1.5 The Maximum Period of a Multiplicative Generator

A multiplicative generator $x_n = ax_{n-1} \mod m$ never has period $m$ since the output 0 reproduces itself. So what is the largest possible period? In the following proposition $\lambda$ is the Carmichael function, and this is exactly the context where it occurred for the first time.

**Proposition 2 (Carmichael 1910)** The maximum period of a multiplicative generator with generating function $s(x) = ax \mod m$ is $\lambda(m)$. A sufficient condition for the period $\lambda(m)$ is:

(i) $a$ is primitive mod $m$.

(ii) $x_0$ is relatively prime to $m$.

**Proof.** We have $x_n = a^n x_0 \mod m$. If $k = \text{ord}_m a$ is the order of $a$ in the multiplicative group of $\mathbb{Z}/m\mathbb{Z}$, then $x_k = x_0$. Thus the period is $\leq k \leq \lambda(m)$. Now assume $a$ is primitive mod $m$, hence $1, a, \ldots, a^{\lambda(m)-1} \mod m$ are distinct, and let $x_0$ be relatively prime to $m$. Then the $x_n$ are distinct for $n = 0, \ldots, \lambda(m) - 1$, and the period is $\lambda(m)$. ◇

**Corollary 1** Let $m = p$ prime. Then the generator has the maximum period $\lambda(p) = p - 1$ if and only if:

(i) $a$ is primitive mod $p$.

(ii) $x_0 \neq 0$.

Thus for prime modules we are in a comfortable situation: The period misses the maximum value for one-step recursive generators only by 1, and any initial value is good except 0.

Section 1.9 will broadly generalize this result.