A Full-Period Linear Congruential Generator Never Repeats Within Its Period, Which Marks It as Not Random

— A **32**-bit linear congruential generator has period **4294967296** and is used up in **4.294967** s at 10^9 draws per second — the separator is whether the output is the whole state or part of it — [Paper 763]

Yuuki YAMAGISHI (山岸 勇輝)
Yamagishi Complexity Torus Lab, Japan
September 2026

— *From thinking to syncing.* —

Abstract

Pseudo-random generators are said to be better the longer their period. If no value repeats within the period, all the better, it seems.Repeated values are counted for true random numbers and for two ways of producing output.No new theorem or law is claimed. First, a long period can still be used up——32 bits give period 4294967296, used up in 4.294967 s at 10^9 draws per second (Section 2). **Second, true random numbers repeat far sooner than the period ——82137.861970 draws to the first repeat at 32 bits, 1.912421×10^{-5} of the period** (Section 2). **Third, and this is the core. A full-period generator that outputs its state never repeats——drawing 5000 16-bit values, true random numbers repeat 187.250000 times, the generator 0.000000 times** (Section 3). **Fourth, not repeating marks it as not random——the true expectation is 185.940004, and the trial follows it** (Section 3). **Fifth, outputting only part of the state brings repeats back——the top 16 bits of a 32-bit generator give 187.480000, a relative difference of 0.008282 from expectation** (Section 3). **Sixth, the separator is whether the output is the whole state or part of it ——"a longer period makes a better generator" has no truth value until one says what is output** (Section 4).

Keywords: pseudo-random numbers, linear congruential generator, period, birthday repeats, full-period condition, state and output.

Scope of this paper (scope note): **No new theorem or law is claimed——linear congruential generators, the full-period condition (Hull and Dobell), the expected number of birthday repeats, and outputting only the upper bits of the state are all known (Hull and Dobell 1962, Press et al. 2007).Other tests are not treated——spectral tests and multidimensional structure are not treated; only repeats of values are counted.Other generators are not treated——generators other than linear congruential ones are not treated.Cryptography is not treated——unpredictability and security are not the subject.Speeds are set values——10^8 and 10^9 draws per second are for the order of the time to use up the period.Relation to earlier papers**: **Paper 504 showed that falling and non-falling noise are two ends of one expression——its scope note stated that random number generators would not be evaluated: it used a linear congruential generator, and the quality of pseudo-random numbers was not its subject. There the generator was a tool. Here its period and repeats are counted.Paper 223 is also cited——there a linear congruential generator passing every test put its points on fifteen planes when taken in triples. Here the simplest count of all, repeats of single values, distinguishes a generator that outputs its state from true randomness.**What is added is **setting the time to use up the period beside the draws to a true first repeat**, **showing repeats in 5000 draws splitting into $\mathbf{187.250000}$ for true, $\mathbf{0.000000}$ for the state, and $\mathbf{187.480000}$ for upper bits**, **running a 16-bit generator through a full cycle to confirm its full period**, and **placing the separator on whole state against part**.

1. Notation and the Question

Setting: **a linear congruential generator updates its state x as below. With m a power of 2, the period equals m (full period) when c is odd and $a-1$ is a multiple of 4. Drawing true uniform random numbers from m values, the draws to the first repeat and the expected number of repeats among k draws are as follows.**

$$x_{k+1} = (a\,x_k + c) \bmod m, \qquad E[\text{first repeat}] \approx \sqrt{\frac{\pi m}{2}} + \frac{2}{3}, \qquad E[\text{repeats}] = k - m\Big(1 - \big(1 - \tfrac{1}{m}\big)^k\Big)$$

For 32 bits $a = 1664525$ and $c = 1013904223$; for 16 bits $a = 25173$ and $c = 13849$.

Question: **is a generator that never repeats within its period a good random source?**

2. Period, and True Repeats

Computation 2.1: **the 32-bit generator's period, the time to use it up, and the draws to a true 32-bit first repeat were derived.**

quantity	value
full-period condition	satisfied
period	**4294967296**
time to use up (10^8 per second)	**42.949673** s
time to use up (10^9 per second)	**4.294967** s
draws to a true first repeat	**82137.861970**
as a fraction of the period	1.912421×10^{-5}

> **Observation 2.2**
>
> **true random numbers repeat far sooner than the period.Drawing 32-bit values, the first repeat comes after about 82137.861970 draws, while a full-period generator does not return to a state until 4294967296——never repeating within the period is a property true randomness does not have.**

3. Not Repeating Is the Mark

Computation 3.1: **the 16-bit generator was run 65536 steps to confirm its full period, and repeats among 5000 16-bit draws were compared, averaged over 200 trials.**

source	repeats (200-trial average)
true random numbers	**187.250000**
(expectation)	**185.940004**
state of the **16**-bit generator	**0.000000**
top **16** bits of the **32**-bit generator	**187.480000**

Observation 3.2

this is the core: a full-period generator that outputs its state never repeats.The 16-bit generator produced 65536 distinct values in 65536 steps and returned to its start, and repeats in 5000 draws were 0.000000—— true numbers would repeat 187.250000 times, so counting repeats alone tells them apart.

Observation 3.3

outputting only part of the state brings repeats back.The top 16 bits of the 32-bit generator repeat 187.480000 times, a relative difference of 0.008282 from expectation——the same value now comes from different states, so it repeats as true numbers do.

Observation 3.4

counting draws to the first repeat for true 16-bit numbers gave 321.254500 on average over 2000 trials.This follows the expectation 321.515086——the formula for repeats is confirmed by the trial.

4. The Separator

Observation 4.1

the separator is whether the output is the whole state or part of it.The whole state never repeats within the period, which marks it as not random; part of it repeats as true numbers do——"a longer period makes a better generator" has no truth value until one says what is output.

Observation 4.2

beside Paper 504.Paper 504 used a linear congruential generator as a tool and stated that its quality was not the subject——this counts that tool's period and repeats.

Observation 4.3

beside Paper 223 as well.Paper 223 showed that a linear congruential generator passing every test puts its triples on fifteen planes——here the simplest count, repeats of single values, is enough to distinguish a generator that outputs its state.

Observation 4.4

what is not said.Other tests, other generators and cryptographic use are not treated——what is shown is that never repeating can be a mark rather than a virtue.

5. Roll Call and Closing

1. **period 4294967296** (Computation 2.1): **32 bits.**
2. **used up in 4.294967 s** (Computation 2.1): **10^9 per second.**
3. **true first repeat 82137.861970** (Observation 2.2): **far sooner than the period.**
4. **true repeats 187.250000** (Computation 3.1): **in 5000 draws.**
5. **expectation 185.940004** (Computation 3.1): **as the formula says.**
6. **state itself 0.000000** (Observation 3.2): **the core.**
7. **upper bits 187.480000** (Observation 3.3): **repeats return.**
8. **relative difference 0.008282** (Observation 3.3): **like true numbers.**
9. **first repeat 321.254500** (Observation 3.4): **true 16-bit numbers.**
10. **whole state or part** (Observation 4.1): **the separator; Paper 504 and Paper 223.**

Closing: **A full-period linear congruential generator never repeats within its period, and never repeating is what marks it as not random.A 32-bit generator has period 4294967296, used up in 4.294967 s at 10^9 draws per second, while a true 32-bit random source first repeats after about 82137.861970 draws——never repeating within the period is a property true randomness does not have.Drawing 5000 16-bit values, true random numbers repeat 187.250000 times (expected 185.940004), a generator outputting its state 0.000000 times, and the top 16 bits of a 32-bit generator 187.480000 times——counting repeats alone tells a state-outputting generator from true randomness.The separator is whether the output is the whole state or part of it——"a longer period makes a better generator" has no truth value until one says what is output.Placed among the earlier papers——Paper 504 used the**

generator as a tool without asking its quality, and Paper 223 showed its structure in triples; this counts repeats of single values.To be honest——other tests, other generators and cryptographic use are not treated.

References

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. Yamagishi, Y. (2026). *It Passes Every Test, and the Points Lie on Fifteen Planes* [Paper 223]. Zenodo. 10.5281/zenodo.22120728
4. Yamagishi, Y. (2026). *Falling Noise and Non-Falling Noise Are Not Two Noises but Two Ends of One Expression* [Paper 504]. Zenodo. 10.5281/zenodo.22861737

— *From thinking to syncing.* —

Yuuki YAMAGISHI (山岸 勇輝)

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