全周期の線形合同法は周期の中で値が重ならず、重ならないことが乱数でない印になる

— **32** ビットの線形合同法は周期 **4294967296** で、**1** 秒に 10^9 回引けば **4.294967** 秒で使い切る — 分離子は、出しているのが状態そのものか、状態の一部か — [論文763]

山岸 勇輝 (Yuuki YAMAGISHI)
Yamagishi Complexity Torus Lab, Japan｜山岸勇輝ラボ
2026年9月

— From thinking to syncing. —

要旨

擬似乱数は、周期が長いほど良いと言われる。周期の中で同じ値が出ないなら、なおさら良さそうに見える。同じ値の重なりを、本物の乱数と二通りの出し方で数える。新しい定理も法則も主張しない。 第一に、周期は長くても、使い切れる——32 ビットで周期 4294967296、1 秒に 10^9 回なら 4.294967 秒（第2節）。 第二に、本物の乱数は、周期よりずっと早く重なる——32 ビットで最初の重なりまで 82137.861970 回、周期の 1.912421×10^{-5} 倍（第2節）。 第三に、これが本稿の芯である。状態をそのまま出す全周期の生成器は、一度も重ならない——16 ビットの値を 5000 個引いて、本物は 187.250000 回、生成器は 0.000000 回（第3節）。 第四に、重ならないことが、本物でない印になる——本物の期待値は 185.940004 回で、試行もそれに乗る（第3節）。 第五に、状態の一部だけを出すと、重なりが戻る——32 ビットの上位 16 ビットで 187.480000 回、期待値との相対差 0.008282（第3節）。 第六に、分離子は、出しているのが状態そのものか、状態の一部かである——「周期が長いほど良い乱数」は、何を出しているかを言うまで真偽が決まらない（第4節）。 キーワード：擬似乱数、線形合同法、周期、誕生日の重なり、全周期の条件、状態と出力。

本稿の射程（射程注記）：新しい定理も法則も主張しない——線形合同法、全周期の条件（ハル＝ドーベル）、誕生日の重なりの期待値、状態の上位ビットだけを出す作り方は、いずれも既知である（ハル＆ドーベル 1962、プレスほか 2007）。他の検定を扱わない——スペクトル検定や多次元の構造は扱わず、値の重なりだけを数える。他の生成器を扱わない——線形合同法以外の生成器は扱わない。暗号を扱わない——予測されにくさや安全性は主題ではない。速さは置いた値である——1 秒に 10^8 回・10^9 回は、使い切る時間の桁を見るための値である。既刊との関係：論文504 は、下がる雑音と下がらない雑音が一つの式の両端であることを示した——その射程注記は「乱数生成器を評価しない——線形合同法で作っており、擬似乱数の質そのものは主題ではない」と明記していた。そこでは線形合同法を道具として使った。ここではその道具の周期と重なりを数える。論文223 も引く——そこでは検定を全部通る線形合同法の点が、三つ組にすると十五枚の平面に乗った。ここでは一つずつの値の重なりという最も単純な数え方で、状態をそのまま出す生成器が本物と見分けられる。加えたのは、周期を使い切る時間と、本物の最初の重なりまでの回数を並べたこと、5000 個で重なりが本物 **187.250000**・状態そのもの **0.000000**・上位ビット **187.480000** と分かれることを示したこと、16 ビットの生成器を実際に一周させて全周期を確かめたこと、分離子を「状態そのものか、一部か」に置いたことである。

1. 記法と問い

設定：線形合同法は、状態 x を次の式で更新する。m が 2 の冪なら、c が奇数で $a-1$ が 4 の倍数のとき、周期は m に等しい（全周期）。本物の一様乱数を m 通りから引くと、最初の重なりまでの回数と、k 個引いたときの重なりの数の期待値は次になる。

$$x_{k+1} = (a\,x_k + c) \bmod m, \qquad E[\text{最初の重なり}] \approx \sqrt{\frac{\pi m}{2}} + \frac{2}{3}, \qquad E[\text{重なりの数}] = k - m\Big(1 - \big(1 - \tfrac{1}{m}\big)^k\Big)$$

32 ビットは $a = 1664525$・$c = 1013904223$、16 ビットは $a = 25173$・$c = 13849$ を使う。

問い：周期の中で同じ値が出ない生成器は、良い乱数なのか。

2. 周期と、本物の重なり

計算 2.1：32 ビットの生成器の周期、使い切る時間、本物の 32 ビット乱数の最初の重なりまでの回数を出した。

量	値
全周期の条件	満たす
周期	**4294967296**
使い切る時間（10^8 回/秒）	**42.949673** 秒
使い切る時間（10^9 回/秒）	**4.294967** 秒
本物の最初の重なりまでの回数	**82137.861970**
その周期に対する倍率	1.912421×10^{-5}

> **観察 2.2**
>
> **本物の乱数は、周期よりずっと早く重なる。32 ビットの値を引くと 82137.861970 回ほどで最初の重なりが出るが、全周期の生成器は 4294967296 回まで一度も同じ状態に戻らない——周期の中で重ならないことは、本物の乱数には無い性質である。**

3. 重ならないことが、印になる

計算 3.1：16 ビットの生成器を 65536 回まわして全周期を確かめ、16 ビットの値を 5000 個引いたときの重なりの数を、200 回の平均で比べた。

引き方	重なりの数（200 回の平均）
本物の乱数	**187.250000**
（期待値）	**185.940004**
16 ビットの生成器の状態そのもの	**0.000000**
32 ビットの生成器の上位 **16** ビット	**187.480000**

観察 3.2

これが本稿の芯である。状態をそのまま出す全周期の生成器は、一度も重ならない。**16** ビットの生成器は **65536** 回で **65536** 種類を出して元に戻り、**5000** 個の中の重なりは **0.000000** 回である——本物なら **187.250000** 回重なるので、重なりを数えるだけで本物と見分けられる。

観察 3.3

状態の一部だけを出すと、重なりが戻る。**32** ビットの生成器の上位 **16** ビットでは **187.480000** 回で、期待値との相対差は **0.008282** である——同じ値が別の状態から出てくるので、本物と同じように重なる。

観察 3.4

本物の **16** ビット乱数で最初の重なりまでを数えると、**2000** 回の平均で **321.254500** 回だった。期待値 **321.515086** に乗る——重なりの期待値の式が、この試行で確かめられた。

4. 分離子

観察 4.1

分離子は、出しているのが状態そのものか、状態の一部かである。状態そのものなら周期の中で重ならず、それが本物でない印になり、一部なら重なりが本物と同じに戻る——「周期が長いほど良い乱数」は、何を出しているかを言うまで真偽が決まらない。

観察 4.2

論文**504** と並べる。**504** は線形合同法を道具として使い、擬似乱数の質は主題でないと明記した——ここはその道具の周期と重なりを数えた。

> **観察 4.3**
>
> 論文223 とも並べる。223 は、検定を全部通る線形合同法の点が三つ組にすると十五枚の平面に乗ることを示した——ここでは一つずつの値の重なりという最も単純な数え方で、状態をそのまま出す生成器が見分けられる。

> **観察 4.4**
>
> 言わないこと。他の検定も、他の生成器も、暗号の用途も扱わない——示したのは、重ならないことが良さではなく印になる場合があることである。

5. 点呼と結び

1. 周期 **4294967296**（計算 2.1）：**32** ビット。
2. **4.294967** 秒で使い切る（計算 2.1）：10^9 回/秒。
3. 本物の最初の重なり **82137.861970** 回（観察 2.2）：周期よりずっと早い。
4. 本物の重なり **187.250000**（計算 3.1）：5000 個で。
5. 期待値 **185.940004**（計算 3.1）：式どおり。
6. 状態そのもの **0.000000**（観察 3.2）：本稿の芯。
7. 上位ビット **187.480000**（観察 3.3）：重なりが戻る。
8. 相対差 **0.008282**（観察 3.3）：本物と同じ。
9. 最初の重なり **321.254500** 回（観察 3.4）：16 ビットの本物。
10. 状態そのものか、一部か（観察 4.1）：分離子・論文504・223。

結び：全周期の線形合同法は周期の中で値が重ならず、重ならないことが乱数でない印になる。32 ビットの生成器は周期 4294967296 で、1 秒に 10^9 回引けば 4.294967 秒で使い切るが、本物の 32 ビット乱数なら 82137.861970 回ほどで最初の重なりが出る——周期の中で重ならないことは、本物の乱数には無い性質である。16 ビットの値を 5000 個引くと、本物の乱数は 187.250000 回（期待値 185.940004）重なるのに、状態をそのまま出す生成器は 0.000000 回で、32 ビットの生成器の上位 16 ビットだけを出すと 187.480000 回に戻る——重なりを数えるだけで、状態そのものを出す生成器は本物と見分けられる。分離子は、出しているのが状態そのものか、状態の一部かである——「周期が長いほど良い乱数」は、何を出しているかを言うまで真偽が決まらない。既刊との位置——論文504 は線形合同法を道具として使い質を問わなかった。論文223 は三つ組の構造

を示した。ここは一つずつの値の重なりを数えた。正直に言えば——他の検定も他の生成器も暗号の用途も扱っていない。

参考文献

1. Hull, T. E., & Dobell, A. R. (1962). Random number generators. *SIAM Review*.
2. Press, W. H., Teukolsky, S. A., Vetterling, W. T., & Flannery, B. P. (2007). *Numerical Recipes: The Art of Scientific Computing* (3rd ed.). Cambridge University Press.
3. 山岸勇輝 (2026).『検定を全部通り、それでも点は十五枚の平面に乗っている』[論文223]. Zenodo. 10.5281/zenodo.22120728
4. 山岸勇輝 (2026).『下がる雑音と下がらない雑音は二つではなく、一つの式の両端である』[論文504]. Zenodo. 10.5281/zenodo.22861737

— *From thinking to syncing.* —

山岸 勇輝 (Yuuki YAMAGISHI)

© 2026 Yamagishi Complexity Torus Lab, Japan · Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0)