1.4 The Maximum Period Length

Under what conditions does the period of a linear congruential generator with module \( m \) attain the theoretic maximum length \( m \)? A multiplicative generator will never attain this period since the output 0 reproduces itself forever. Thus for this question we consider mixed generators with nonzero increment. As the trivial generator with generating function \( s(x) = x + 1 \mod m \) shows the period length \( m \) really occurs; on the other hand this example also shows that a period of maximum length is insufficient as a proof of quality for a random generator. Nevertheless maximum period is an important criterion, and the general result is easily stated:

**Proposition 1** (Hull/Dobell 1962, Knuth) The linear congruential generator with generating function \( s(x) = ax + b \mod m \) has period \( m \) if and only if the following three conditions hold:

(i) \( b \) and \( m \) are coprime.

(ii) Each prime divisor \( p \) of \( m \) divides \( a - 1 \).

(iii) If \( 4 \) divides \( m \), then \( 4 \) divides \( a - 1 \).

From the first condition we conclude \( b \neq 0 \), hence the generator is mixed. Before giving the proof of the proposition we state and prove a lemma. (We’ll use two more lemmas from Part III, Appendix A, that we state here without proofs.)

**Lemma 1** Let \( m = m_1 m_2 \) with coprime natural numbers \( m_1 \) and \( m_2 \). Let \( \lambda, \lambda_1, \) and \( \lambda_2 \) be the periods of the congruential generators \( x_n = s(x_{n-1}) \mod m, \mod m_1, \mod m_2 \) with initial value \( x_0 \) in each case. Then \( \lambda \) is the least common multiple of \( \lambda_1 \) and \( \lambda_2 \).

**Proof.** Let \( x_n^{(1)} \) and \( x_n^{(2)} \) be the corresponding outputs for \( m_1 \) and \( m_2 \). Then \( x_n^{(i)} = x_n \mod m_i \). Since \( x_{n+\lambda} = x_n \) for all sufficiently large \( n \) we immediately see that \( \lambda \) is a multiple of \( \lambda_1 \) and \( \lambda_2 \). On the other hand from \( m \mid t \iff m_1, m_2 \mid t \) we get

\[
x_n = x_k \iff x_n^{(i)} = x_k^{(i)} \quad \text{for } i = 1 \text{ and } 2.
\]

Hence \( \lambda \) is not larger than the least common multiple of \( \lambda_1 \) and \( \lambda_2 \). \( \square \)

The two lemmas without proofs:

**Lemma 2** Let \( n = 2^e \) with \( e \geq 2 \).

(i) If \( a \) is odd, then

\[
a^{2^s} \equiv 1 \pmod{2^{s+2}} \quad \text{for all } s \geq 1.
\]
(ii) If $a \equiv 3 \pmod{4}$, then $n \mid 1 + a + \cdots + a^{n/2-1}$.

**Lemma 3** Let $p$ be prime, and $e$, a natural number with $p^e \geq 3$. Assume $p^e$ is the largest power of $p$ that divides $x - 1$. Then $p^{e+1}$ is the largest power of $p$ that divides $x^p - 1$.

**Proof of the proposition** For both directions we may assume $m = p^e$ where $p$ is prime by Lemma 1.

"⇒": Each residue class in $[0 \ldots m - 1]$ occurs exactly once during a full period. Hence we may assume $x_0 = 0$. Then

$$x_n = (1 + a + \cdots + a^{n-1}) \cdot b \mod m \quad \text{for all } n.$$  

Since $x_n$ assumes the value 1 for some $n$ we conclude that $b$ is invertible mod $m$, or that $b$ and $m$ are coprime.

Let $p \mid m$. From $x_m = 0$ we now get $m \mid 1 + a + \cdots + a^{m-1}$, hence

$$p \mid m \mid a^m - 1 = (a - 1)(1 + a + \cdots + a^{m-1}).$$

Fermat’s little theorem gives $a^p \equiv a \pmod{p}$, hence

$$a^m = a^{p^e} \equiv a^{p^e-1} \equiv \ldots \equiv a \pmod{p},$$

hence $p 
\mid a - 1$. This proves (ii).

Statement (iii) corresponds to the case $p = 2$ with $e \geq 2$. From (ii) we get that $a$ is even. The assumption $a \equiv 3 \pmod{4}$ would result in the contradiction $x_{m/2} = 0$ by Lemma 2. Hence $a \equiv 1 \pmod{4}$.

"⇐": Again we may assume $x_0 = 0$. Then

$$x_n = 0 \iff m \mid 1 + a + \cdots + a^{n-1}.$$  

In particular the case $a = 1$ is trivial. Hence assume $a \geq 2$. Then

$$x_n = 0 \iff m \mid \frac{a^n - 1}{a - 1}. $$

We have to show:

- $m \mid \frac{a^{m-1}}{a-1}$—then $\lambda \mid m$;
- $m$ doesn’t divide $\frac{a^{m/p-1}}{a-1}$—then $\lambda \geq m$ since $m$ is a power of $p$.

Let $p^h$ be the maximum power that divides $a - 1$. By Lemma 3 we conclude

$$a^p \equiv 1 \pmod{p^{h+1}}, \quad a^p \not\equiv 1 \pmod{p^{h+2}}$$

and successively

$$a^{p^k} \equiv 1 \pmod{p^{h+k}}, \quad a^{p^k} \not\equiv 1 \pmod{p^{h+k+1}}.$$
for all $k$. In particular $p^{k+e} \mid a^m - 1$. Since no larger power than $p^h$ divides $a - 1$ we conclude that $m = p^e \mid \frac{a^m - 1}{a - 1}$. The assumption $p^e \mid \frac{a^{m/p^e} - 1}{a - 1}$ leads to the contradiction $p^{e+h} \mid a^{p^e - 1} - 1$. ♦

The main application of Proposition 1 is for modules that are powers of 2:

**Corollary 1** (Greenberger 1961) For the module $m = 2^e$ with $e \geq 2$ the period $m$ is attained if and only if:

(i) $b$ is odd.

(ii) $a \equiv 1 \pmod{4}$.

For prime modules Proposition 1 is useless, as the following corollary shows.

**Corollary 2** For a prime module $m$ the period $m$ is attained if and only if $b$ is coprime with $m$ and $a = 1$.

This (lousy) result admits an immediate generalization to squarefree modules $m$:

**Corollary 3** For a squarefree module $m$ the period $m$ is attained if and only if $b$ is coprime with $m$ and $a = 1$.

In summary Proposition 1 shows how to get the maximum possible period, and Corollary 1 provides a class of half-decent useful examples.