HRF 談話室 A (2024 年 1 月 1 日)

乗算合同法の表現定理と開示

1. 法 d の合同と合同算法 (2024 / Jan. 1)

小中学校での整数算術の知識を再確認し、磨きます。

定義 1.（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 が y で割り切れるとき、y を x の『因数』と言う。特に整数 x が素数 p で割り切れるとき、p を x の『素因数』と言う。任意の（正の）整数 $x \geq 2$ は素因数分解される。[1]

(C) 整数 x, y が共通な因数を持たないとき、従って共通な素因数がないとき、『互いに素』と言う。

(D) 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）**

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；このつまらない場合を『互いに素』の定義から除外しない方が便利です。

補題 2.（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、法 d での結果は変らない。

（証明） (A) 明らかです。

[1] 素数 $p_1, p_2, \cdots$ を昇順に取って割り算を続け、素因数分解はできますが、他に素因数分解がないのか、これは大問題です。整数の素因数分解一意である事はガウスが『証明した』のです。なぜ証明が必要か、これからその理解に向かって進みます。

(B) 上の **(A)** から自明。
(C) $xy \equiv xz (\mathrm{mod}\ d)$ 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、$y \equiv z\ (\mathrm{mod}\ d)$ を意味します。
(D) 例えば仮定 $x' \equiv x\ (\mathrm{mod}\ d)$ 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 $x'y \equiv xy\ (\mathrm{mod}\ d)$。この議論は他のすべての場合でも成り立ち、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 $x \equiv y\ (\mathrm{mod}\ 1)$ 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[2]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、置換すると整数を作る式 $f(x, y, z, \cdots)$ 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。

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。

2. 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[3]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、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[4]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。Transportability 移植可能性の要求です。

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

[2]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。

[3]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。

[4]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**は用いる事ができません。

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 (特にコンピュータゲーム上で) 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、

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

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、

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

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　検定で選ぶ、

という事になります。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』事は非常に実現の難しい作業です。楽な仕事ではありません。

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。

3. 乗算合同 (MC) 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に出会います。まず乗算合同 (MC) 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 $d \ge 2$ と d とは素な任意の整数 $0 < n < d$ に対して定まる計算諸言語で標準的な関数 $\mathrm{mod}(n, d)$ で始めます。

定義 3.（乗算合同法 multiplicative congruential method[5]）
法 modulus の整数 $d \geq 2$ 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：

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

ここで $n \neq 0$ は法 d とは素な任意の整数で、種 seed と呼ばれる。 **(定義 3 終)**
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薄いので、多くの場合略記 (d, z) を用います。

4. コンピュータ上の乗算合同 (MC) 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、

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

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

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

を $0 \leq u_k < 1$ 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。
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：

$$\begin{aligned} z^T X &= (x_1x_2x_3\cdots x_T).(x_1x_2x_3\cdots x_Tx_1x_2x_3\cdots) \\ (z^T - 1)X &= x_1x_2x_3\cdots x_T \\ X &= \frac{x_1x_2x_3\cdots x_T}{z^T - 1} = \frac{n}{d}. \end{aligned}$$

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

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[6]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:

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

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：

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

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 3. (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)[7]

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、

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

[6] $\overline{z} := z - 1$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。

[7] 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/indexarchive20jan6.html

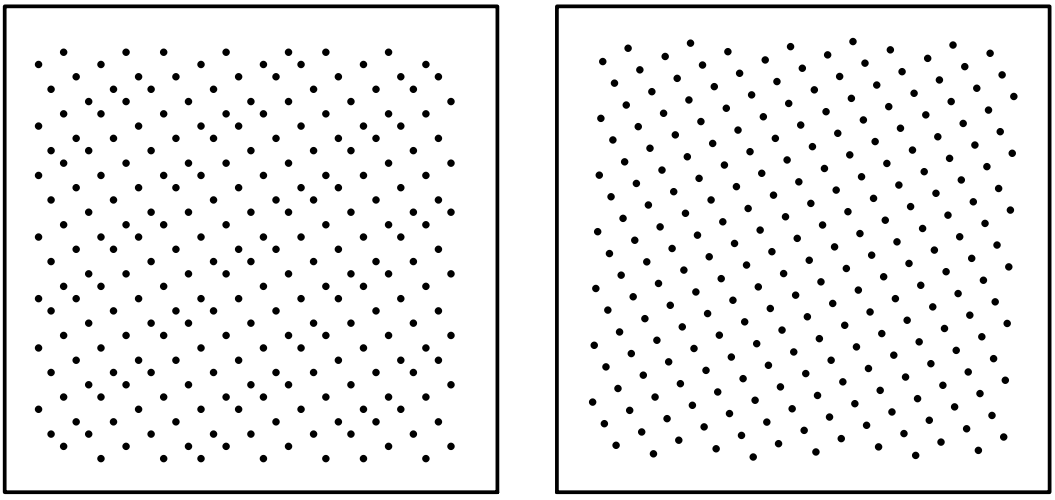
がもとの一様乱数列を次の形で『一様近似』する：

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

(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：

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

Figure 1.



(End of Figure 1)

（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。 ■

前頁の第 1 図は、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 (v_{k-1}, v_k) の右図の点から**定理 3 (B)** によって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 3 (A)** によって点の座標は $1/34$ の一様精度で近く、図全体 d 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、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。

Appendix 素因数分解の一意性について

A1. Euclid の互除法について

まず最初に、ユークリッド Euclid の互除法を説明しなければなりません。これはユークリッドの時代をはるかに超えた 19 世紀に与えられた平易な考え方から入る方が分り易いと思います。

正の整数 a, b を取り、その整数係数 A, B による 1 次結合 $s := Aa + Bb$ の全体を S と記します。

Lemma A1 a, b は正の整数としてその整数 A, B による 1 次結合の全体

$$S := \{Aa + Bb | \ A \text{ と } B \text{ は整数 } \}$$

の中で正で最小のものを m とする。
(A) S の整数はすべて m の (正、負の) 倍数である:[8]
(B) m は a, b の (正の) 最大公約数 (greatest common divisor GCD) である。
(C) (ユークリッドの互除法の結論) 正の整数 a, b の最大公約数 m は整数 A, B によって $m = Aa + Bb$ と表される。[9]
(証明) (A,B) S は $a = 1 \cdot a + 0 \cdot b = a$ 及び $b = 0 \cdot a + 1 \cdot b$ を含んでいます。S の正の最小値 m は、S の整数だから $m = Aa + Bb$ の形を特定の (一意ではないが) 組 A, B で持ちます。q は商 (quotient)、r は余り (remainder) で $0 \leq r < m$ とします。 S の任意の整数 x は $x = A'a + B'b$ の形で A', B' は整数、これを m で割って整数の商を q、整数の正又は 0 の余りを r、とすると、割り算の意味から $r = A'a + B'b - qm = (A' - qA)a + (B' - qB)b$、これは S の数です。S の正の最小値が m だからそれより小さい余り r は 0 です。即ち『S の数はすべて m で割り切れる m の倍数』で、逆に $m = Aa + Bb$ のすべての正負の倍数はやはり S の数、故に $S = \{cm | \ c = 0, \pm 1, \pm 2, \cdots\}$ と分ります。
(C) S には a も b も含まれるから m は a, b の両方を割り切る公約数です。a, b の最大公約数を $M := (a, b) > 0$ とする[10]と、$M = (a, b) \geq m$ です。一方 M は『$m = Aa + Bb$ を割り切る』のだから $M \leq m$ も成り立つはず、$M = m$ でなければなりません ■

[8] この意味で整数の集合 S は『単項イデアル』と呼ばれます。

[9] 表す整数の組 $A.B$ は一意ではない；$A'a + B'b = 0$ となる整数をそれぞれ加えた $A + A', B + B'$ も可能な整数の 1 組である。

[10] 最大公約数の記法 $(a.b)$ は 2 成分ベクトル、ベクトル a とベクトル b の内積、その他に多用される記号ですが、混乱のおそれはないと思うので用います。

次が Euclid の互除法に基づいて Gauss が示したという美しい鍵です。

補題 (EG) 整数 $x \geq 2$ が正の互いに素な整数による因数分解 $x = ab$ を持ち、素数 $p > 1$ が x を割り切るなら、p は a, b の一方を割り切る。
(証明) 仮定は素数 p が積 ab を割り切るのだから、2 つの可能性　(1) p は a を割り切らない、　(2) p は a を割り切る、しかありません、(2) の場合は補題は成立ちます。(1) の場合に p が b を割り切る事を示します。この場合 p と a は互いに素で Euclid の関係 $1 = Pp + Aa$ が成り立ちます。これは $b = Pbp + Aab$ であり、b が p で割り切れる事を意味します。■

綺麗です。間然する所がありません。

定理. (整数の素因数分解の一意性 (Euclid-Gauss)　整数の素因数分解は一意である。
(証明) 整数 x が 2 通りの素因数分解:

$$x = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

を持つとします。Euclid-Gauss の補題から、p_1 に対し $p_1 = q_1{}'$ となる右辺の素数 $q_1{}'$ がなければなりません。それらを両辺から割って除けば、$m-1$ 個と $n-1$ 個の等式が残ります。この手続きは $m = n$ であり両辺が 1 の等式になるまで続けられ、素因数分解は一意です。■

これが何の役にたつのか、と言えばどんな整数でも素因数分解はただ一通りですから、2 つの整数 a, b について、その素因数分解を (重複する素因数はまとめて)

$$a = (p)^m (q)^n \cdots (r)^s, \quad b = (p)^{m'} (q)^{n'} \cdots (r)^{s'}$$

とすれば,[11] a, b の最大公約数 GCD と最小公倍数 LCM が

$$\mathrm{GCD}(a,b) = p^{\min(m,m')} q^{\min(n,n')} \cdots r^{\min(s,s')}$$
$$\mathrm{LCM}(a,b) = p^{\max(m,m')} q^{\max(n,n')} \cdots r^{\max(s,s')}$$

と表される事になります。

[11] 整数 a, b のすべての素因数をまとめて $p, q, \cdots, r$ と書きます。それぞれに含まれない素因数は指数 0 を付けて表す事にし、a, b に含まれる素因数の冪を $\{m, n, \cdots s\}$ 及び $\{m', n', \cdots s'\}$ と書きましょう。