Review. $x \pmod n$ is a primitive root.

$\iff$ The (multiplicative) order of $x \pmod n$ is $\phi(n)$. (That is, the order is as large as possible.)

$\iff$ $x, x^2, \ldots, x^{\phi(n)}$ is a list of all invertible residues modulo n.

Lemma 101. Suppose $x \pmod n$ has (multiplicative) order k.

(a) $x^a \equiv 1 \pmod n$ if and only if $k|a$.

(b) $x^a \equiv x^b \pmod n$ if and only if $a \equiv b \pmod k$.

(c) x^a has order $\frac{k}{\gcd(k,a)}$.

Proof.

(a) "$\Longrightarrow$": By Lemma 94, $x^k \equiv 1$ and $x^a \equiv 1$ imply $x^{\gcd(k,a)} \equiv 1 \pmod n$. Since k is the smallest exponent, we have $k = \gcd(k,a)$ or, equivalently, $k|a$.
"$\Longleftarrow$": Obviously, if $k|a$ so that $a = kb$, then $x^a = (x^k)^b \equiv 1 \pmod n$.

(b) Since x is invertible, $x^a \equiv x^b \pmod n$ if and only if $x^{a-b} \equiv 1 \pmod n$ if and only if $k|(a-b)$.

(c) By the first part, $(x^a)^m \equiv 1 \pmod n$ if and only if $k|am$. The smallest such m is $m = \frac{k}{\gcd(k,a)}$. □

Example 102. (homework) Redo Example 99, starting with the knowledge that 3 is a primitive root.

Solution.

residues	1	2	3	4	5	6
3^a	3^0	3^2	3^1	3^4	3^5	3^3
order$=\frac{6}{\gcd(a,6)}$	$\frac{6}{6}$	$\frac{6}{2}$	$\frac{6}{1}$	$\frac{6}{3}$	$\frac{6}{1}$	$\frac{6}{3}$

Example 103. (homework) Let p be a prime such that $p \equiv 3 \pmod 4$. Show that $\phi\left(\frac{p-1}{2}\right) = \phi(p-1)$.

Solution. First, note that $p-1$ is divisible by 2 but not by 4.

Hence, $p-1 = 2m$ with $m = \frac{p-1}{2}$, and the factors 2 and m are coprime.

Therefore, $\phi(p-1) = \phi(2)\phi(m) = \phi(m)$.

Armin Straub
straub@southalabama.edu

Example 104. In Example 77, we used the B-B-S PRG with $M=77$ and seed 3.

Recall that $y_0=3$ and that $y_{n+1}\equiv y_n^2 \pmod{77}$. Hence, $y_1=9$, $y_2=4$, $y_3=16$, $y_4=25$, $y_5=9$, so that the values y_n now start repeating. (The actual output of the PRG is just the least bit of each y_n.)

Can you see how to predict that the y_n's eventually repeat with a period of 4?

Solution. (poor) As we observed earlier, there are only $\phi(77)/4=15$ invertible quadratic residues. Hence, the period can be at most 15. However, this is a terrible overestimate. The actual period is considerably smaller and we can easily get a better estimate.

Solution.

- Observe that the numbers (of which the last bit is output) are $y_n=y_{n-1}^2=y_{n-2}^4=\ldots=y_0^{2^n} \pmod{M}$. Hence, $y_n\equiv y_0^{2^n} \pmod{M}$.
- Instead of determining the period directly modulo $M=pq$, we determine the periods modulo p and q. [Why? By the CRT, $y_m\equiv y_n \pmod{M}$ if and only if $y_m\equiv y_n \pmod{p}$ and $y_m\equiv y_n \pmod{q}$.] The period modulo M then is the lcm of of the two periods modulo p and q.
- $y_m\equiv y_n \pmod{p}$ if and only if $y_0^{2^m}\equiv y_0^{2^n} \pmod{p}$. This happens if $2^m\equiv 2^n \pmod{\phi(p)}$.
  Comment. More precisely, $y_m\equiv y_n \pmod{p}$ if and only if $2^m\equiv 2^n \pmod{k}$ where k is the order of $y_0 \pmod{p}$. Example 106 indicates that, a random y_0 is likely to have order $\phi(p)$ or close to that.
- Since $m,n\geqslant 1$, $2^m\equiv 2^n \pmod{p-1}$ is equivalent to $2^m\equiv 2^n \left(\mathrm{mod}\,\frac{p-1}{2}\right)$ or $2^{m-n}\equiv 1 \left(\mathrm{mod}\,\frac{p-1}{2}\right)$. For the latter, we used that $p\equiv 3 \pmod{4}$, so that $\frac{p-1}{2}$ is not divisible by 2.
  Why?
- $2^{m-n}\equiv 1 \left(\mathrm{mod}\,\frac{p-1}{2}\right)$ if and only if $m-n$ (the period!) is a multiple of the order of $2 \left(\mathrm{mod}\,\frac{p-1}{2}\right)$.

In our example, the order of $2 \left(\mathrm{mod}\,\frac{7-1}{2}\right)$ is 2 (so that $y_n \pmod{7}$ repeats with period 2), and the order of $2 \left(\mathrm{mod}\,\frac{11-1}{2}\right)$ is 4 (so that $y_n \pmod{11}$ repeats with period 4).

We conclude that $y_n \pmod{77}$ must repeat with period $\mathrm{lcm}(2,4)=4$.

Hence, the period of the PRG must be a divisor of 4.

Comment. In practice, people say that, for the cycle length of B-B-S to be large, $\gcd(\phi(p-1),\phi(q-1))$ should be small. Can you see how our discussion leads to that conclusion? Also, see Example 103.