LINEAR CONGRUENTIAL GENERATORS

Contents

We consider a finite dynamical system on $\{0, 1, \dots, m\}$

$$X_{n+1} = aX_n + c \qquad \mod m. \tag{0.1}$$

for some $a, c, m \in \mathbb{Z}$. Clearly, any orbit of the dynamical system (0.1) will be **eventually periodic**.

Question: How to choose a, c, m so that orbits of (0.1) look like random sequences?

- First choose m so that mod$-m$ operation is computationally simple.
- Requirements on a, c so that **period** is as **large** as possible.
- Requirements on a so **large potency**.
- **Spectral tests**

Remark 1. These are only necessary conditions in the sense that small period and potency give sequences with **poor statistical behavior**.

1. Conditions for large period

1.1. **Period length m.** Iff conditions for period m.

Theorem 1.1 (Theorem A pg.17 in Knuth)**.** *The LCG (X_0, a, c, m) has period m iff*

- *$gcd(c, m) = 1$.*
- *Writing $m = \prod_i p_i^{e_i}$ we have $a = 1 \sim p_i$ for all i.*

Proof. **Step 1:** (Reduction to the case where $m = p^e$): Suppose that $m = m_1 m_2$ with $\gcd(m_1, m_2) = 1$. We form the sequences

$$Y_n = X_n \sim m_1 \qquad\qquad Z_n = X_n \sim m_2.$$

Then, if $X_n = X_k \sim m$

$$Y_n = \underbrace{(X_k + qm_1m_2)}_{X_n} + rm_1 = X_k + m_1(qm_2 + r)$$

so we must have $Y_n = Y_k \sim m_1$. Similarly $Z_n = Z_k$. A similar reasoning shows $X_n = X_k \sim m$ iff $Y_n = Y_k \sim m_1$ and $Z_n = Z_k \sim m_2$. Thus, the period λ of X_n satisfies $\lambda = \gcd(\lambda_1, \lambda_2)$.

Step 2: (Proof for $m = p^e$): W.l.o.g take $X_0 = 0$. An elementary computation shows that

$$X_n = \frac{a^n - 1}{a - 1} c \sim m$$

- We must have $\gcd(c, m) \neq 1$: If not we cannot have $X_n = 1$ (write $m = cm'$).
- $\lambda = p^e$ iff
$$a = 1 \sim p \qquad (\text{if } p > 2) \qquad\qquad a = 1 \sim 4 \qquad (\text{if } p = 2)$$
$\Rightarrow$ suppose $\lambda = p^e$. If $a \neq 1 \mod p$ is easy to see that $(a^n - 1)/(a-1) = 0 \sim p^e$ iff $a^n - 1 = 0 \sim p^e$. **finish this direction**

  $\Leftarrow$ Suppose $a = 1 + qp^f$ with $q \notin \mathbb{Z}p$ and $f < e$:
(p^e is a multiple of λ): By the auxiliary lemma below for any $g \in \mathbb{N}$
$$a^{p^g} = 1 \sim p^{f+g} \qquad \text{but} \qquad a^{p^g} \neq 1 \sim p^{f+g+1}.$$
Thus, for any $g \in \mathbb{N}$
$$(a^{p^g} - 1)/(a-1) = 0 \sim p^g \qquad \text{but} \qquad (a^{p^g} - 1)/(a-1) \neq 0 \sim p^{g+1} \tag{1.1}$$
In particular holds for $g = e$ and (**key:**)
$$(a^{p^e} - 1)/(a-1) = 0 \sim p^e.$$
Hence, p^e must be a multiple of λ (the period). In particular, since p is prime, we must have $\lambda = p^{\tilde{g}}$ for some $\tilde{g} \leqslant e$.
($p^e = \lambda$): On the other hand, from the definition of the period $\lambda = p^{\tilde{g}}$, it must satisfy
$$(a^{p^{\tilde{g}}} - 1)/(a-1) = 0 \sim p^e.$$
But writing $p^e = p^{\tilde{g}} p^{e-\tilde{g}}$ the second inequality in (1.1) implies that $\tilde{g} = e$.

Step 3: (Proof auxiliary lemma): We want to show that for p prime, if
$$x = 1 \sim p^e \qquad\qquad x \neq 1 \sim p^{e+1}$$
then
$$x^p = 1 \sim p^{e+1} \qquad\qquad x^p \neq \sim p^{e+2}.$$
This is easy if we write $x = 1 + qp^e$ with $\gcd(q, p) = 1$. □

1.2. Maximal period length if $c = 0$.

Theorem 1.2 (Theorem B pg. 20 in Knuth)**.**

We now give iff conditions to find primitive elements mod m.

Theorem 1.3 (Theorem C pg. ... in Knuth)**.**

2. Relevant examples

- **L'Ecuyer:**
$$m = 2^{64} \qquad\qquad a = 3202034522624059733 \qquad\qquad c = 1.$$