2.4 Linear Congruential Generators with Known Module

This section uses elementary methods only and is independent of the general theory from the preceding sections of Chapter 2.

Assume the parameters $a$ and $b$ of the linear congruential generator $x_n = ax_{n-1} + b \mod m$ are unknown, whereas the module $m$ is known.

We’ll show that for predicting the complete output sequence we only need 3 successive elements $x_0, x_1, x_2$ of the sequence, even for a composite module $m$. Starting with the relation

$$x_2 - x_1 \equiv a(x_1 - x_0) \pmod{m}$$

we immediately get (assuming for the moment that $x_1 - x_0$ and $m$ are coprime)

$$a = \frac{x_2 - x_1}{x_1 - x_0} \mod m,$$

where the division is mod $m$ (using the extended Euclidean algorithm). The increment $b$ is given by

$$b = x_1 - ax_0 \mod m.$$

So we found the defining formula and may predict the complete sequence.

A typical tool for this simple case was the sequence of differences

$$y_i = x_i - x_{i-1} \text{ for } i \geq 1.$$ 

It follows the rule

$$y_{i+1} \equiv ay_i \pmod{m}.$$

Note that the $y_i$ may be negative lying between the bounds $-m < y_i < m$. Since $m$ is known we might replace them by $y_i \mod m$, but this was irrelevant in the example, and for an unknown $m$—to be considered later on—it is not an option.

**Lemma 6** (on the sequence of differences) Assume the sequence $(x_i)$ is generated by the linear congruential generator with module $m$, multiplier $a$, and increment $b$. Let $(y_i)$ be the sequence of differences, $c = \gcd(m, a)$, and $d = \gcd(m, y_1)$. Then:

(i) The following statements are equivalent:
   (a) The sequence $(x_i)$ is constant.
   (b) $y_1 = 0$.
   (c) $y_i = 0$ for all $i$.
(ii) $\gcd(m, y_i) | \gcd(m, y_{i+1})$ for all $i$.
(iii) $d | y_i$ for all $i$. 


Proposition 7 Assume the sequence \((x_i)\) is generated by a linear congruential generator with known module \(m\), but unknown multiplier \(a\) and increment \(b\). Then the complete output sequence is predictable from its first three

Proof. (i) Note that \(y_i = 0\) implies that all following elements are 0.
(ii) If \(c\) divides \(y_i\) and \(m\), then it also divides \(y_{i+1} = ay_i + km\).
(iii) is a special case of (ii).
(iv) follows from \(d | \gcd(y_1, \ldots, y_t)\), and this, from (iii).
(v) Let \(m = cn\) and \(a = ca\). Then \(y_{i+1} = cay_i + km\), hence \(c|y_{i+1}\) for \(i \geq 1\).
(vi) follows from \(c | \gcd(y_2, \ldots, y_t)\) and this, from (v).
(vii) \(y_iy_{i+2} - y_{i+1}^2 \equiv a^2y_i - a^2y_i\) (mod \(m\)).
(viii) by induction: For \(i = 1\) the assertion is the definition of \(b\). For \(i \geq 2\) we have
\[
x_i - \tilde{a}x_{i-1} - \tilde{b} \equiv x_i - \tilde{a}x_{i-1} - x_{i-1} + \tilde{a}x_{i-2} \equiv y_i - \tilde{a}y_{i-1} \equiv 0 \pmod{\tilde{m}},
\]
as claimed. ◊

The trivial case of a constant sequence merits no further care. However it shows that in general the parameters of a linear congruential generator are not uniquely determined by the output sequence. For the constant sequence may be generated with an arbitrary module \(m\) and an arbitrary multiplier \(a\) if only the increment is set to \(b = -(a - 1)x_0 \mod m\). Even if \(m\) is fixed \(a\) is not uniquely determined, not even \(a \mod m\).

Previously we considered the case where \(y_1\) and \(m\) are coprime, yielding \(a = y_2/y_1 \mod m\). In the general case it might happen that division \(m\) is not unique. This happens if and only if \(m\) and \(y_1\) have a non-trivial common divisor, hence \(d = \gcd(m, y_1) > 1\). The sequence of reduced differences \(\bar{y}_i = y_i/d\) (see (iii) in Lemma 6) then follows the recursive formula
\[
\bar{y}_{i+1} \equiv \bar{a}\bar{y}_i \pmod{\bar{m}}
\]
with the reduced module \(\bar{m} = m/d\) and reduced multiplier \(\bar{a} = a \mod \bar{m}\), from which we get a unique \(\bar{a} = \bar{y}_2/\bar{y}_1\). Setting \(\bar{a} = \bar{a} + km\) with an arbitrary integer \(k\) and \(\bar{b} = x_1 - \bar{a}x_0 \mod m\), from Lemma 6 (viii) we also get \(x_i = \bar{a}x_{i-1} + \bar{b} \mod m\) for all \(i \geq 1\). This proves:
elements $x_0, x_1, x_2$. If the sequence $(x_i)$ is not constant, then the multiplier \( a \) is uniquely determined up to a multiple of the reduced module \( \bar{m} \).

Thus also in this situation we sometimes have to content ourselves with predicting the sequence without revealing the parameters used for its generation. Here is a simple concrete example: For \( m = 24 \), \( a = 2k + 1 \) with \( k \in [0 \ldots 11] \), \( b = 12 - 2k \) mod 24, and initial value \( x_0 = 1 \) we always get the sequence \( (1, 13, 1, 13, \ldots) \).