Review. The **multiplicative order** of an invertible residue a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$. The order always divides $\phi(n)$.

Definition 97. If the multiplicative order of an residue a modulo n equals $\phi(n)$ [in other words, the order is as large as possible], then a is said to be **primitive root** modulo n.

A primitive root is also referred to as a **multiplicative generator** (because the products of a, that is, $1, a, a^2, a^3, \ldots$, produce all invertible residues).

Example 98. Compute the multiplicative order of 2 modulo $7, 11, 9, 15$. In each case, is 2 a primitive root?

Solution.

- $2 \pmod 7$: $2^2 \equiv 4, 2^3 \equiv 1$. Hence, the order of 2 modulo 7 is 3.
  Since the order is less than $\phi(7) = 6$, 2 is not a primitive root modulo 7.
- $2 \pmod{11}$: Since $\phi(11) = 10$, the only possible orders are $2, 5, 10$. Hence, checking that $2^2 \not\equiv 1$ and $2^5 \not\equiv 1$ is enough to conclude that the order must be 10.
  Since the order is equal to $\phi(11) = 10$, 2 is a primitive root modulo 11.
- $2 \pmod 9$: Since $\phi(9) = 6$, the only possible orders are $2, 3, 6$. Hence, checking that $2^2 \not\equiv 1$ and $2^3 \not\equiv 1$ is enough to conclude that the order must be 6. (Indeed, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, $2^6 \equiv 1$.)
  Since the order is equal to $\phi(9) = 6$, 2 is a primitive root modulo 9.
- **(homework)** The order of $2 \pmod{15}$ is 4 (a divisor of $\phi(15) = 8$).
  2 is not a primitive root modulo 15. In fact, there is no primitive root modulo 15.

Comment. It is an open conjecture to show that 2 is a primitive root modulo infinitely many primes. (This is a special case of Artin's conjecture which predicts much more.)

Comment. There exists a primitive root modulo n if and only if n is of one of $1, 2, 4, p^k, 2p^k$ for some odd prime p.

Example 99. (homework) Determine the orders of each (invertible) residue modulo 7. In particular, determine all primitive roots modulo 7.

Solution. First, observe that, since $\phi(7) = 6$, the orders can only be $1, 2, 3, 6$. Indeed:

residues	1	2	3	4	5	6
order	1	3	6	3	6	2

The primitive roots are 3 and 5.

Example 100. 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, $y_1^2 = 9$, $y_2^2 = 4$, $y_3 = 16$, $y_4 = 25$, $y_5 = 9$, 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?

(To be continued.)

Armin Straub
straub@southalabama.edu