要求によって、私達はコンピュータ上の乱数生成は整数の列、ある大きな整数 z を定めて、

$$\{x_k |\ x_k \text{ は整数で } 0 \le x_k < z,\ \ k = 0, 1, \cdots, T\}$$

の形の有限整数列 $\{x_1, x_2, \cdots, x_T\}$ を生成して、有理数列、

$$\{u_k := x_k/z |\ k = 1, 2, \cdots, T,\ \ 0 \le u_k < 1\}$$

を $0 \le u_k < 1$ の一様乱数として出力すべきだ、という状況を理解しました。

[12]位数 order は多用されてわずらわしいのですが、慣習なので我慢しましょう。

思考実験をします。上のような整数列の（メモリーに置くのではなく）生成を目指すなら、我々の整数演算にはいままで気付かれていなかった見事な構造的可能性が存在するのです。

最初の小さな工夫として、この整数列を周期 T の周期列の 1 周期と解釈します。直ちに我々は z 進循環小数の有理数、

$$X = 0.x_1x_2x_3\cdots x_T\ x_1x_2x_3\cdots x_T\ x_1x_2x_3\cdots = 0.\dot{x}_1x_2\cdots\dot{x}_T$$

との自明な対応に気付きます。中学算数で明らかな様に次の変形が可能です：

$$z^TX = (x_1x_2x_3\cdots x_T).(x_1x_2x_3\cdots x_Tx_1x_2x_3\cdots)$$

$$(z^T-1)X = x_1x_2x_3\cdots x_T$$

$$X = \frac{x_1x_2x_3\cdots x_T}{z^T-1} = \frac{n}{d}.$$

正又は 0 の整数列 $\{x_1, x_2, \cdots, x_T\}$ は『すべて 0』ではないと仮定します。そうすると有理数 X は $X > 0$ を満たし、上の既約分数 n/d の形に変形され、分子 numerator は $n > 0$ であり、分母 d と n とは互いに素な正の整数となります。分母 denominator d は整数 $z^T - 1$ の約数だから z と d も互いに素です。念のため加えれば、中間の式の分子は次を表します：

$$x_1x_2x_3\cdots x_T := x_1z^{T-1} + x_2z^{T-2} + \cdots + x_T$$

まとめると、コンピュータ上の再現移植可能な乱数列を 0 以上 z 未満のすべてが 0 ではない整数を用いて長さ T だけ与える事は、整数の 3 つ組 (d, z, n) で z, n は d とは素であり、$n < d$ を満たすものを取る事と同値です。但し乱数は $\{x_k/z | 1 \le k \le T\}$ の有理数の形で与えられますから、整数の上限 z は (分数 x_k/z が例えば単精度、倍精度の数となる様に) 十分大きく取らなければなりません。

目覚しいのは 3 つ組 (d, z, n) からの乱数の再構成です。$0 < X \le 1$ の[13]循環小数 X を表すある既約分数 $X = n/d$ から z 進で小数点以下の各桁の整数 $\{x_k\}$ を得るのは簡単な割り算です。割り算の第 1 段は、n を z 倍して d で割って商 x_1 と余り r_1 とを得る作業です。演算関係は次の等式になります：

$$zn = x_1d + r_1, \quad r_1 := zn - x_1d, \quad r_1 \equiv nz \pmod{d}.$$

小数点以下第 2 位の整数 x_2 は、余り r_1 を z 倍して割り算から商 x_2 と余り r_2 として得られます:

$$zr_1 = x_2d + r_2, \quad r_2 = zr_1 - x_2d, \quad r_2 \equiv nz^2 \pmod{d}.$$

[13] $\overline{z} := z - 1$ とすると、無限循環小数 $0.\overline{z}\overline{z}\overline{z}\cdots$ は、例えば等比数列の総和法によって、1 だと分かります。

以下割り算を続けて小数点以下第 k 位の整数 x_k と余り r_k とは次の通り：

$$zr_{k-1} = x_k d + r_k, \quad r_k = zr_{k-1} - x_k d, \quad r_k \equiv nz^k \pmod{d}.$$

宇宙開闢以来存在する『数』がどのように 21 世紀を予測されたのか不思議ですが、これは次の重要な、『どのような乱数生成機構を選ぶべきか』という 20 世紀乱数理論の最大の問題を決着する知見を与えます。

定理 12. （コンピュータ上の任意の一様乱数の乗算合同法乱数近似）[14]

正の整数 z は $1/z$ がコンピュータ上の実数単精度或いは倍精度に相応しい大きさだと仮定する。すべてが 0 ではなく、0 以上 $z-1$ 以下の整数を成分とする十分に長い周期 T の任意の整数列 $\{x_k|\ 0 \le x_y < z,\ 1 \le k \le T\}$ を考える。

(A) 整数列が与える一様乱数の見本列 $\{u_k := x_k/z|\ 1 \le k \le T,\ 0 \le u_k < 1\}$ には、それに伴われ T, z で定まる正の整数 d, n が存在し、z, n は d とは素であり、$0 < n < d$ が成り立って、(d, z, n) 乗算合同 (MC) 法生成機構からの一様乱数見本列、

$$\{v_k := r_k/d|\ 0 \le k \le T-1, \quad r_k = \mathrm{mod}(nz^k, d), \quad 0 < v_k \le 1\}$$

がもとの一様乱数列を次の形で『一様近似』する：

$$0 < v_{k-1} - u_k < 1/z, \quad 1 \le k \le T.$$

(B) 逆に正の整数 (d, z, n) の組で d が z, n とは素、かつ $n < d$ を満たして生成される周期 T の乗算合同法 (乱) 数列 $\{v_k|\ 0 \le k \le T-1\}$ からはもとの乱数列 $\{u_k|\ 1 \le k \le T\}$ が次の式で再現される：

$$u_k = v_{k-1} - v_k/z, \quad 1 \le k \le T.$$

（証明）(A) $k \ge 2$ に対して上の第 k 段割り算の等式から $zr_{k-1} - x_k d = r_k$ です。$r_0 := n$ と置けば、この等式は $k = 1$ でも成り立ちます。これを dz で割って次を得ます：

$$r_{k-1}/d - x_k/z = (r_k/d)/z, \quad 0 < v_{k-1} - u_k = v_k/z.$$

すべての $1 \le k \le T$ で $0 < v_k < 1$ だからこれは一様近似の成立です。

(B) 自明です。 ■

第 2 頁の第 1 図左は、素数の法 $p = 251$、原始根乗数 $z = 34$ の乗算合同法 (p, z) が作る周期 $T = p - 1 = 250$ の 2 連の点の右図から**定理 12 (B)** によって

[14] H. Nakazawa and N. Nakazawa: *Designs of uniform and independent random numbers with long period and high precision*, file name *3978erv.pdf*, March 9-July 8, 2008, www10.plala.or.jp / h-nkzw / indexarchivenew.html

その元になる乱数の 2 連図を再現、並べて示したものです。**定理 12 (A)** によって点の座標は $1/34$ の一様精度で近いので図全体も近さが視認されます。実用乗算合同法 (d, z) では $d \approx 2^{54}$ や $z > d^{1/2} \approx 2^{27} \approx 134217728$ にもなりますから、乗算合同法そのものを取らない理由はありません。

我々はこれから乗算合同法乱数が他に卓越した利点、精密多様な性能検定の可能性を持つ事を見、また空間格子にもきれいな無相関を保って配布できる事も見ます。乗算合同法の簡明な構造、しかも群の構造、それにもかかわらずそれが許す豊穣な諸検定は、数の不思議な恩寵とでも言うべきでしょうか。

第 2 章　素数と合成数の法の乗算合同法と周期

2. 1. 素数の法の乗算合同法の周期

法の整数 d、乗数 z、seed 種 n の乗算合同法 (d, z, n) が生成する整数の列 $\{r_0, r_1, r_2, \cdots\}$ について第 1 に問題になるのはその長さ、繰り返す周期です。この列は既約剰余類群 $Z_d{}^*$ の中の元 z が作る巡回部分群 H_z の n 剰余類、

$$nH_z := \{nz^k (\mathrm{mod}\ d) |\ k = 0, 1, 2, \cdots, T-1\}$$

であり、周期は z の位数です。

我々が目指すのは精細ではなくても良いが利用に十分な数学状況の理解です。現在大方針は乗算合同法だと明解に納得しました。その設計では Fishman と Moore によって[15]打ち立てられた大原則の exhaustive tests、つまり法 d や乗数 z のどの組が優れているのか、は全く予断できる所がない、有資格のものをすべて検定するしかない、というのが永遠の真実です。ただ、僅かな設計の自由度として望む長さの周期を得るように法 d と乗数 z を選ぶ事はできますし、また法と乗数の形をこの『すべての有資格のものを検定する計算労力を少しでも減らす』ものに選ぶ事もできます。

この自由度を生かすために第 1 に必要な事は奇素数の法 $d = p \gg 2$ とその法での原始根乗数 z の存在と位数構造の理解です。20 世紀の乱数理論では法として 2 の大きい冪にも重要な役目がありました。有限体 $\boldsymbol{F}_2$ を用いた GFSR generalized feedback shift register 法やその変形も多く用いられました[16]が、これは全周期に亙る検定が不可能なのでお勧めできません。 21 世紀になって私達はさらに乗算合同法としての検定から、『2 の大きい冪の法は奇素数の法と組み合わせる事ができない』という[17] 20 世紀には理解されていなかった特

---

[15] 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), pp. 24-45.

[16] この構成での大問題は、周期の非常な長大さ (2^{600} 以上!) と、使い切られる事のない『全周期での equidistribution 均等分布』という名目的性質以外には統計分布性能の検定評価がない事、そして『有限体 $\boldsymbol{F}_2$ 上の巨大次数の原始多項式』という、生成方式を与える有資格者の余りに膨大な数の存在が『優れた原始多項式を検定で選ぶ』事を不可能にする点です。**定理 12(A)** によれば、この様な乱数を有限周期 T で切って、乗算合同法で表されるはずですが、既約分数 n/d の形を得る事は明らかに不可能、初めから乗算合同法で進む以外の方法がありません。

[17] H. Nakazawa and N. Nakazawa: *Designs of uniform and independent random numbers with long period and high precision*, file name *3978erv.pdf*, March 9-July 8, 2008, www10.plala.or.jp / h-nkzw / indexarchivenew.html; 従って例えば $d = 10^k$ の様な法は用いる事ができません。この『相関』は乱数の例えば 2 連出力の半周期までの点を平面に打ち出すと明瞭に見られますが、1 周期を打つと前半の打点を綺麗に補填して見えなくなってしまう、という意地の悪いものです。

殊な相関の発生にも気付かされました。21 世紀の乱数生成機構としては、だから、(d, z) 乗算合同法であって法 d として、

(1) 奇素数単独　(2) 奇素数 2 つ以上の組み合わせ　(3) 2 の大きな冪

しか可能性は無くなりました。このうち (2) は乗数の非資格者候補を『有望ではなかろう』と篩い落とす直感手段の有利があって、我々は現在専一に検定探索を行ってきました。それでも現実としては、現在検定作業開始から数年以上を経ても『漸く 2 個』の合格 MC 生成機構しか得られていません。幸いそれら合格者は十分な大周期と優れた高性能を持つもので、後章に詳しく開示します。将来は (1) の巨大な単独奇素数の法や (3) の『2 の超巨大冪の法』でも、と夢見がちですが、これらにはコンピュータでの計算、あるいは検定上の大問題があって、残念ながら取り下げなければなりません。後に事情を明快に御理解頂けるでしょう。

以下話を (2) に限ります。順序としてまず奇素数の法の一般性質を振り返り、検定計算のための小さな工夫を述べます。どんな素数の法 $d = p > 2$ の既約剰余類群も簡明な構造を持ちます：法 p の既約剰余類が

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

である事です。MC 法にはこの『巡回群』の原始根による巡回表現が必要です。どんな奇素数の法 $p > 2$ にもにも最大の位数 $p - 1$ の原始根がある事は周知です。ただこの事実の一般証明は『法 p では方程式 $z^k \equiv 1 \bmod p$ の解は k 以下の個数しかない』という事実に基づくのが現在のスタンダードで超絶的、取り付き難いと思われ触れません。我々は MC 乱数、原始根の巡回列の周期がより長い事を望むので、素数の法の原始根と関係する MC 法とが専一の道具立てです。しかも優れた MC 乱数生成機構の探索はできるだけ簡単にしたい、『原始根の探索』に手間を掛けたくないのです。ここでは次の**定理 13** に記す 2 種類の素数とその容易に得られる原始根とを記して、まず『原始根探索の計算負荷』を軽減します。

定理 13.（特別な素数 $p > 2$ の法とその原始根）

(A) 正の整数 q が素数で $p = 2q + 1$ も素数のとき、p を Sophie Germain 素数（SG 素数）[18] と言う。$z = 2$ は SG 素数の原始根で位数 $2q$ であるか、或いは原始根のマイナスで位数 q か、である。

(B) 正の整数 r が素数であり $p = 4r + 1$ も素数であるとき、p を中澤直也素数（NN 素数）と呼ぼう。$z = 2$ は NN 素数 p の (最小の) 原始根である。

[18] $q = 2$ は最小の SG 素数 $p = 5$ を与えます。乗数 $z = 2$ は 4 乗して初めて法 5 で 1 に合同になり、法 5 の原始根です。$q = 3$ は SG 素数 $p = 7$ を与え、乗数 $z = 2$ は 3 乗して法 7 で 1 に合同になり、法 7 の原始根ではありませんが、その負の数 $-2 \equiv 5 \pmod{7}$ は $7 - 1 = 6$ 乗して初めて 1 に合同になる原始根です。

（証明）(A) SG 素数 $p=2q+1$ が与える既約剰余類群 ${Z_p}^*=\{1,2,\cdots,p-1\}$ の位数は $p-1=2q$ です。故に Lagrange の定理によって、元 $z=2$ が作る巡回部分群 H_2 の位数は $2q$ の約数で $2,q,2q$ の 3 つのどれかです。$p=5,7,\cdots$ の SG 素数のどれであっても、$z=2$ の位数は 2 ではなく、位数は q か $2q$ のどちらかです。位数 $2q$ なら原始根です。$z=2$ の位数が奇数 q なら原始根ではないが -2 の位数は 2 ではないし、q は奇数だから $(-2)^q\equiv(-1)^q2^q\equiv-1$ であって -2 の位数は $2q$、原始根以外ありません。この場合 2 は原始根のマイナスです。
(B) 最初に最も小さい法の場合を片付けます。最小の NN 素数は $p=13=4\times3+1$ に対して $p-1=12=\sharp{Z_{13}}^*$ で、$z=2$ が持ち得る位数は Lagrange の定理から約数の $2,r=3,4,2r=6,4r=12$ のどれかです。簡単な計算は法 13 で $z^2=4,\ z^3=8,\ z^4=16\equiv3,\ z^5\equiv6,\ z^6\equiv12\equiv-1,\ z^{12}\equiv1$ を与えます。故に $z=2$ は最大位数 $12=p-1$ の原始根と分かります。次の NN 素数は $r=7$ に対する $p=29$ なので一般の NN 素数を $p=4r+1\geq29$ と仮定します。Lagrange の定理は $z=2$ の位数は $4r$ の約数 $\{2,4,r,2r,4r\}$ に限ると教え、仮定 $p\geq29$ は $z=2$ の位数は 2 や 4 ではないと示します。$z^{2r}\equiv-1$ を見ましょう；これが示されれば $z=2$ の位数が r や $2r$ ではなく最大の $4r$ だと分ります。次の積 M を考えます：[19]

$$M:=(2\cdot1)(2\cdot2)\cdots(2\cdot r)\{2\cdot(r+1)\}\{2\cdot(r+2)\}\cdots\{2\cdot(2r)\}=2^{2r}(2r)!$$

これは p を法として次の表現も持ちます：

$$\begin{aligned}M&=2\cdot4\cdot\cdots\cdot(2r)\cdot(2r+2)\cdot(2r+4)\cdots(2r+2r)\\&=2\cdot4\cdots(2r)\cdot(p-(2r-1))\cdot(p-(2r-3))\cdots(p-1)\\&\equiv(-1)^r(2r)!=-(2r)!\ (\mathrm{mod}\ p)\end{aligned}$$

ここで r が奇（素）数である事を用いました。これらは法 p での合同式、

$$2^{2r}(2r)!\equiv-(2r)!\ (\mathrm{mod}\ p)$$

を与えます。$(2r)!$ は法の素数 $p=4r+1$ とは素だから、両辺を $(2r)!$ で割る事ができて、求める合同式 $2^{2r}\equiv-1\ (\mathrm{mod}\ p)$ を得ます。 ■

上の**定理 13** の特殊な奇素数の法 p で『原始根の最小のもの』が 2 或いは -2 である、と分かる事は技術的に重要です。法 p の原始根が $z\equiv2^k\ (\mathrm{mod}\ p)$ 或いは $z\equiv(-2)^k\ (\mathrm{mod}\ p)$、但し k は $p-1$ とは素、としてすべて得られ、全原始根を検定等で容易に sweep できるからです。

これから先は実際検定での細かい技術的事項になります。検定計算はとにかく時間を要し、計算プログラム自体も複雑になります。乗算合同法 (d,z) 乱数

[19]以下のきれいな証明は中澤直也から中澤宏に 2013 年 4 月 17 日に示されました。

生成機構として優れたものは非常に稀にしか存在せず、奇素数の法自体沢山の異なるものを試みなければなりません。1 つの奇素数の法 p の原始根乗数として検定に合格するものがない、という事は常態であり、我々は素数 p のすべての有資格原始根をすばやく exhaustive に掃過して進まなければなりません。ただこれに関連する事柄は、単純平易ではありませんが、実際問題として後に触れる方が興味を繋ぐ上ではよいと思います。話はここで技術の別の理解に向かいたいのですが、その前に周期に関する重要一般的な事柄を述べます。

我々の目的は相続く乱数に優れた独立性を与える乗算合同法生成機構 (d, z, n) を得る事です。周期 T は勿論大規模シミュレーション計算にも十分な長さで、使い切られる事のない様にしなければなりません。奇素数の法 $d = p$ とその原始根乗数 z の構成なら、巡回列は乗数の位数 $h = p - 1$ で 1 に合同になり、それ以後は繰り返しだから周期は $T = h = p - 1$ で、これから考えても最長周期の原始根などを乗数に選ぶ他はありません。ただ実際にシミュレーションに用いる事ができる**実用周期**または**使い得る周期**は $p - 1$ ではありません。奇素数の法 $d = p$ の乗算合同法 (p, z, n) 乱数生成機構は既約剰余類群 $Z_p{}^* = \{1, 2, \cdots, p - 1\}$ のすべての数を巡回しますが、$T := p - 1$ は偶数で、任意の法 p の原始根 z に対して $\zeta :\equiv z^{T/2}$ は方程式 $\zeta^2 \equiv 1 \pmod p$ を満たします。移項し因数分解すれば、

$$\zeta^2 - 1 = (\zeta + 1)(\zeta - 1) \equiv 0 \pmod p,$$

即ち $\zeta \equiv \mp 1 \pmod p$ です。ζ は巡回列の途中で $\zeta \not\equiv 1$ だから $\zeta := z^{T/2} \equiv -1 \equiv p - 1 \pmod p$ となります。この後の巡回列は前半の列にマイナスを付けたもので、前半と独立とは言えません。だから一様独立な乱数の見本列として使える**実用周期**或いは**使い得る周期**は原始根の半位数 $T/2$ の部分だけです。この事実は後に、SG 素数の法 p に関しては原始根のマイナスであって原始根ではない場合の $z = 2$ も (p, z) 乱数生成機構の乗数を生成する最小のものとして有用な場合を与える、という事に触れておきます。[20]

2. 2. オイラーの関数と合成数の法、孫子の定理

情報数学などを学生時代に学ばれた読者には少し緩いでしょうが、物理関係を学ばれ、シミュレーションを用いて研究をなさろうという科学者、技術者には必要と思うので、群からさらに少しの遠出をします。既に仄めかした所から、大きな素数の法と原始根の乗算合同法生成機構 (p, z, n) で優れた統計性を

[20] **実用周期**は、厳格な意味の 1 つのシミュレーションに使う事のできる乱数の最大周期です。MC 乱数生成機構は実用周期 T を越えても乱数生成を続けます。新しいシミュレーションプログラムなら。次の T 以内で動かしてもよいのです。心配は、長大なコンピュータゲームで『支障なく動く』事を悪用される事です。後に我々が提示する MC 乱数の実用周期は長大で、その心配は殆どないと思いますが。

持つものが発見できるなら、以下は必要ない、とも感じられるかも知れません。しかし現実技術の世界は厳しく、合成数の法を援用しないと計算可能性が閉ざされます; 次章の検定の議論です。今最も緊要なのは合成数の法、それも $d = p_1p_2$ の 2 つの素数の積の形、をうまく捌く事です。必要になるのはまず、ユークリッドの互除法の幾つかの結論です。中学数学で学んだ議論は初等的ですが端的ではない面があり、以下それを避けます。

2 つの正の整数 m, n を取りその整数係数 1 次結合が作る整数の集まりを考えます。この舞台だけで次の驚くべき事柄が見えます：

補題 14.（最大公約数の定義） 2 つの正整数 m, n の整数係数 1 次結合の集合 S を考える、

$$S := \{Mm + Nn |\ M, N \text{ はすべての整数を動く }\}.$$

集合 S の[21] 正で最小の整数を a とすると、S は a の整数倍からなる集合であり、a は m, n の最大公約数 $a = (m, n)$ である:

$$S = \{ka |\ k = 0, \pm 1, \pm 2, \cdots\}.$$

（証明） まず S には $m = 1 \cdot m + 0 \cdot n$ と $n = 0 \cdot m + 1 \cdot n$ が含まれる事に注意します。S に所属する正の最小整数 a が $a = Mm + Nn$ の形である、と仮定し、S の任意の数 $x = M'm + N'n$ を a で割る整数割り算の商を q、余りを r とすれば、割り算の等式は $x = qa + r,\ 0 \leq r < a$ です。これは次を意味します：

$$0 \leq r = x - qa = (M' - qM)m + (N' - qN)n \in S, \quad 0 \leq r < a.$$

a が S の正で最小の整数ですから $r = 0$, つまり S の任意の数 x は a で割り切れます。これらは a が m と n の公約数で、m と n の最大公約数[22]$h = (m, n)$ に対して $a \leq h$ を満たす事を意味します。一方で m, n の最大公約数 $h = (m, n)$ は $a = Mm + Nn$ を割り切るから $a \geq h$ であり、$a = (m, n)$ です。 ■

これがユークリッドの互除法の結論です:

定理 15.（ユークリッドの互除法） 任意の 2 つの正整数 m, n の最大公約数 (m, n) は整数の組 M と N によって $(m, n) = Mm + Nn$ と[23]表される。

（定理 15 終り）

漸くガウスの定理、『整数 $x > 2$ の素因数分解の一意性』を議論できる眺望を得ます。

---

[21] ここでのテーマは『整数環』の中の『単項イデアル』です。立派な名前は必要ではありませんが。

[22] 最大公約数の記号 (m, n) は少し紛らわしいですが端的で便利なので使います。

[23] 整数 M, N は一意ではありません。$M'm + N'n = 0$ となる整数 M', N' は例えば $M' = n,\ N' = -m$ など無数にあり、$1 \equiv (M + M')m + (N + N')n \equiv \cdots$ も成り立ちます。

(正の整数の一意素因数分解定理) 整数 $x \geq 2$ の素因数分解を $x = p_1 p_2 \cdots p_s$ とする。この分解は素数 $p_1, p_2, \cdots, p_s$ の順序を除いて一意である。
(証明) 最初に次の補題を考えます。

(補題) 正の整数 a, b が互いに素、即ち最大公約数 $(a, b) = 1$ である、或いは共通素因数を持たない場合、を考える。このとき積 $x = ab$ を割り切る素数 $p > 0$ は a か b か、或いは両方か、を割り切る。
(補題の証明) 仮定から $x = ab$ は素数 p で割り切られます。もし p が a を割り切れば補題は成り立ちます。そうではないなら、p の約数は 1 と p だけだから p と a とは素、故にユークリッドの互除法の結論から整数 P と A とがあって

$$Pp + Aa = 1$$

が成り立ちます。これは $b = Pbp + Aab$ であり、ab は p で割り切られるのだから、b が p で割り切れます。 **(補題の証明終り)**

(一意素因数分解定理のガウスの証明) 正の整数 a の 2 通りの素因数分解、

$$a = {p_1}^{m_1} {p_2}^{m_2} \cdots {p_s}^{m_s} = {q_1}^{n_1} {q_2}^{n_2} \cdots {q_t}^{n_t}$$

があるとします。上の補題から素数 p_1 は a の任意の素因数分解を割り切り、その結果問題はどの素因数分解にでも同じ素因数 p_1 がある、それは割って除いて次の a_1 を考えればよくなります:

$$a_1 = {p_1}^{m_1 - 1} {p_2}^{m_2} \cdots {p_s}^{m_s}.$$

$m_1 - 1 \geq 0$ のどの場合であっても元々の素因数分解から一つずつ素因数を減らし、『どんな素因数分解も同数 $s = t$ の同じ素因数の集まりである』、『a の素因数分解は一意の形である』という結論で議論は終ります。 ■

整数の一意素因数分解定理は沢山の構造を保障します。

定理 2 つの整数 a, b の素因数分解 (存在しない素因数は 0 乗と表して)

$$a = {p_1}^{m_1} {p_2}^{m_2} \cdots {p_s}^{m_s}, \quad b = {p_1}^{n_1} {p_2}^{n_2} \cdots {p_s}^{n_s}$$

と記す。素因数分解の一意性から次が成り立つ:

$$\begin{aligned} \text{最大公約数 (GCD)} = (a, b) &= {p_1}^{\min(m_1, n_1)} {p_2}^{\min(m_2, n_2)} \cdots {p_s}^{\min(m_s, n_s)}, \\ \text{最小公倍数 (LCM)} &= {p_1}^{\max(m_1, n_1)} {p_2}^{\max(m_2, n_2)} \cdots {p_s}^{\max(m_s, n_s)}. \end{aligned}$$

(証明) 明らかです。 ■

2. 3. 孫子の定理

次のテーマは孫子[24]の定理です。合成数の法の構造理解と応用に不可欠です。

定理 16.（孫子の定理）

(A) 2 つの互いに素な正の整数 d_1, d_2 と任意の 2 つの整数 x_1, x_2 に対して、連立合同式、

$$x \equiv x_1 \pmod{d_1}, \quad x \equiv x_2 \pmod{d_2}$$

は整数 x を法 $d = d_1 d_2$ で一意に定める。

(B) 既約剰余類群 ${Z_d}^*$ の元 x と、既約剰余類群 ${Z_{d_1}}^*$ の元 $x_1 \equiv x \pmod{d_1}$ 及び既約剰余類群 ${Z_{d_2}}^*$ の元 $x_2 \equiv x \pmod{d_2}$ の対 (x_1, x_2) とは 1 対 1 に対応する。

(C) 既約剰余類群 ${Z_d}^*$ の元の数を $\phi(d) = \sharp {Z_d}^*$ と記してオイラーの関数と言う。互いに素な正の整数 d_1 と d_2 に対して、オイラーの関数は『乗法性』を持つ:

$$\phi(d_1 d_2) = \phi(d_1)\phi(d_2).$$

（証明）(A) d_1 と d_2 は共通素因数が無く互いに素、最大公約数は $(d_1, d_2) = 1$ であり、ユークリッドの互除法**定理 15** の**等式** $D_1 d_1 + D_2 d_2 = 1$ を満たす整数 D_1, D_2 が存在します。この**等式**を法 d_1 や d_2 で見れば次が成り立ちます:

$${D_2 \equiv {d_2}^{-1} \pmod{d_1}}, \quad {D_1 \equiv {d_1}^{-1} \pmod{d_2}}.$$

整数 $X := D_2 d_2 x_1 + D_1 d_1 x_2$ を定義すると[25] X が与えられた連立合同式の解と直ちに見通せます。他の解 X' があるなら、それも法 d_1, d_2 のどちらでも同じ x_1, x_2 だから、差 $X - X'$ はどちらの法でも 0、互いに素な d_1 と d_2 それぞれの倍数、つまり $d = d_1 d_2$ の倍数で $X - X'$ は法 d で 0、法 d では同じもので、連立合同式の解は法 d で一意です。

(B) 上の **(A)** から既約剰余類群 ${Z_{d_1}}^*$ の任意の元 $x_1 \not\equiv 0 \pmod{d_1}$ 及び既約剰余類群 ${Z_{d_2}}^*$ の任意の元 $x_2 \not\equiv 0 \pmod{d_1}$ の対 (x_1, x_2) は法 $d = d_1 d_2$ での 1 つの整数 X に対応[26]し、$k = 1, 2$ のどちらでも 0 に合同ではありません。だから互いに素な d_1 の倍数でも d_2 の倍数でもない、つまり $d = d_1 d_2$ の倍数ではなく d とは素、$X \in {Z_d}^*$ です。逆に任意の $X \in {Z_d}^*$ は法 d_1 で見て $x_1 \in {Z_{d_1}}^*$ であり法 d_2 でも同様に $x_2 \in {Z_{d_2}}^*$ です。これは ${Z_d}^*$ の任意の元 X と、${Z_{d_1}}^*$ の元 x_1 と $x_2 \in {Z_{d_2}}^*$ との対 (x_1, x_2) と、の間の 1 対 1 対応を証明しています。

(C) 上の **(B)** によって、$d_1 > 0$ と $d_2 > 0$ が素なら $\sharp {Z_{d1}}^* \times \sharp {Z_{d_2}}^* = \sharp {Z_{d_1 d_2}}^*$ が成り立ちます。これがオイラーの関数の乗法性、

---

[24] 中国南北朝時代 439-589 の算術書『孫子算経』の著者 Sunzi です。

[25] この形は $X := \{D_1 d_1 D_2 d_2/(D_1 d_1)\}x_1 + \{D_1 d_1 D_2 d_2/(D_2 d_2)\}x_2$ だと考えると d が 3 個以上の互いに素な数の積の場合にも使える事が分かります。

[26] **(A)** では x_1, x_2 はそれぞれの法で 0 に合同でもよかったのに対し、**(B)** では x_2, x_2 のどちらもそれぞれの法で 0 ではない場合を考えています。

$$\text{整数 } d_1 > 0 \text{ と } d_2 > 0 \text{ が素なら} \phi(d_1 d_2) = \phi(d_1)\phi(d_2)$$

の成立です。 ■

今や任意の法の整数 $d > 0$ に対する既約剰余類群 ${Z_d}^*$ の元の数、オイラーの関数の値を計算できます。$p = 1$ は素数ではないが、法 $p = 1$ ではすべての整数は合同で、整数全体が 1 つの既約剰余類 $\{1\}$ ですから $\phi(1) = \sharp\{1\} = 1$ とします。素数 $p \geq 2$ については、$\phi(2) = \sharp\{1\} = 1$、$\phi(3) = \sharp\{1, 2\} = 2$、$\phi(5) = \sharp\{1, 2, 3, 4\} = 4$、$\cdots$ です。一般に素数 $p \geq 2$ と素な整数は $\{1, 2, \cdots, p-1\}$ の $p - 1$ 個であって:

定理 17.（オイラーの関数） 整数 $d \geq 2$ の素因数分解を $d = ab \cdots f$ とすると

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

が法 d での同値類の総数 $\phi(d)$ である。 **（定理 17 終り）**

孫子の定理で触れた互いに素な因子からなる法 $d_1 d_2$ を持つ既約剰余類群 ${Z_{d_1 d_2}}^*$ と『直積群』と呼ばれる『${Z_{d_1}}^*$ の元と ${Z_{d_2}}^*$ の元を 2 成分とするいわばベクトルの群』との 1 対 1 対応は『群の同型』という考え方に昇華されますが、以下にはオイラーの関数だけで十分なので触れません。ただ 5 世紀の古い時期に、直積群に達する知識が得られていた事は感動的です。

乗算合同法は既約剰余類群の中で巡回部分群を利用するものです。その特性の中で設計が容易なのは周期構造で、できるだけ大きな周期のものを取る技術原則から言えば、大きな奇素数の法とその原始根乗数か、あるいは異なる奇素数の法を 2 つ組み合わせて出来るだけ大きな周期となる孫子の定理を用いる組み合わせか、以外には実際技術的な方策はありません。だから複雑な構造の既約剰余類群にはあまり技術的関心はないので、これからは優れた乗算合同法乱数生成機構を選ぶ手段、検定の実際に力を向けます。検定は乱数理論、乱数技術での最大の乗り越えるべき困難です。

進む前に、2 つの正の互いに素な奇素数の積[27]を法とする MC 乱数の周期を考えておきます。既に述べた様に、奇素数の法 p と原始根乗数で優れた MC 乱数生成機構が見出されれば言う事はないのですが、十分長い周期を素数 p の法の $p - 1$ に求めると p は巨大になり、その原始根の数が多すぎて検定計算の収束が見えません。実際には、だから、低次の検定で見当をつけて見込み薄のものを除外した 2 つの奇素数の法と、原始根乗数、場合によっては原始根のマイナスでそれ自身は原始根ではない乗数も貪欲に利用せざるを得ません。正しい原理と、次の章で述べる正しい正単体検定基準と、の発見から数年を経た現在ても『未だ 2 個』という希少さが成功の現実です。この希少さを十分に御認識下さい。

[27]前にも触れた通り 2 の冪と奇整数とを含む法は考えるべきではありません。

第3章　乗算合同法と格子

3. 1. 乗算合同 MC 法生成機構 (d, z) に伴われる格子

MC 生成機構 (d, z, n)、詳しくは非負の法の整数 d、d とは素、共通素因数のない整数の乗数 $z > 0$, そして d とは素な整数の初期値 $n > 0$ の 3 つ組、が生成する整数列は、

$$\{X_j \equiv nz^j \pmod d |\ j = 0, 1, 2, \cdots,\ 0 < n_j < d\}$$

です。法 d で同値なすべての整数を考えている、と示すのが記号 $(\mathrm{mod}\ d)$ の意味でした。[28] n は d とは素な任意の整数の『種 seed』で、乱数の出発値を選ぶだけ、どの初期値 n でも出力『周期列』は同じだから n は列全体の統計的性質の検定で考える必要はありません。$\{v_j = X_j/d |\ j = 0, 1, 2, \cdots\}$ が出力一様 (有理数) 乱数列です。

大切なのは相続く l 個の出力

$$S_j = (nz^j, nz^{j+1}, \cdots, nz^{j+l-1}) \pmod d, \quad j = 0, 1, 2, \cdots$$

を l 次元ユークリッド空間の中で法 d で座標が合同な (行) ベクトル達と見る、$j = 0, 1, 2, \cdots$ の変化が l 次元ユークリッド空間 R_l の無限個の格子点列の位置の進行と見る視点です。『格子』像は導入したベクトルの成分に $\mathrm{mod} d$ を施す操作を、幾何学的視覚的に考える事を可能にします。『法 d で合同な整数を全部同時に考える』見方です。

再説明します。整数 A と B が法 d の整数倍の違いしかない事、等式

$$A - B = \alpha d, \quad A = B + \alpha d$$

がある整数 α について成り立つ事[29]を『整数 A と B は法 d で合同』と言いました。そして l 次元ユークリッド空間の 2 点 (或いは 2 つの位置行ベクトル) の

[28] 短気に、それではやってられない、$0 \le X < d$ の一意の整数を取る、と指示するには

$$\{X_j = \mathrm{mod}(nz^j\, d) |\ j = 0, 1, 2, \cdots\}$$

とします。この章ではこの立場はとらない方の利点を利用します。ついでながら、計算諸言語の関数 $\mathrm{mod}(A,\, d)$ は、非負の整数 $A \ge 0$ を法の整数 $d > 0$ で割り、商は非負整数 $Q \ge 0$、として余りの整数 $R \ge 0$、

$$A = Qd + R, \quad R = A - Qd = \mathrm{mod}(A,\, d) \ge 0$$

を定義としました。

[29] この、『値はどうでもよい』整数をギリシャ文字で宛てるのは便利です。以後説明なしで多用します。

座標がそれぞれ法 d で合同なとき、『2 点は法 d で合同』、と言いましょう。この様に幾何学と対応付けると l 次元ユークリッド空間 R_l の 1 つの (整数座標の) 点 $(a_1, a_2, \cdots, a_l)$ は無数の点

$$(a_1 + \alpha_1 d, a_2 + \alpha_2 d, \cdots, a_l + \alpha_l d), \quad (\alpha_1 \text{ から } \alpha_l \text{ は任意の整数})$$

と『法 d で合同』と言う事ができます。幾何学的にユークリッド空間の 2 点の座標が法 d で合同のとき、『2 点は法 d で合同』と短く言うのです。[30]

MC 法乱数に関係した次の l 個の位置行ベクトルを定義します:

$$\begin{aligned}
\boldsymbol{e}_1 : &= (1, z, z^2, \cdots, z^{l-2}, z^{l-1}) \\
\boldsymbol{e}_2 : &= (0, d, 0, 0, \cdots, 0, 0) \\
\boldsymbol{e}_3 : &= (0, 0, d, 0, \cdots, 0, 0) \\
&\cdots\cdots\cdots\cdots \\
\boldsymbol{e}_{l-1} : &= (0, 0, 0, 0, \cdots, d, 0) \\
\boldsymbol{e}_l : &= (0, 0, 0, 0, \cdots, 0, d)
\end{aligned}$$

ここでは MC 乱数に関係して、R_l の中の整数座標の点だけを考えます。MC 乱数からの相続く l 個の座標を持つ点

$$(a_1 + \alpha_1 d, a_2 + \alpha_2 d, \cdots, a_l + \alpha_l d), \quad (\alpha_1 \text{ から } \alpha_l \text{ は整数})$$

を全空間 R_l に法 d で合同な座標を持って散らばらせるのです。乱数問題としての考察ではすべて位置ベクトル $n\boldsymbol{e}_1$ を空間 R_l から各座標軸方向に法 d で引き戻して、原点から発する 1 つの稜の長さ d の超立方体の中にある、と考えてもよいのですが、合同算法での引き戻しは議論の間には行わない方が計算構造や論理構造が見易いので、あからさまには記しません。この様な考え方と表記法、特に原点から発する超立方体ではなく全空間に存在する点の座標と見る事、そして法 d で合同な点の全体、格子で考える事、の大利点を我々はこれから様々に経験します。

まず次の事柄に触れます。空間の点の位置ベクトルの第 2 から第 l 座標軸方向の法 d での引き戻しや移動はベクトル $\boldsymbol{e}_2$ から $\boldsymbol{e}_l$ の整数倍を加えて実現できます。第 1 軸方向には、

$$(d, 0, 0, \cdots, 0, 0) = d\boldsymbol{e}_1 - z\boldsymbol{e}_2 - z^2\boldsymbol{e}_3 - \cdots - z^{l-2}\boldsymbol{e}_{l-1} - z^{l-1}\boldsymbol{e}_l$$

の整数倍を用いればよろしい。だから、空間 R_l で出力列 S_j の点と法 d で合同なすべての点は位置行ベクトルの組 $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ の整数係数 1 次結合で表

[30] 空間 R_l を各座標方向に周期 d のトーラスと考えてもよいのですが、高次元空間のトーラスのイメージに悩むよりは座標の合同と思う方が楽でしょう。

され[31]ます。この事は、S_l の点と、それに法 d で合同な点達とは基ベクトルの組 $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ が張る格子の上にある、格子の上に座席を取る、という事です。

ある格子は無数の基ベクトルの組を持ちます。簡単のため平面 R_2 の格子を取り、我々はこの格子点の集まりからどの様に格子ベクトルを得るか、を考えます。もし R_2 の中の直線の上に 2 つの格子点があるなら、我々はその直線を『格子線』と呼びます。実際は格子線上には無数の格子点が載っています。この格子線上で隣り合う 2 つの格子点 O と A を任意に取り、第 1 の基ベクトルを $\boldsymbol{e}_1 := \overrightarrow{\mathrm{OA}}$ と定義します。次にこれと平行で隣接する格子線[32]を取り、その上の任意の格子点 B を取って $\boldsymbol{e}_2 := \overrightarrow{\mathrm{OB}}$ と定義すると 2 ベクトル $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ はこの格子の基ベクトルの 1 組になります。これらベクトルの張る平行 4 辺形はその内部にも頂点を除く辺上にも格子点を持ちません。この平行 4 辺形をその頂点 O が各格子点を動くように平行移動すれば、全格子平面が隙間も重複もなく埋め尽くされます。これは格子の基ベクトルの整数倍を平行 4 辺形に加えれば、全格子点が掃過 sweep される、という事です。元の $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ がどう選ばれてもこれらは確かにこの平面格子の基ベクトルの組で、平行 4 辺形の面積は基ベクトルの取り方によらず一定です。

この結論はユニバーサルです。2 次元 (d, z) 格子は $\{(1, z),\ (0, d)\}$ を基ベクトルの 1 組としますから、これらが作る行列式の絶対値から、(d, z) の基ベクトルの張る平行 4 辺形の一定面積は d です。この様な MC 格子の 2 次元の状況は、第 1 章第 2 ページの第 1 図の右で見た様に容易に視覚で直観的に観察する事ができます。

今度は空間 R_3 の中の格子を考えます。R_3 の中の平面が 1 直線上にない 3 つの格子点を含むなら『格子平面』と呼びます；勿論その上には無数の格子点が載っていて、それ自体 2 次元格子を作っています。この 2 次元格子の基ベクトルの組は上と同様に 3 つの格子点 O, A, B を取って $\{\boldsymbol{e}_1 = \overrightarrow{\mathrm{OA}}, \boldsymbol{e}_2 = \overrightarrow{\mathrm{OB}}\}$ と作られます。3 次元格子の中で先の 2 次元格子平面と平行で隣り合う今 1 つの 2 次元格子平面を取り、その上の任意の格子点 C を取って 3 つのベクトル、

$$\{\boldsymbol{e}_1 = \overrightarrow{\mathrm{OA}},\quad \boldsymbol{e}_2 = \overrightarrow{\mathrm{OB}},\quad \boldsymbol{e}_3 = \overrightarrow{\mathrm{OC}}\}$$

を作れば、これが 3 次元格子の基ベクトルの 1 組です。特に (d, z) 生成機構からの $l = 3$ 連に対する基ベクトルの組、

$$\boldsymbol{e}_1 = (1, z, z^2),\quad \boldsymbol{e}_2 = (0, d, 0),\quad \boldsymbol{e}_3 = (0, 0, d)$$

[31]正確には位置行ベクトルの組 $\{e_1, e_2, \cdots, e_l\}$ の整数係数の 1 次結合になります。但しすべての整数係数 1 次結合ではありません。座標が d の倍数、d と素ではないもの、典型的には原点、は S_j の点と合同な点のものではありません。用語としては『格子』と言う時にはこの様な欠損のないもの、『格子を作るベクトル（基ベクトル）の**すべての**整数係数 1 次結合』を考えると約束します。

[32]即ち第 1 の直線と平行で間に格子点が存在しないもの。

は自明な行列式 d^2 を与え、この 3 次元格子の基ベクトルの組はつねに体積 d^2 を張る、と分かります。

3 次元以上の幾何学状況の図示は困難になりますが、言葉としては、或いは概念的には次元 l を高めながら続ける事が可能です。現在の乱数では $l = 6$ までを問題と[33]します。ここに述べた諸結論は一般の格子についてと考えてよいのですが、イメージを見難くしないため (d, z) 格子として定理に纏めます。

定理 18.（乗算合同法 (d, z) 格子の基ベクトルとユニモジュラー変換）
(A) 乗算合同法 (d, z) 生成機構からの相続く乱数の l 連、$l \geq 2$、は l 次元ユークリッド空間 R_l の d と z で定まる格子 $L_l(d, z)$ に座席を取る。基ベクトルの 1 組は

$$\begin{aligned}
\boldsymbol{e}_1 : &= (1, z, z^2, \cdots, z^{l-2}, z^{l-1}) \\
\boldsymbol{e}_2 : &= (0, d, 0, 0, \cdots, 0, 0) \\
\boldsymbol{e}_3 : &= (0, 0, d, 0, \cdots, 0, 0) \\
&\cdots\cdots\cdots\cdots \\
\boldsymbol{e}_{l-1} : &= (0, 0, 0, 0, \cdots, d, 0) \\
\boldsymbol{e}_l : &= (0, 0, 0, 0, \cdots, 0, d)
\end{aligned}$$

で与えられる。これらを行ベクトルとする $l \times l$ 行列 $E_l(d, z)$ を『l 次の (d, z) 基行列』と[34]呼ぶ。その行列式の絶対値は $|\det E_l(d, z)| = d^{l-1}$ である。
(B) $l \times l$ 整数行列 U_l が行列式 $\det U_l = \pm 1$ のとき『U_l はユニモジのュラー行列である』と言う。(d, z) 格子 $L_l(d, z)$ のすべての基行列はその 1 つの $E_l(d, z)$ 基行列にすべての $l \times l$ ユニモジュラー行列 U_l を掛けて得られる。
（証明） この証明や以下の要所で誤解を招かなければ、基 (d, z) 行列 $E_l(d, z)$ 等は (d, z) を、場合によっては次元数 l も、省いて簡明に記す約束にします。
(A) 基ベクトルの形と (d, z) 生成機構からの相続く l 連出力の点が 基行列 $E_l(d, z)$ の行ベクトルの d とは素な整数を係数とする 1 次結合で表される事、それら行ベクトルのすべての整数係数 1 次結合である格子 $L_l(d, z)$ の格子点に座席を取る事、は既に構成で見ました。$E_l(d, z)$ の形から行列式は自明です。
(B) 格子 L_l の基ベクトルの組の多意性は与えられた格子の基ベクトルの取り方で触れました。$E_l(d, z)$ の他の基行ベクトルの組 $\{\boldsymbol{e}_1', \boldsymbol{e}_2', \cdots, \boldsymbol{e}_l'\}$ がある、と考えると、これらも $E_l(d, z)$ の格子ベクトルだから元の基行ベクトルの整数係

[33] これは計算可能な時間の問題、コンピュータ速度の問題です。乗算合同法がコンピュータ上の任意の一様乱数を表せる事実からは新原理の超高速計算機の実現がより高次元まで優れた乱数を与えるだろうと期待されます。
[34] 別の基ベクトルの組で作る場合も含めて基行列と呼ぶ事にします。

数 $\{u_{jk}\}$ による 1 次結合で表されます：

$$\begin{aligned}
\boldsymbol{e}_1{}' &= u_{11}\boldsymbol{e}_1 + u_{12}\boldsymbol{e}_2 + \cdots + u_{1l}\boldsymbol{e}_l, \\
\boldsymbol{e}_2{}' &= u_{21}\boldsymbol{e}_1 + u_{22}\boldsymbol{e}_2 + \cdots + u_{2l}\boldsymbol{e}_l, \\
&\cdots\cdots\cdots\cdots\cdots, \\
\boldsymbol{e}_l{}' &= u_{l1}\boldsymbol{e}_1 + u_{l2}\boldsymbol{e}_2 + \cdots + u_{ll}\boldsymbol{e}_l.
\end{aligned}$$

簡略化した行列表現を導入します:

$$E_l := \begin{pmatrix} \boldsymbol{e}_1 \\ \boldsymbol{e}_2 \\ \cdots \\ \boldsymbol{e}_l \end{pmatrix}, \quad E_l{}' := \begin{pmatrix} \boldsymbol{e}_1{}' \\ \boldsymbol{e}_2{}' \\ \cdots \\ \boldsymbol{e}_l{}' \end{pmatrix}, \quad U_l := \begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1l} \\ u_{21} & u_{22} & \cdots & u_{2l} \\ \cdots & \cdots & \cdots & \cdots \\ u_{l1} & u_{l2} & \cdots & u_{ll} \end{pmatrix}.$$

これで関係はコンパクトに $E_l{}' = U_l E_l$ と書かれます。行列積の行列式を取って $|\det E_l{}'| = |\det U_l| \cdot |\det E_l|$ です。体積の不変の関係 $|\det E_l| = |\det E_l{}'|$ は既知だから $|\det U_l| = 1$、U_l は $\det U_l = \pm 1$ のユニモジュラー行列です。 ■

ここで考えている格子は最も単純な格子で、結晶物理学などの精緻複雑な構造の結晶格子とは違います。それでも確認すべき事は沢山あります。一般論は避けますが、**定理 18 (B)** の証明の議論は (d, z) 格子 $L_l(d, z)$ に限らず空間 E_l の中で $l \times l$ 基行列 A を持つ任意の格子について成り立つ事を注意します。

3. 2. スペクトル検定のための格子の双対基ベクトルと双対格子

MC(d, z) 生成機構からの相続く l 連の張る格子で基ベクトルの任意の 1 組 $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ を取り、l 次元（行）ベクトルの組 $\{\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_l\}$ を次の内積関係（直交関係）で定義します：

$$(\boldsymbol{e}_j, \boldsymbol{f}_k) = \delta_{jk}.$$

上で $(\boldsymbol{e}_j, \boldsymbol{f}_k)$ はベクトルの内積です。行列 A の転置を ${}^tA$、逆行列を A^{-1}、単位行列を I と記し、基行ベクトルを行とする行列形で、これは端的な形にまとめられます：

$$E := \begin{pmatrix} \boldsymbol{e}_1 \\ \boldsymbol{e}_2 \\ \cdots \\ \boldsymbol{e}_l \end{pmatrix}, \quad F := \begin{pmatrix} \boldsymbol{f}_1 \\ \boldsymbol{f}_2 \\ \cdots \\ \boldsymbol{f}_l \end{pmatrix},$$

$$dI = E\,{}^tF = F\,{}^tE, \quad F = d\,({}^tE)^{-1} = d\,{}^t(E^{-1}).$$

F を双対基行列と呼びます。$\det dI = d^l$ から F の行列式は次元 l に依存しません：

$$|\det(F\,{}^tE)| = |\det F| \cdot |\det\,{}^tE| = d^l, \quad |\det F| = d.$$

F の具体形を見ましょう。

補題 19. (d, z) 乱数生成機構に伴われる l 次元格子の基ベクトル、

$$\begin{aligned}
\boldsymbol{e}_1 : &= (1, z, z^2, \cdots, z^{l-2}, z^{l-1}),\\
\boldsymbol{e}_2 : &= (0, d, 0, 0, \cdots, 0, 0),\\
\boldsymbol{e}_3 : &= (0, 0, d, 0, \cdots, 0, 0),\\
&\cdots\cdots\cdots\cdots,\\
\boldsymbol{e}_{l-1} : &= (0, 0, 0, 0, \cdots, d, 0),\\
\boldsymbol{e}_l : &= (0, 0, 0, 0, \cdots, 0, d),
\end{aligned}$$

に対応する双対格子の基ベクトルは**整数成分**であって、次の通り：

$$\begin{aligned}
\boldsymbol{f}_1 : &= (d, 0, 0, 0, \cdots, 0, 0),\\
\boldsymbol{f}_2 : &= (-z, 1, 0, 0, \cdots, 0, 0),\\
\boldsymbol{f}_3 : &= (-z^2, 0, 1, 0. \cdots, 0, 0),\\
&\cdots\cdots\cdots\cdots,\\
\boldsymbol{f}_{l-1} : &= (-z^{l-2}, 0, 0, 0, \cdots, 1, 0),\\
\boldsymbol{f}_l : &= (-z^{l-1}, 0, 0, 0, \cdots, 0, 1).
\end{aligned}$$

（証明） 内積を取れば $(\boldsymbol{e}_j, \boldsymbol{f}_k) = d\delta_{jk}$ は明らかです。 ■

基行列 E のユニモジュラー変換 $E' := UE$ を考えると $E = U^{-1}E'$ です。双対基行列 F に関する方程式を E' で書けば、

$$dI = F\,{}^tE = F\,{}^t(U^{-1}E') = F\,{}^tE'\,{}^t(U^{-1}).$$

両側を ${}^t(U^{-1})$ と ${}^tU$ で挟んで次が成り立ちます：

$$dI = F'\,{}^t(E'), \quad F' := {}^t(U^{-1})F.$$

これは重要な対応を意味します。

補題 20. （双対 (d, z) 格子）

(A) (d,z) 乱数の相続く l 連が空間 R_l で定める整数 (d,z) 格子 $L := L_l(d,z)$ の任意の整数基 (d,z) 行列 $E_l(d,z)$ に対する双対基 (d,z) 行列 $F_l(d,z)$ は整数成分で、次で定義される：

$$F_l(d,z) = d\,{}^t\{E_l(d,z)^{-1}\}, \quad |\det F_l(d,z)| = d,$$

$F_l(d,z)$ の行ベクトルが 1 次独立な基として R_l に作る整数格子を**双対** (d,z) **格子** ${L_l}^*(d,z)$ と名付ける。

(B) 基 (d,z) 整数行列 $E_l(d,z) = E$ のユニモジュラー行列 $U_l = U$ によるユニモジュラー変換を $E' := UE$ とすると、E' に対する双対基 (d,z) 整数行列 F' はユニモジュラー行列 $U^* := {}^t(U^{-1})$ による F のユニモジュラー変換 $F' = U^*F$ である。

(C) 任意の基 (d,z) 整数行列 E に対する双対基ベクトルが整数行ベクトルとして作る行列 F は双対 (d,z) 格子 $L^* := {L_l}^*(d,z)$ の基整数行列であり、格子 L と双対格子 L^* とはそれらの基 (d,z) 整数行列と双対基 (d,z) 整数行列との間に 1 対 1 の対応を持つ。従って (d,z) 格子 L のすべての l 次基整数行列 $E_l(d,z)$ の掃過は、(d,z) 双対格子 L^* のすべての l 次双対基整数行列 $F_l(d,z)$ の掃過に対応する。

（証明） **(A)** 関係 $dI = F\,{}^tE$ の行列式は $d^l = |\det F| \cdot |\det {}^tE|$ を与え、一方 $\det E = \pm d^{l-1}$ だから $|\det F| = d$ を得ます。だから F は正則行列でその行ベクトルは 1 次独立、ユニバーサルなユニモジュラー行列と共に基ベクトルとして (双対) 格子 $L^* = {L_l}^*(d,z)$ を作ります。

(B) 基 $E = E_l(d,z)$ 行列とその双対 (d,z) 行列 $F = F_l(d,z) = d\,{}^t(E^{-1})$ について、E のユニモジュラー変換である $E' = UE$ に対応する双対基行列を F' と置くと、

$$\begin{aligned} F' : \ &= d\,{}^t\{(E')^{-1}\} = d\,{}^t\{(UE)^{-1}\} = d\,{}^t(E^{-1}U^{-1}) \\ &= ({}^t\{U^{-1}\})(d\,{}^t\{E^{-1}\}) = {}^t\{U^{-1}\}F \end{aligned}$$

です。整数成分のユニモジュラー行列 U は $\det U = \pm 1$ だから正則で、逆行列の余因子による公式は U^{-1} も整数行列で $\det U^{-1} = 1/\det U = \pm 1$ であると証明します。故に $U^* := {}^t(U^{-1})$ もユニモジュラー行列です。これは基行列 E の U によるユニモジュラー変換には対応する双対基行列 F の $U^* = {}^t(U^{-1})$ によるユニモジュラー変換が対応する事を証明します。

(C) U と U^* の対応も 1 対 1 ですから、格子の基ベクトルとそのユニモジュラー変換の全体を取る事は対応する双対基ベクトルとそのユニモジュラー変換の全体を取る事です。言葉を変えるなら、格子 $L_l(d,z)$ の基ベクトルの作る量のすべての基ベクトルに関する探索を行う事は、その量を双対格子 ${L_l}^*$ の対応する双対基ベクトルで表してすべての双対基ベクトルにわたる探索をする事と同じです。 ■

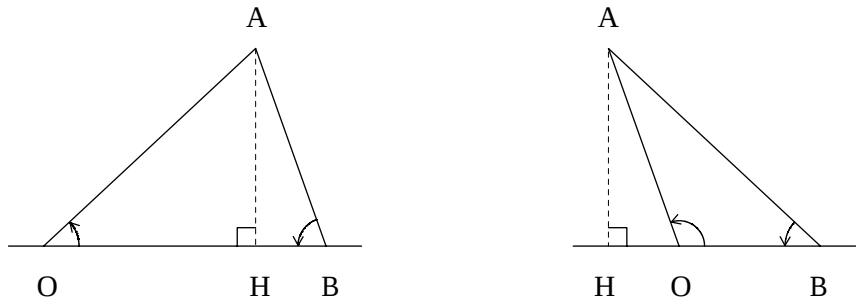
この **(C)** の事実はスペクトル検定で用いられます。

3. 3. 乱数生成機構 (d, z) 格子のスペクトル検定

スペクトル検定は Fishman と Moore の 1986 年の研究[35]で最初に現実的な応用がなされたと思います。難しいテーマで、現在でも乱数を使われる科学者、技術者に理解が十分行きわたっていると思われません。見やすい 2 次の場合から議論を始めます。

2 次元平面 R_2 を取り、基ベクトル $\boldsymbol{e}_1 = \overrightarrow{\mathrm{OA}}$ と $\boldsymbol{e}_2 = \overrightarrow{\mathrm{OB}}$ が張る 2 次元格子[36]を考え、その中の 3 点を図示します。これらベクトルはそれぞれに平行な無数の格子線と無数の格子平行 4 辺形を（勿論 ΔOAB も）定めています。点 O を

第 2 図　スペクトル検定の原理



(第 2 図終り)

通り $\boldsymbol{e}_2 = \overrightarrow{\mathrm{OB}}$ 方向の格子線と、点 A を通るそれに平行な格子線とはその間に格子点を含まず、平面 R_2 で隣接しています。前出の双対基ベクトル $\boldsymbol{f}_1$ は $\boldsymbol{e}_2$ とは直交し、$(\boldsymbol{e}_1, \boldsymbol{f}_1) = d$ だから $\overrightarrow{\mathrm{HA}}$ の方向です。だから頂点 A の $\overline{\mathrm{OB}}$ への高さ μ は

$$\mu = |(\boldsymbol{e}_1, \boldsymbol{f}_1)|/\|\boldsymbol{f}_1\| = d/\|\boldsymbol{f}_1\|, \quad \|\boldsymbol{f}_1\| \text{ はベクトル } \boldsymbol{f}_1 \text{ の長さ},$$

で与えられるのです。

得られた理解は端的な補題に纏められます。

補題 21.（乗算合同法乱数 (d, z) 生成機構の 2 次スペクトル検定）

MC 乱数生成機構 (d, z) からの相続く 2 連が 2 次元平面 R_2 で座席を取る 2 次元格子 $L_2(d, z)$ の最隣接平行格子線の最大間隔 ${\mu_2}^{\max}(d, z)$ は、2 次元双対 (d, z) 格子、${L_2}^*(d, z)$ の中で正で最短の長さを持つ双対格子ベクトル $\boldsymbol{f}_{\min}$ によって次の表現を持つ：

[35] p.14 の脚注 15 参照。

[36] 議論を (d, z) 格子に限る必要はありませんが、議論を他の量で複雑化する事を避けて、基ベクトルは行列式絶対値の面積 d、ΔOAB は面積 $d/2$ を張る、と仮定します。

$$\mu_2{}^{\max}(d,z) = d/\|\boldsymbol{f}_{\min}\|.$$

ここで $\|\boldsymbol{f}_{\min}\|$ は双対最短ベクトル $\boldsymbol{f}_{\min}$ のユークリッド長さである。

（証明） 2 次元 (d,z) 格子 $L_2(d,z)$ の任意の基ベクトル $\boldsymbol{e}_1$ について、今 1 つの基ベクトルに平行な格子線とそれに最隣接の格子線の間隔が $d/\|\boldsymbol{f}_1\|$ である事は見られました。同じ関係は $\boldsymbol{e}_1$ に平行な最隣接格子線間隔と $\boldsymbol{e}_2$ とについても、格子 $L_2(d,z)$ の他の任意の基ベクトルの組についても成り立ちます。故に 2 次元 (d,z) 格子 $L_2(d,z)$ のすべての平行隣接格子線の間隔の最大値は、双対 (d,z) 格子 $L_2{}^*(d,z)$ のすべての双対基ベクトルで最小の正の長さを持つもの $\boldsymbol{f}_{\min}$ の長さ $\|\boldsymbol{f}_{\min}\|$ で上の通り与えられます。（双対）格子の**基**ベクトルの長さの正の最小値が（双対）格子ベクトルの長さの正の最小値である事は一般の格子の基ベクトルの取り方、『任意格子線上の最短ベクトルを取って $\cdots$』を想起すれば自明です。 ■

直ちに乗算合同法 (d,z) 乱数生成機構の相続く l 連が空間 R_l で座席を占める格子 $L_l(d,z)$ の基格子ベクトルと双対基格子ベクトルに一般化されます。

定理 22.（乗算合同法乱数 (d,z) 生成機構の l 次スペクトル検定）

MC 乱数生成機構 (d,z) からの相続く l 連が空間 R_l で座席を取る l 次元格子 $L_l(d,z)$ の中の最隣接平行 $l-1$ 次元格子超平面の最大間隔 $\mu_l{}^{\max}(d,z)$ は、l 次元双対 (d,z) 格子の正で最短の長さを持つ（行）ベクトル $\boldsymbol{f}_{\min}$ によって次で与えられる：

$$\mu_l{}^{\max}(d,z) = d/\|\boldsymbol{f}_{\min}\|.$$

（証明） (d,z) 生成機構に伴われる l 次元格子 $L_l(d,z)$ の基ベクトルの任意の組が $\{\boldsymbol{e}_l = \overrightarrow{\mathrm{OA}_j}|\ j = 1,2,\cdots,l\}$ であり、それに対応する双対基行ベクトルの組が $\{\boldsymbol{f}_l|\ j = 1,2,\cdots,l\}$ であるとします。任意の基ベクトル、簡単のため $\boldsymbol{e}_1$ を取ります。このベクトルの終点 A_1 は残る $l-1$ 個の基ベクトルが張る $(l-1)$ 次格子超平面、即ち E_l 内の点集合、

$$\{c_2\overrightarrow{\mathrm{OA}_2} + c_3\overrightarrow{\mathrm{OA}_3} + \cdots + c_l\overrightarrow{\mathrm{OA}_l}|\ c_2, c_3, \cdots, c_l \text{ は}\textbf{実数}\}$$

に対面しています。超平面までの点 A_1 の高さを μ と記すと、双対基ベクトル $\boldsymbol{f}_1$ はこの超平面を張るすべてのベクトルと直交しますから、

$$\mu = |(\boldsymbol{e}_1, \boldsymbol{f}_1)|/\|\boldsymbol{f}_1\| = d/\|\boldsymbol{f}_1\|$$

となります。この関係は他の任意の基ベクトルとその双対基ベクトルについて、そして格子 $L_l(d,z)$ の他の任意の基ベクトルの組と双対基ベクトルの組について成り立ちます。自明に（双対）**基**ベクトルの正で最短のものは正で最短の（双対）格子ベクトルです。 ■

スペクトル検定は**定理 22** から、正の最短双対ベクトル $\boldsymbol{f}_{\min}$ を探索する問題

です。必要な (d,z) 双対ベクトルは一般に $\{\boldsymbol{f}_1,\boldsymbol{f}_2,\cdots,\boldsymbol{f}_l\}$ の 1 次結合ですが、この形では長さ $\|\boldsymbol{f}\|$ の計算が過重です。Dieter (1975) に[37]学びます。

補題 23.（デカルト座標での双対格子ベクトル）

任意の双対 (d,z) 格子ベクトル $\boldsymbol{f}$ が $\boldsymbol{f}=(y_1,y_2,\cdots,y_l)$ とデカルト座標で表される必要十分条件は次の成立である：

$$y_1+zy_2+z^2y_3+\cdots+z^{l-1}y_l\equiv 0\ (\mathrm{mod}\ d).$$

（証明） $\boldsymbol{f}$ が双対格子ベクトルなら整数 $\{c_1,c_2,\cdots,c_l\}$ が存在して、

$$\begin{aligned}\boldsymbol{f} &= c_1\boldsymbol{f}_1+c_2\boldsymbol{f}_2+\cdots+c_l\boldsymbol{f}_l\\ &= (c_1d-c_2z-c_3z^2-\cdots-c_lz^{l-1},c_2,c_3,\cdots,c_l)\end{aligned}$$

であって次が成り立ちます：

$$y_1+zy_2+z^2y_3+\cdots+z^{l-1}y_l=c_1d\equiv 0\ (\mathrm{mod}\ d).$$

故に与式は必要条件です。逆に与式の成立は整数座標双対ベクトル $\boldsymbol{f}$ について等式 $y_1+zy_2+z^2y_3+\cdots+z^{l-1}y_l=kd$ が成り立つ整数 k を与えます。これは、

$$\begin{aligned}\boldsymbol{f} &= (kd-zy_2-z^2y_3-\cdots-z^{l-1}y_l,y_2,y_3,\cdots,y_l)\\ &= k\boldsymbol{f}_1+y_2\boldsymbol{f}_2+y_3\boldsymbol{f}_3+\cdots+y_l\boldsymbol{f}_l\end{aligned}$$

を意味し、$\boldsymbol{f}$ は双対基ベクトルの整数係数 1 次結合として双対格子ベクトルです。与式は $\boldsymbol{f}$ が双対格子ベクトルである十分条件でもあります。 ■

[37] U. Dieter: *How to calculate shortest vectors in a lattice,* Mathematics of Computation **29** (1975), pp. 827-833.

第4章　正 l 格子に基づくスペクトル検定と稜検定

スペクトル検定では MC 乱数の l 連の点が位置を占める l 次元格子を l 次元ユークリッド空間 R_l の $l-1$ 次元格子平面の間の距離の最大値が『あまり大きくない』MC 乱数生成機構を選ぶ、という議論になりました。ここからはさらに、話題を格子そのものとその単位胞 (unit cell) の形にも向けます。以下では MC(d,z) 乱数生成機構からの相続く l 連の点が座席を取る l 次元空間 R_l の格子を $L_l(d,z)$ と記し、もとは理想的な正単体を形成していた l 個の基ベクトル $\{\overrightarrow{\mathrm{OA}},\overrightarrow{\mathrm{OB}},\cdots,\overrightarrow{\mathrm{OF}}\}$ が『理想から連続的に変形して』**体積 d^{l-1} の超平行面体を張る**、と考え、**ベクトルの $l+1$ 個の端点 $\{\mathbf{O},\mathbf{A},\mathbf{B},\cdots,\mathbf{F}\}$ で囲まれる体積が正 l 単体に近い形を取る**、条件を考えます。次元数 $l\geq 4$ でも正単体或いは正格子の帰納的構成は明快で、それからの連続微小変形とすると視覚的、幾何学的或いは思考的な理解は大いに楽になります。これが (d,z) 乱数検定問題の本質で、一般の l 次元格子ではなく理解容易な**正 l 格子の『近傍』だけ**を問題とするのです。

4. 1. 正単体と正格子の構成

単体というのは錐体のように中身の詰まった幾何学的存在ですが、我々は格子に興味を持つのだからもっと緩く、例えば 3 角形の外枠（周或いは辺)、角錐体の外枠（稜全体）のようなものにも同じ用語を充てる事にします。我々は特に正 l 単体に興味を持ちます。それには次元 l に関する次の明快な帰納的構成があります。[38]

定義 24.（正 l 単体の帰納的構成）
(A) 直線 R_1 上の任意の長さ $r>0$ のベクトル (線分でもよいが) $\overrightarrow{\mathrm{OA}}$ を（正）1 単体と呼ぶ事にする。
(B) 2 次元平面 R_2 内の長さ r の 1 単体 $\overrightarrow{\mathrm{OA}}$ の両端から半径 r の円周を描き、それらの 2 つの交点の任意の 1 つを B として作られるベクトル $\overrightarrow{\mathrm{OA}},\overrightarrow{\mathrm{OB}}$ が定める面積 $(3^{1/2}/4)r^2$ の正 3 角形の周全体と内部を正 2 単体と呼ぶ。
(C) 3 次元空間 R_3 内に 1 辺 r の正 2 単体 ΔOAB を置き、その 3 頂点から半径 r の球面を描いて、それらの 2 交点の任意の 1 つを C として作られる 3 ベクトル $\overrightarrow{\mathrm{OA}},\overrightarrow{\mathrm{OB}},\overrightarrow{\mathrm{OC}}$ が張る正 4 面体の形の錐体、体積 $(3!)^{-1}2^{-1/2}r^3$ を正 3 単体と呼ぶ。
(D) 一般の次元 $l\geq 4$ についても帰納的に、l 個の頂点 {O,A,B,$\cdots$,E} から正 $(l-1)$ 単体が得られたとして空間 R_l の中にそれを置き、空間 E_l の $l+1$ 個の

[38] 下の定義 24 の中で、正単体の体積については HN の示した数値には誤りがあり、以下は NN の指摘による正確な数値です。その後の計算には影響しません。HN の深いお詫びと共に訂正した数値も掲げます。

頂点 {O,A,$\cdots$,E} から半径 r の超球面を描き、それらの 2 つの交点の 1 つ F を取って、共通の基点 O からの第 l 番目のベクトル $\overrightarrow{\mathrm{OF}}$ とし、l 個のベクトル $\overrightarrow{\mathrm{OA}}, \overrightarrow{\mathrm{OB}}, \overrightarrow{\mathrm{OC}}, \cdots, \overrightarrow{\mathrm{OF}}$ が張る（或いは $(l+1)$ 個の点 O, A, B, C, $\cdots$, F が定める）線形包、超体積 $(l+1)^{1/2}(l!2^{l/2})^{-1}r^l$ の錐体を正 l 単体と呼ぶ。 **（定義 24 終り）**

上の手順が示す様に、$l+1$ 個の点が囲む（これらの点の線形包である）正 l 単体の形はその $l+1$ 個の頂点間の ${}_{l+1}C_2 = l(l+1)/2$ 個の距離が全て r に等しい、という条件で決まります。正 l 単体を張る l ベクトル達を『基ベクトル』とする格子を正 l 格子と呼びます。上の正 l 単体のコンパスによる構成は、正 l 格子が一定幅のコンパスだけを用いて格子点のすべてを作図できる事を意味します。この状況は一様独立乱数の相続く l 連の座席配置としては（離散的構造であるという点に目をつぶれば）理想的です。

ここで必要なのは正 l 単体、正 l 格子に伴われる基準値を計算し、実際にスペクトル検定や他の検定を行う事です。それは大仕事になりますから、先だって最も簡単な 2 次スペクトル検定でこの『2 正単体基準、或いは 2 次元正格子基準』ではどの様な視野になるか、を見ましょう。正 2 単体は長さ r の稜を持つ正 3 角形で、$l=2$ 次元空間で $(3^{1/2}/4)r^2$ の面積の正 3 角形を張る 2 つの基ベクトル $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ を持つ正 2 格子は『最隣接格子点間距離が r である 3 角格子』と呼ばれます。この格子で隣接平行格子線の最大間隔 ${\mu_2}^{*\max}(r)$ は基ベクトルが張る正 3 角形の任意の頂点の対面する底辺への高さで、3 角関数を用いて容易に、

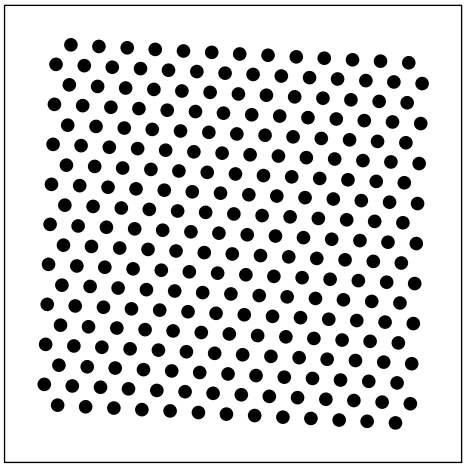
$$ {\mu_2}^{*\max}(r) = (3^{1/2}/2)r \approx 0.8660r $$

と計算されます。対して (d,z) 生成機構の 2 次元格子 $L_2(d,z)$ の最大格子線間隔は ${\mu_2}^{\max}(d,z) = d/\|\boldsymbol{f}_{\min}\|$ ですから、2 次スペクトル検定での (d,z) 生成機構の自然な評価値は、

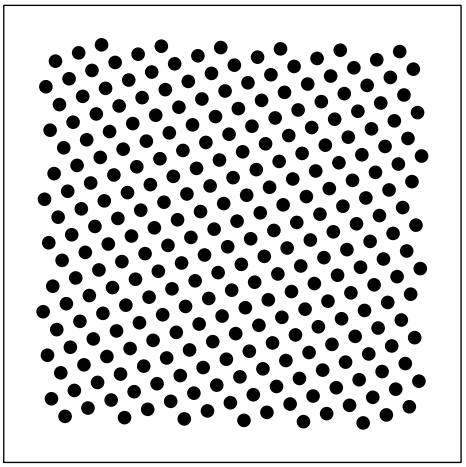
$$ \rho_2(d,z) := {\mu_2}^{\max}(d,z)/{\mu_2}^{*\max}(d) $$

で定義されます。但し (d,z) 格子 $L_l(d,z)$ は整数座標で構成されますから、3 角関数値など無理数座標を要する正 l 格子を正確に再現できない、$\rho_l(d,z)$ 検定評価値は 1 を正確に再現できない、という Diophantus 近似の状況は予期すべきです。下に 3 ページに亘って第 3 図を示します。

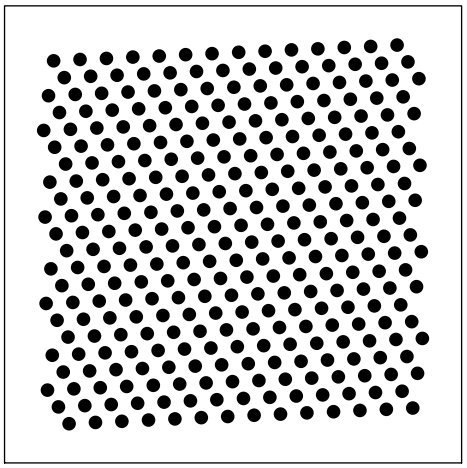
第 3 図　相続く乱数 2 連の配置と 2 次スペクトル検定評価値 ρ の対応



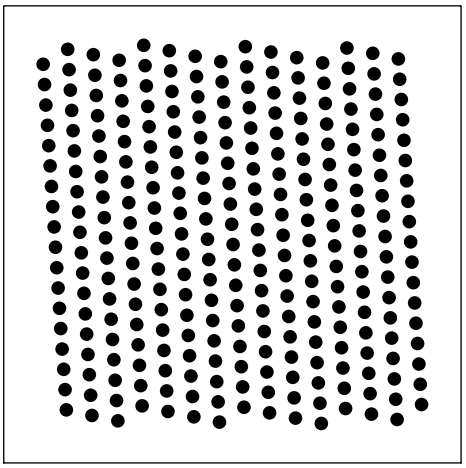
$\rho = 1.0503 \quad (257, 27)$



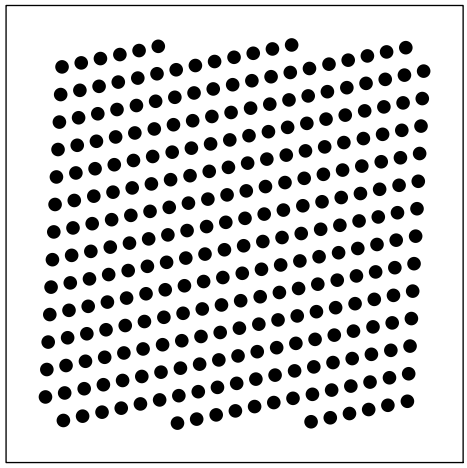
$\rho = 1.0983 \quad (283, 83)$



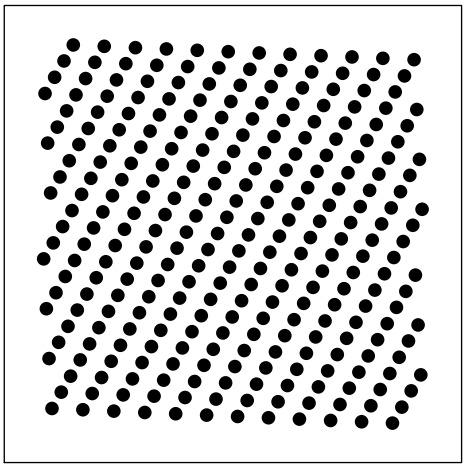
$\rho = 1.1459 \quad (317, 245)$



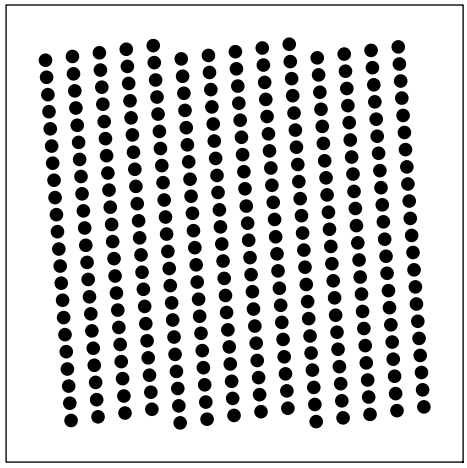
$\rho = 1.1982 \quad (281, 266)$



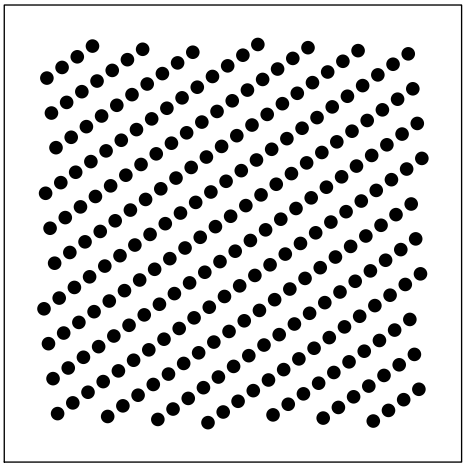
$\rho = 1.2491 \quad (277, 20)$



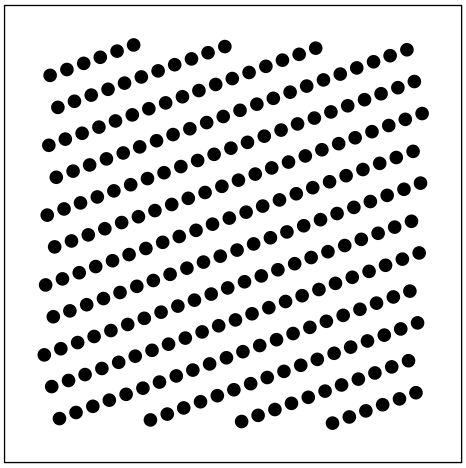
$\rho = 1.3012 \quad (283, 113)$



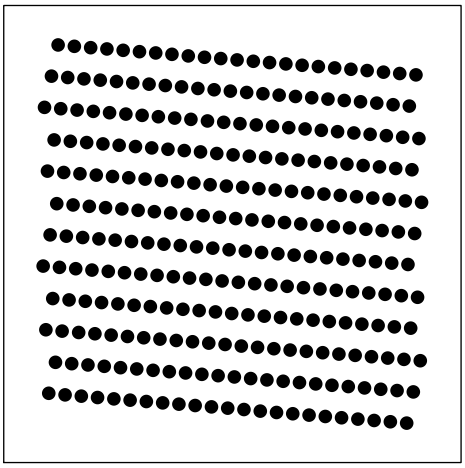
$\rho = 1.3501 \quad (311, 297)$



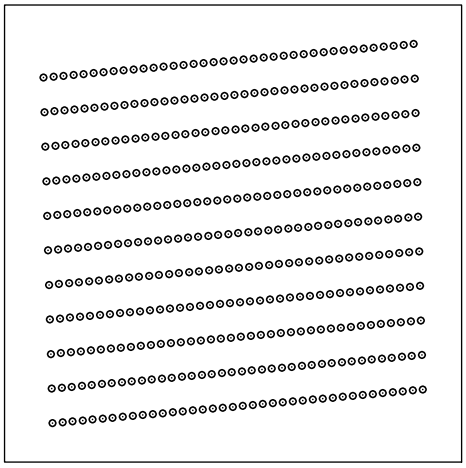
$\rho = 1.3947 \quad (251, 76)$



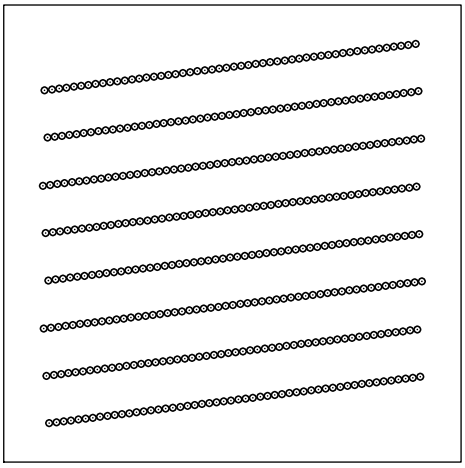
$\rho = 1.4547 \quad (251, 46)$



$\rho = 1.4959 \quad (281, 117)$



$\rho = 1.9915 \quad (419, 381)$



$\rho = 2.7283 \quad (419, 262)$

(第 3 図終わり)

上の第 3 図から $\rho = \rho_2(d, z)$ という 2 次スペクトル検定値が実際の乱数 2 連の点の分布とどの様に対応しているか、様相を実感して下さい。既に触れた様に巡回列はその各値を 1 周期の間に 1 度ずつ、そして 1 度だけ取り、第 3 図はすべて巡回列です。だから l 連の出力点は l 次元空間の格子 $L_l(d, z)$ の格子点に 1 度ずつ座席を取り、重複はありません。[39] 格子点の全体、座席配置は、従って相続く l 出力の独立性を視覚で検定できる**相関図**になっています。出力プロットが作る格子の上で、隣接平行格子線最大間隔の理想は 3 角格子の場合でそれは格子の最もコンパクトな単位胞、正 3 角系の頂点から対辺への垂線の長さです。MC 法 (d, z) 格子でのそれらからの乖離、小さくなる倍率の逆数が 125% 未満が Fishman と Moore の導入したスペクトル検定の合格値上限です。我々はもっと多くの正確強力な基準を必要とします。それらは次の節以下で実際に算出します。第 3 図を示した機会に、別の実際問題にも触れます。これらは全て巡回列の 2 連の点を全周期プロットしています。視察で格子構造を見ると言っても、周期の小さな部分、或いは独立乱数と看做して使用可能な半周期にせよ、格子構造の視認は難しい事があります。それに実用周期が 2^{52}（巡回列としての全周期なら 2^{54} を超えるかもしれませんが）ともなると、それら乱数達を生成するだけでも 2 年ほども掛かります。これをプロットして『見る』という事自体可能ではありません。まして実際にそれだけ膨大な数の点をプロットした場合、格子構造を**見る**ためには顕微鏡的な拡大が必要です。このため第 3 図は小さな法 d に対して描かれています。この意味で第 3 諸図は toy models と言うべきものです。しかし以前に触れたように、各図の点は乱数の出力順に描かれていて、もし PDF 図をゆっくりと表示させる事ができれば、各出力の順に描いていく過程が動画として見られます。現在のコンピュータは大変高速ですから描画は瞬時に終るでしょうが、DOS プロンプトを多数出して、各プロンプト上で意味も描画もない計算を実行し続けるプログラムを走らせれば、PDF は十分遅く描画される様にできます。全体の何割まで描画が進むと格子構造が見えるか、経験されると良いでしょう。

4. 2. l 次正単体基準

この節では表題の l 次正単体基準を導出します。それは正単体の解析幾何学の議論でかなりの難しい計算となります。結論は定理として次節 **4. 3** に纏め、それを用いれば用は足りますので、長い推論を忌避される場合はそちらにお回り下さい。以下この節の議論に省略はありません。

我々は正 l 格子、$l \geq 3$、に伴われる諸基準量を必要とします。それらを得る

[39] この制限と言うか呪縛は後の第 9 章で、法 $d = p_1 p_2 \cdots p_m$ が大きくなると一般に外れる状況が見られます。深刻な問題ではありません。

ために空間 E_l 内で原点 O から発する次の l 個のベクトルを取ります：

$$\begin{aligned}
\boldsymbol{e}_1{}^* &:= \overrightarrow{\mathrm{OQ}_1} = (b, a, a, \cdots, a, a),\\
\boldsymbol{e}_2{}^* &:= \overrightarrow{\mathrm{OQ}_2} = (a, b, a, \cdots, a, a),\\
\boldsymbol{e}_3{}^* &:= \overrightarrow{\mathrm{OQ}_3} = (a, a, b, \cdots, a, a),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\boldsymbol{e}_{l-1}{}^* &:= \overrightarrow{\mathrm{OQ}_{l-1}} = (a, a, a, \cdots, b, a),\\
\boldsymbol{e}_l{}^* &:= \overrightarrow{\mathrm{OQ}_l} = (a, a, a, \cdots, a, b).
\end{aligned}$$

一般性を失う事なく $a > 0$ と $b \neq a$ と[40]を仮定します。下の第 4 図での行列式変形は基ベクトルの張る体積の表現を与え、正 l 格子 $L_l{}^*(d)$ が得られる事は次の 2 条件が保証します：

(A) ベクトルの行列式絶対値は超平行面体の体積 $d^{l-1} > 0$ を[41]与える。

(B) ベクトルとすべての稜は等長で正 l 単体を張る。

第 4 図　正 l 単体を張る基ベクトルの行列式

$$\begin{vmatrix} b & a & a & \cdot & \cdot & \cdot & a & a \\ a & b & a & \cdot & \cdot & \cdot & a & a \\ a & a & b & \cdot & \cdot & \cdot & a & a \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a & a & a & \cdot & \cdot & \cdot & b & a \\ a & a & a & \cdot & \cdot & \cdot & a & b \end{vmatrix} = \begin{vmatrix} s & s & s & \cdot & \cdot & \cdot & s & s \\ a & b & a & \cdot & \cdot & \cdot & a & a \\ a & a & b & \cdot & \cdot & \cdot & a & a \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a & a & a & \cdot & \cdot & \cdot & b & a \\ a & a & a & \cdot & \cdot & \cdot & a & b \end{vmatrix}$$

$$= \begin{vmatrix} s & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ a & c & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ a & 0 & c & \cdot & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a & 0 & 0 & \cdot & \cdot & \cdot & c & 0 \\ a & 0 & 0 & \cdot & \cdot & \cdot & 0 & c \end{vmatrix} = sc^{l-1}.$$

ここで $s := (l-1)a + b,\ \ c := b - a.$　　**(第 4 図終り)**

状況を分析します。上の l ベクトルは同一の長さ $\|\boldsymbol{e}_j{}^*\| = \{(l-1)a^2 + b^2\}^{1/2}$ を持ちます。また $j \neq k$ なら内積はすべて $(\boldsymbol{e}_j{}^*, \boldsymbol{e}_k{}^*) = (l-2)a^2 + 2ab$ で互い

[40]望む事はこれらベクトルが l 次元空間 R_l ですべての座標が正の部分、第 1 象限にある様に決めたいという事です。正単体の帰納的構成から、すべての座標が負の象限にも解があるのでしょうが、それはすべてのベクトルのマイナスを考えればよいので触れません。$b = a$ だとこれらのベクトルは 1 次独立性ではなく、格子の基ベクトルとなる事はできません。

[41]これは上のベクトルの 1 次独立性の保証でもあります。

に同一角度で交わる事も分ります。だから l 単体としてのすべての稜が等長である条件は、残る ${}_l\mathrm{C}_2 = l(l-1)/2$ 個の点の対の間の距離、

$$\|\boldsymbol{e}_k{}^* - \boldsymbol{e}_j{}^*\|^2 = \|\overrightarrow{\mathrm{Q}_j\mathrm{Q}_k}\|^2 = 2(b-a)^2, \quad j \neq k, \quad 1 \leq j,k \leq l,$$

が $\|\boldsymbol{e}_j{}^*\|^2$ と等しい事です。仮定 $b = \xi a$ を置いてこの条件 **(B)** を考えると、a は 0 ではないからそれは ξ の方程式 $(l-1) + \xi^2 = 2(\xi-1)^2$、即ち、

$$\xi^2 - 4\xi - l + 3 = 0, \quad \xi = \xi_\pm := 2 \pm (l+1)^{1/2} \quad \text{（複号同順）}$$

となる、と分かります。このどちらを取っても正 l 単体が構成されますが a と b の符号の問題が生じます。$\xi_\pm := 2 \pm (l+1)^{1/2}$ と置きましょう。ξ_+ はすべての $l = 2, 3, \cdots$ で正なので扱いが簡単です。一方 ξ_- は l によって符号が変ります：

$$\begin{array}{llll} (l=2) & \xi_- = 2 - 3^{1/2} > 0 & (l=3) & \xi_- = 2 - 4^{1/2} = 0 \\ (l=4) & \xi_- = 2 - 5^{1/2} < 0 & (l=5) & \xi_- = 2 - 6^{1/2} < 0 \\ (l=6) & \xi_- = 2 - 7^{1/2} < 0 & & \end{array}$$

この状況は計算を複雑にします。我々は a も b も正の場合[42] $a > 0$ だけを考えます。

$l \geq 2$ で $\xi = \xi_+ > 3$ を取り、$\Lambda := (l+1)^{1/2}$ と置きます。これで $\xi = 2 + \Lambda$ と書く事ができます。

$$\begin{aligned} s &= (l-1)a + b = (l - 1 + \xi)a = (l + 1 + \Lambda)a = a\Lambda(\Lambda+1), \\ c &= b - a = (\xi - 1)a = a(\Lambda + 1) \end{aligned}$$

だから条件 **(A)** は、

$$d^{l-1} = |a\Lambda(\Lambda+1) \cdot \{a(\Lambda+1)\}^{l-1}| = a^l \Lambda (\Lambda+1)^l$$

を与えます。これは $a > 0$ と $b > 0$ を次の様に決定します:、

$$\begin{aligned} a &= \frac{d^{(l-1)/l}}{\Lambda^{1/l}(\Lambda+1)} = \frac{d^{(l-1)/l}(\Lambda-1)}{\Lambda^{1/l}(\Lambda+1)(\Lambda-1)} = \frac{d^{(l-1)/l}(\Lambda-1)}{\Lambda^{1/l} l}, \\ b &= \xi a = (\Lambda+2)a = \frac{d^{(l-1)/l}(\Lambda+2)(\Lambda-1)}{\Lambda^{1/l} l} > 3a. \end{aligned}$$

[42]従って正単体が第 1 象限にある場合です。正 l 単体の次元 l に関する帰納的構成で我々は各段で 2 つの可能性がある事を知りました。座標での表し方には空間回転の無限の可能性がありますが、私達は空間 R_l の第一象限、a, b がすべて正の空間部分、での解だけを考える事にします。なお $\xi = \xi_-$ にも興味がない訳ではありません。特に次元 $l = 3$ では物理との対応を最も鮮やかにして、正 4 面体（正 3 単体）が作る面心立方格子（正 3 格子）の構成が得られます。

諸量が今や算出されます。正 l 格子の平行隣接超格子 $l-1$ 次元平面の間の最大距離は $\mu_l{}^*(d)$ と記されました。それは、例えば $\boldsymbol{e}_0 := (1,1,\cdots,1)/l^{1/2}$、点 O からの単位ベクトル、と $\overrightarrow{\mathrm{OQ}}_j$ との内積を用いて次の様に d と l で表されます：

$$\begin{aligned}\mu_l{}^*(d) &= |l^{-1/2}\{(l-1)a+b\}| = l^{-1/2}(l-1+\xi)a \\ &= l^{-1/2}(\Lambda^2+\Lambda)\frac{d^{(l-1)/l}(\Lambda-1)}{\Lambda^{1/l}l} = \frac{d^{(l-1)/l}\Lambda(\Lambda+1)(\Lambda-1)}{l^{3/2}\Lambda^{1/l}} \\ &= \frac{d^{(l-1)/l}\Lambda^{(l-1)/l}}{l^{1/2}} = d^{(l-1)/l}(l+1)^{(l-1)/(2l)}l^{-1/2}.\end{aligned}$$

正 l 格子 $L_l{}^*(d)$ の中の正 l 単体の 1 稜の長さ、或いは格子 $L_l{}^*(d)$ の格子点間の最短距離、を $\varepsilon_l{}^*(d)$ と記すと、$\varepsilon_l{}^*(d) = \{2(b-a)^2\}^{1/2} = 2^{1/2}|b-a|$ で次になります：

$$\begin{aligned}\varepsilon_l{}^*(d) &= 2^{1/2}\frac{d^{(l-1)/l}\{(\Lambda+2)-1\}(\Lambda-1)}{\Lambda^{1/l}l} = 2^{1/2}\frac{d^{(l-1)/l}(\Lambda+1)(\Lambda-1)}{\Lambda^{1/l}l} \\ &= 2^{1/2}\frac{d^{(l-1)/l}l}{\Lambda^{1/l}l} = 2^{1/2}d^{(l-1)/l}(l+1)^{-1/(2l)}.\end{aligned}$$

後にこれを最短 $\varepsilon_l{}^{*(2)}(d)$ で割った比が必要になるので、その比を $\gamma_l{}^*$ とすると次の通りです:

$$\gamma_l{}^* = \frac{\varepsilon_l{}^*(d)}{\varepsilon_l{}^{*(2)}(d)} = \frac{2^{1/2}d^{(l-1)/l}(l+1)^{-1/(2l)}}{2d^{(l-1)/l}(l+1)^{(l-1)/(2l)}l^{-1/2}} = 2^{-1/2}\left(\frac{l}{l+1}\right)^{1/2} < 1.$$

この様に $\gamma_l{}^*$ は d に関係せず l と共に増大し、$l\to\infty$ で極限 $2^{-1/2}\approx 0.7071$ に下から近づきます。節を変えて、すべてを次の**定理 25** に纏めます。

4. 3. $l \geq 2$ 次元の正格子での結論

定理 25. （正 l 格子基準) l 次元正格子 $L_l{}^*(d)$ は次の諸基準 **(A)-(D)** を与える:
(A) 平行隣接 $l-1$ 次元超格子平面の最大格子間隔は次の通り:

$$\mu_l{}^*(d) = d^{(l-1)/l}(l+1)^{(l-1)/(2l)}l^{-1/2}.$$

$l = 2,3,\cdots$ に対する具体形は:

$$\mu_2{}^*(d) := 2^{-1/2}3^{1/4}d^{1/2} \approx 0.93060d^{1/2},$$
$$\mu_3{}^*(d) := 3^{-1/2}4^{2/6}d^{2/3} \approx 0.91649d^{2/3},$$
$$\mu_4{}^*(d) := 4^{-1/2}5^{3/8}d^{3/4} \approx 0.91429d^{3/4},$$
$$\mu_5{}^*(d) := 5^{-1/2}6^{4/10}d^{4/5} \approx 0.91575d^{4/5},$$
$$\mu_6{}^*(d) := 6^{-1/2}7^{5/12}d^{5/6} \approx 0.91844d^{5/6}.$$

(B) Fishman と Moore (1986) で用いられた『数の幾何学』の結論に基づく 2 次から 6 次のスペクトル検定評価基準値 $\lambda_l{}^*(d)$ は、それぞれ異なる幾何学的形状の格子に関係し次の通り定まる：

$$\lambda_2{}^*(d) := 2^{-1/2}3^{1/4}d^{1/2} \approx 0.93060d^{1/2} = \mu_2{}^*(d),$$
$$\lambda_3{}^*(d) := 2^{-1/6}d^{2/3} \approx 0.80909d^{2/3} < \mu_3{}^*(d),$$
$$\lambda_4{}^*(d) := 2^{-1/4}d^{3/4} \approx 0.84090d^{3/4} < \mu_4{}^*(d),$$
$$\lambda_5{}^*(d) := 2^{-3/10}d^{4/5} \approx 0.81225d^{4/5} < \mu_5{}^*(d),$$
$$\lambda_6{}^*(d) := 2^{-1/2}3^{1/12}d^{5/6} \approx 0.77490d^{5/6} < \mu_6{}^*(d).$$

(C) 正 l 格子の最隣接格子点間距離 $\varepsilon_l{}^*(d) = 2^{1/2}d^{(l-1)/l}(l+1)^{-1/(2l)}$ は、それぞれの次元 $l = 2, 3, \cdots$ に対して次の通り定まる：

$$\varepsilon_2{}^*(d) := 2^{1/2}3^{-1/4}d^{1/2} \approx 1.07457d^{1/2},$$
$$\varepsilon_3{}^*(d) := 2^{1/2}4^{-1/6}d^{2/3} \approx 1.12246d^{2/3},$$
$$\varepsilon_4{}^*(d) := 2^{1/2}5^{-1/8}d^{3/4} \approx 1.15649d^{3/4},$$
$$\varepsilon_5{}^*(d) := 2^{1/2}6^{-1/10}d^{4/5} \approx 1.18222d^{4/5},$$
$$\varepsilon_6{}^*(d) := 2^{1/2}7^{-1/12}d^{5/6} \approx 1.20251d^{5/6}.$$

正 l 格子の格子点間次最隣接距離は $\gamma_l{}^* = \{l/[2(l+1)]\}^{1/2} < 2^{-1/2}$ を最隣接最隣接格子点間距離に掛けたものであって、各次数で倍数を記せば次の通り：

$$\gamma_2{}^* := (2/6)^{1/2} \approx 0.57735,$$
$$\gamma_3{}^* := (3/8)^{1/2} \approx 0.61237,$$
$$\gamma_4{}^* := (4/10)^{1/2} \approx 0.63246,$$
$$\gamma_5{}^* := (5/12)^{1/2} \approx 0.64550,$$
$$\gamma_6{}^* := (6/14)^{1/2} \approx 0.65465.$$

（定理 25 終り）

$l=2$ 次元での基準値 ${\lambda_2}^*(d)$ と ${\mu_2}^*(d)$ の一致は数の幾何学の結論が 3 角格子（正 2 格子）に関するものである事を意味します。3-6 次元での乖離は、数の幾何学の結論が正 l 単体基準ではなく、**平行隣接超格子平面間隔の最大値の幾何学的最小**を基準とする事の反映です。既述の通り、相続く乱数の独立性を反映する様に選ばれた正単体基準への改訂は、『旧 (数の幾何学) 基準で選ばれた優れた部分 MC 法乱数を孫子の定理で合成しても優れた合成 MC 法乱数がどうしても得られらない』というスペクトル検定に関わる謎を解きほぐし、乱数の検定方式を正しい軌道に乗せました。『可能な最小値に基づく検定ではない』という事は新しい問題の発生でしたが、それは『格子の幾何学的な近さ』を考える検定で解消されました。越えるべき技術問題はまだ終りではありません。次節の正格子基準合格 MC 乱数生成機構を実際に見て、この先に立ちはだかる技術問題と、第 9 章での孫子の定理に基づくその問題の『魔術的解消』とでも言うべきものを見て下さい。

4. 4. 正単体基準最大最小稜検定

これまでの考察から、我々は乗算合同法 (d,z) の検定は、『その相続く l 連の点が空間 R_l で張る格子 $L_l(d,z)$ がどれだけ正 l 格子 ${L_l}^*(d)$ に近いか』を評価するものである、という理解を得ました。スペクトル検定に限って言うと、格子 $L_l(d,z)$ の平行隣接 $(l-1)$ 次元超平面の最大間隔 $\mu_l(d,z)$ がどれほど正 l 格子 ${L_l}^*(d)$ のそれ ${\mu_l}^*(d)$ に近いか、で評価すべきです。正単体が作る正格子で明らかになるのは、『正格子が微小に変形するとき、それまで最隣接距離にあった格子点間も連続的にその隣接距離を変える』という事実です。その距離の変化がどれくらいなら『微小』か、という時基準として単位胞だけを見てもわからない、『格子』を見ようという理解です。

一様独立な MC 乱数が作る格子としての理想は正格子です。数の幾何学基準とは違う、『格子の最も正単体に近い単位胞』が微小変形したときに取る格子の形は $l\geq 3$ では $\mu_l(d,z)>{\mu_l}^*(d)$ でも $\mu_l(d,z)<{\mu_l}^*(d)$ でも実際あり得ます。検定値、

$$\rho_l(d,z):=\mu_l(d,z)/{\mu_l}^*(d)$$

で言うと 1 より大きい事も小さい事もある、それを我々は捌かなければならないのです。正しい展望は、**基ベクトルの張る単体の近さよりも格子としての近さである**と理解して得られました。詳しく述べれば:

格子の基ベクトルの取り方は様々ですが『正格子』の本質は単一幅のコンパスで次々に交点を取って構成される所にあり、その ${}_{l+1}C_2=(l+1)l/2$ 個の正単体等長格子点間の最短稜が、格子の変形に伴って $l=2,3,\cdots,6$ に対し

て長さが、

$$1/\gamma_l{}^* = 2^{1/2}(1+1/l)^{-1/2} > 3^{1/2} \approx 1.73$$

倍であった『次最短ベクトルの変化よりはまだ小さい』程度の微小変化をする、正格子での等長最短格子ベクトル $(l+1)l/2$ 個が依然として最短格子ベクトルに留まっている、その様な格子 $L_l(d,z)$ は高精度乱数生成機構として十分な資格を持つ、という事です。この基準の採択を科学技術者、クリエータの御使用に勧めます。

この新しい視点、帰結はそれまでの『数の幾何学』の結論とは異なります。現在確かめられているのはここで導入する『正単体基準最大最小稜検定』には少なくとも複数の合格者がある、という事実です。これまでの『数の幾何学の検定基準』では、2 つの合格 MC 生成機構を孫子の定理で合成して新しい長周期の MC 乱数生成機構を見つける事ができないのが事実です。HRF では『正格子に基づくスペクトル検定と正格子基準最小最大稜検定』の採用をお勧めします。第 6 章の開示、そして第 9 章の高速計算の技術を見て頂けば、他に選択肢はないと御理解頂けるでしょう。実際手段を広く認識し納得して頂く様に、以下に繰り返しを恐れず正確に纏めます。2 次元では基準はスペクトル検定と変りませんから省きます。3 次以上は難しい実行手順、合格の稀な探索手順ですが、着実に行う事ができます。応用では単に MC 乱数生成機構のプログラムルーチンを取り替えるだけの労力なのですから。

4. 5. 正格子を基準とする諸検定のまとめ

$l \geq 3$ 次元で格子が正格子に近いための基準は上で詳しく与えられましたが、全体が余りに大部、多くの事項を含むので、再参照が容易になる様に、**定理 26** として表の様に纏めて進みます。

定理 26.（正 l 格子基準、或いは正 l 単体基準） l 次元正格子 $L_l{}^*(d)$ について:
(A) 平行隣接 $l-1$ 次元超格子平面の最大格子間隔は次の通り:

$$\mu_l{}^*(d) = d^{(l-1)/l}(l+1)^{(l-1)/(2l)}l^{-1/2}.$$

$l = 2, 3, \cdots$ に対して具体形を記すと:

$$\mu_2{}^*(d) := 2^{-1/2}3^{1/4}d^{1/2} \approx 0.93060d^{1/2},$$
$$\mu_3{}^*(d) := 3^{-1/2}4^{2/6}d^{2/3} \approx 0.91649d^{2/3},$$

$$\mu_4{}^*(d) := 4^{-1/2}5^{3/8}d^{3/4} \approx 0.91429d^{3/4},$$
$$\mu_5{}^*(d) := 5^{-1/2}6^{4/10}d^{4/5} \approx 0.91575d^{4/5},$$
$$\mu_6{}^*(d) := 6^{-1/2}7^{5/12}d^{5/6} \approx 0.91844d^{5/6}.$$

(B) Fishman と Moore (1986) で用いられた『数の幾何学』の結論に基づく 2 次から 6 次のスペクトル検定評価基準値 $\lambda_l{}^*(d)$ は、それぞれ異なる幾何学的形状の格子に関係し次の通り定まる：

$$\begin{aligned}
&\lambda_2{}^*(d) := 2^{-1/2}3^{1/4}d^{1/2} \approx 0.93060d^{1/2} = \mu_2{}^*(d),\\
&\lambda_3{}^*(d) := 2^{-1/6}d^{2/3} \approx 0.80909d^{2/3} < \mu_3{}^*(d),\\
&\lambda_4{}^*(d) := 2^{-1/4}d^{3/4} \approx 0.84090d^{3/4} < \mu_4{}^*(d),\\
&\lambda_5{}^*(d) := 2^{-3/10}d^{4/5} \approx 0.81225d^{4/5} < \mu_5{}^*(d),\\
&\lambda_6{}^*(d) := 2^{-1/2}3^{1/12}d^{5/6} \approx 0.77490d^{5/6} < \mu_6{}^*(d).
\end{aligned}$$

(C) 正 l 格子の最隣接格子点間距離 $\varepsilon_l{}^*(d) = 2^{1/2}d^{(l-1)/l}(l+1)^{-1/(2l)}$ は、それぞれの次元 $l = 2, 3, \cdots$ に対して次の通り定まる：

$$\begin{aligned}
&\varepsilon_2{}^*(d) := 2^{1/2}3^{-1/4}d^{1/2} \approx 1.07457d^{1/2},\\
&\varepsilon_3{}^*(d) := 2^{1/2}4^{-1/6}d^{2/3} \approx 1.12246d^{2/3},\\
&\varepsilon_4{}^*(d) := 2^{1/2}5^{-1/8}d^{3/4} \approx 1.15649d^{3/4},\\
&\varepsilon_5{}^*(d) := 2^{1/2}6^{-1/10}d^{4/5} \approx 1.18222d^{4/5},\\
&\varepsilon_6{}^*(d) := 2^{1/2}7^{-1/12}d^{5/6} \approx 1.20251d^{5/6}.
\end{aligned}$$

正 l 格子で次最隣接格子点間距離は最も隣接の距離の $\gamma_l{}^* = \{l/[2(l+1)]\}^{1/2} < 2^{-1/2}$ 倍であって、各次数で何倍になるかを記せば次の通り：

$$\begin{aligned}
&\gamma_2{}^* := (2/6)^{1/2} \approx 0.57735,\\
&\gamma_3{}^* := (3/8)^{1/2} \approx 0.61237,\\
&\gamma_4{}^* := (4/10)^{1/2} \approx 0.63246,\\
&\gamma_5{}^* := (5/12)^{1/2} \approx 0.64550,\\
&\gamma_6{}^* := (6/14)^{1/2} \approx 0.65465.
\end{aligned}$$

（定理 25 終り）

$l = 2$ 次元での基準値 $\lambda_2{}^*(d)$ と $\mu_2{}^*(d)$ の一致は数の幾何学の結論が 3 角格子（正 2 格子）に関するものである事を意味します。3-6 次元での乖離は、数の幾何学の結論が正 l 単体基準ではなく、**平行隣接超格子平面間隔の最大値の幾何学的最小**を基準とする事の反映です。既述の通り、相続く乱数の独立性を反映する様に選ばれた正単体基準への改訂は、『優れた部分 MC 法乱数を孫子の定理で合成しても優れた合成 MC 法乱数がどうしても得られらない』という旧基準のスペクトル検定に関わる謎を解きほぐし、乱数の検定方式を正しい軌道に乗せました。『可能な最小値を理想とする検定ではない』という事は新しい問

題の発生でしたが、それは『格子の幾何学的な近さ』を考える検定で不都合を解消されました。越えるべき技術問題はまだまだ終りではありません。我々はまず第 6 章でこれら検定が定める『優れた MC 乱数』の姿を実像として見て、同時に生起する『計算と周期』の大問題に至ります。その奇跡的な根本解決、孫子の定理とその応用、は第 9 章で詳しく延べられます。その前に、概念的には平易だが困難な検定での解決をを求める『平面格子や空間格子の (時空) 格子点に置かれた自由度への MC 乱数の配布問題』も議論しなければなりません。『前途未だ遼遠』です。しかしどれも美しく解決されます。乗算合同法乱数のこの驚くべき多才の発見を楽しみとして進みましょう。