p-adic Pseudorandom Number Generators

Etienne Pema Lafleur

Abstract

This paper builds pseudorandom number generators by iterating a function on the p-adic integers $\mathbb{Z}_p$. The main tool is a theorem of Anashin, which states that for 1-Lipschitz functions on $\mathbb{Z}_p$, measure-preservation and ergodicity can be checked by looking at the reduction of the function mod p^k for each k. When these conditions hold, iterating the function gives uniform output and the longest possible period at every working precision. We provide the construction, a small worked example, and a short note on what the framework does not provide.

1 Introduction

A pseudorandom number generator, or PRNG, is a deterministic algorithm that takes an input called a seed and produces a sequence of outputs that appear random. Pseudorandom number generators are ubiquitous in cryptography. [5]. A PRNG is expected to satisfy three key properties: outputs that are uniformly distributed, a long period before the sequence repeats, and unpredictability, meaning an attacker who has seen part of the sequence cannot easily guess what comes next.

One way to build a PRNG is to iterate a function. Pick a state space X, a map $f : X \to X$, and a seed $x_0 \in X$, then set $x_{n+1} = f(x_n)$ and read off some part of each x_n as output. This paper looks at what happens when X is the ring of p-adic integers $\mathbb{Z}_p$.

The reason $\mathbb{Z}_p$ is a suitable choice is that it aligns well with how computers operate in practice. A computer at finite precision is really computing in $\mathbb{Z}/p^k\mathbb{Z}$, and $\mathbb{Z}_p$ is built from all of these finite rings at once. There is also a natural notion of uniform distribution on $\mathbb{Z}_p$, called Haar measure, which becomes the ordinary uniform distribution on each $\mathbb{Z}/p^k\mathbb{Z}$.

The main tool is a theorem of Anashin [1]. It states that for a 1-Lipschitz function f on $\mathbb{Z}_p$, the dynamical properties we want—measure-preservation and ergodicity—can be checked by looking at the reduction of f mod p^k for each k. When the conditions hold, iterating f gives uniform output and the longest possible period at every working precision.

The rest of the paper goes as follows. Section 2 sets up $\mathbb{Z}_p$. Section 3 introduces 1-Lipschitz functions. Section 4 states Anashin's theorem. Section 5 gives the construction and a worked example. Section 6 concludes.

2 The p-adic integers

Fix a prime p. The p-adic integers $\mathbb{Z}_p$ use a distance in which two integers are close when their difference is divisible by a high power of p. For a full treatment, see Gouvêa [4].

2.1 The p-adic absolute value

For a nonzero integer n, write $n = p^v m$ where m is not divisible by p, and set $v_p(n) = v$. Define $v_p(0) = \infty$. The p-adic absolute value is

$$|n|_p = p^{-v_p(n)},$$

with $|0|_p = 0$. So an integer that is divisible by a large power of p is small in absolute value. It satisfies a stronger version of the triangle inequality:

$$|x + y|_p \leq \max\big(|x|_p, |y|_p\big).$$

A distance with this property is called an ultrametric.

2.2 Two views of $\mathbb{Z}_p$

There are two ways to think about $\mathbb{Z}_p$. The first is to complete $\mathbb{Z}$ with respect to the distance $|x - y|_p$, the same way one builds $\mathbb{R}$ from $\mathbb{Q}$. Every element $x \in \mathbb{Z}_p$ has a unique expansion

$$x = \sum_{i=0}^{\infty} a_i p^i, \qquad a_i \in \{0, 1, \ldots, p-1\}.$$

These are the base-p digits of x, and they will be the output of our PRNG.

The second way is the inverse limit

$$\mathbb{Z}_p \;=\; \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}.$$

An element is a list $(x_1, x_2, x_3, \ldots)$ with $x_k \in \mathbb{Z}/p^k\mathbb{Z}$, where each x_{k+1} reduces to x_k mod p^k. We write $x \bmod p^k$ for the truncation of x at level k. A computer working at precision p^k stores $x \bmod p^k$.

2.3 The key fact

The link between the distance and the truncations is:

$$|x - y|_p \leq p^{-k} \iff x \equiv y \pmod{p^k}.$$

So x and y are close to precision p^k exactly when their first k digits agree.

2.4 Haar measure

The space $\mathbb{Z}_p$ is compact, and as a group under addition, it has a unique translation-invariant probability measure μ, called Haar measure. On the residue classes mod p^k:

$$\mu\big(\{x \in \mathbb{Z}_p : x \equiv a \pmod{p^k}\}\big) = \frac{1}{p^k}$$

for every a and every $k \geq 1$. So Haar measure on $\mathbb{Z}_p$ becomes the uniform distribution on $\mathbb{Z}/p^k\mathbb{Z}$ when you reduce mod p^k. This is what makes $\mathbb{Z}_p$ a good state space for a PRNG: uniform output at every working precision comes from a single measure.

3 1-Lipschitz functions

A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is *1-Lipschitz* if

$$|f(x) - f(y)|_p \leq |x - y|_p$$

for all $x, y \in \mathbb{Z}_p$. By the key fact, this is the same as saying that for every k,

$$x \equiv y \pmod{p^k} \implies f(x) \equiv f(y) \pmod{p^k}.$$

This is the property we need for computation. If f is 1-Lipschitz, then for each k the rule

$$f_k(x \bmod p^k) := f(x) \bmod p^k$$

gives a well-defined function

$$f_k : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}.$$

This is the reduction of f mod p^k. Iterating f on $\mathbb{Z}_p$ and then reducing mod p^k gives the same answer as iterating f_k on $\mathbb{Z}/p^k\mathbb{Z}$ directly. So the dynamics on $\mathbb{Z}_p$ and on each finite quotient agree, and the computer only needs to run f_k.

Many natural functions are 1-Lipschitz. Polynomials with integer coefficients $f(x) \in \mathbb{Z}[x]$ are 1-Lipschitz, since $f(x) - f(y) = (x - y) \cdot g(x, y)$ for some $g \in \mathbb{Z}[x, y]$, and $|g(x, y)|_p \leq 1$. In particular, affine maps $f(x) = ax + b$ with $a, b \in \mathbb{Z}_p$ are 1-Lipschitz. Sums, products, and compositions of 1-Lipschitz functions are 1-Lipschitz.

4 Anashin's theorem

A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is *measure-preserving* if

$$\mu\big(f^{-1}(A)\big) = \mu(A)$$

for every measurable set A. This means f does not crowd outputs into any region: applying f to a uniform random input gives a uniform random output.

A measure-preserving f is *ergodic* if the only measurable sets A with $f^{-1}(A) = A$ have $\mu(A) = 0$ or $\mu(A) = 1$. By the Birkhoff ergodic theorem [6], this means almost every orbit visits each residue class mod p^k with

the right frequency, for every k. So measure-preservation gives uniform output at each step, and ergodicity guarantees that the orbit actually explores all of $\mathbb{Z}_p$.

Both definitions involve all measurable subsets, so they appear difficult to check. Anashin's theorem makes them finitary.

Anashin's theorem. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be 1-Lipschitz, and for each $k \geq 1$ let f_k be its reduction mod p^k. Then:*

(i) *f is measure-preserving if and only if f_k is a bijection for every k.*

(ii) *f is ergodic if and only if f_k is a single cycle of length p^k for every k.*

For (i), f is measure-preserving exactly when the preimage of each residue class mod p^k has mass $1/p^k$. Since the p^k classes partition $\mathbb{Z}_p$ into equal pieces, this happens precisely when each class is the image of exactly one class, that is, when f_k is a bijection. For (ii), an ergodic map cannot have a nontrivial invariant set, so the orbit of any point under f_k must reach every element of $\mathbb{Z}/p^k\mathbb{Z}$, making f_k a single p^k-cycle. The reverse implications are the substantive parts of the proof, which appears in Anashin and Khrennikov [3].

Note that the conditions must hold for every k. A map whose reduction mod p is a full cycle but whose reduction mod p^2 is not a full cycle fails to be ergodic.

5 The PRNG construction

Fix a prime p and a 1-Lipschitz function f whose reductions f_k are all single p^k-cycles. By Anashin's theorem, f is measure-preserving and ergodic.

5.1 The recipe

1. Pick a seed $x_0 \in \mathbb{Z}_p$, given by its first k digits for some working precision p^k.
2. Iterate: $x_{n+1} = f(x_n)$.
3. Output $y_n = x_n \bmod p^m$ at step n, where $m \leq k$ is the output precision.

5.2 What we get

Period. Since f_k is a p^k-cycle, the sequence $x_n \bmod p^k$ has period exactly p^k, the longest possible. Each residue class mod p^m is hit exactly p^{k-m} times in one period.

Uniformity. Over one full period, every value in $\{0, 1, \ldots, p^m - 1\}$ appears exactly p^{k-m} times as an output. The empirical distribution is exactly uniform, not just close to it.

These guarantees follow purely from the cycle structure of f_k.

5.3 A worked example

Take $p = 2$ and $f(x) = 1 + 5x$. This is 1-Lipschitz because it is a polynomial with integer coefficients. For affine maps $f(x) = a + bx$ over $\mathbb{Z}_2$, ergodicity holds if and only if a is odd and $b \equiv 1 \pmod 4$. Here $a = 1$ and $b = 5$, so the condition is satisfied.

Starting from $x_0 = 0$ and iterating $x_{n+1} = (1 + 5x_n) \bmod 8$:

n	0	1	2	3	4	5	6	7	8
$x_n \bmod 8$	0	1	6	7	4	5	2	3	0

The orbit visits all eight residues mod 8 before returning to 0, so f_3 is a single 8-cycle. The output stream at precision $m = 1$, i.e. the parity of x_n, is

$$0,\ 1,\ 0,\ 1,\ 0,\ 1,\ 0,\ 1,$$

each bit appearing $4 = 2^{3-1}$ times, as predicted.

6 Conclusion

The p-adic integers are a natural state space for PRNGs because they hold all the finite rings $\mathbb{Z}/p^k\mathbb{Z}$ in one place. A 1-Lipschitz function on $\mathbb{Z}_p$ gives a compatible map on each $\mathbb{Z}/p^k\mathbb{Z}$, and Anashin's theorem translates the dynamical properties we want into finite cycle conditions. When those conditions hold, iterating f gives a PRNG with uniform output and the longest possible period at every working precision.

What the framework does not give is cryptographic unpredictability. The worked example shows why: an observer who knows f and sees one output can produce every future output by simply iterating f_k. Cryptographic unpredictability requires additional hardness assumptions on f that lie outside the dynamical framework. Anashin discusses this in subsequent work [2]. What the p-adic framework provides is a clean foundation for the statistical side of PRNG design, with the cryptographic side left to be addressed separately.

References

[1] V. Anashin, *Uniformly distributed sequences of p-adic integers*, Mathematical Notes **55** (1994), no. 1–2, 109–133.

[2] V. Anashin, *Pseudorandom number generation by p-adic ergodic transformations*, Cryptology ePrint Archive, Report 2004/263, 2004. `https://eprint.iacr.org/2004/263`

[3] V. Anashin and A. Khrennikov, *Applied Algebraic Dynamics*, de Gruyter Expositions in Mathematics, vol. 49, Walter de Gruyter, Berlin, 2009.

[4] F. Q. Gouvêa, *p-adic Numbers: An Introduction*, 3rd ed., Universitext, Springer, Cham, 2020.

[5] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd ed., Chapman & Hall/CRC, Boca Raton, FL, 2020.

[6] P. Walters, *An Introduction to Ergodic Theory*, Graduate Texts in Mathematics, vol. 79, Springer, New York, 1982.