Primitive Roots mod *p*

Fermat's Little Theorem tells us that $a^{p-1} \equiv 1 \pmod{p}$ if p is prime $a \not\equiv 0 \pmod{p}$. Let us look at some examples

$p = 5$	**$p = 7$**		**$p = 13$**		**$p = 23$**		
$a = 2$	**$a = 2$**	**$a = 3$**	**$a = 2$**	**$a = 3$**	**$a = 2$**	**$a = 3$**	**$a = 5$**
$2^{0} \equiv 1$	$2^{0} \equiv 1$	$3^{0} \equiv 1$	$2^{0} \equiv 1$	$3^{0} \equiv 1$	$2^{0} \equiv 1$	$3^{0} \equiv 1$	$5^{0} \equiv 1$
$2^{1} \equiv 2$	$2^{1} \equiv 2$	$3^{1} \equiv 3$	$2^{1} \equiv 2$	$3^{1} \equiv 3$	$2^{1} \equiv 2$	$3^{1} \equiv 3$	$5^{1} \equiv 5$
$2^{2} \equiv 4$	$2^{2} \equiv 4$	$3^{2} \equiv 2$	$2^{2} \equiv 4$	$3^{2} \equiv 9$	$2^{2} \equiv 4$	$3^{2} \equiv 9$	$5^{2} \equiv 2$
$2^{3} \equiv 3$	$2^{3} \equiv 1$	$3^{3} \equiv 6$	$2^{3} \equiv 8$	$3^{3} \equiv 1$	$2^{3} \equiv 8$	$3^{3} \equiv 4$	$5^{3} \equiv 10$
$2^{4} \equiv 1$	$2^{4} \equiv 2$	$3^{4} \equiv 4$	$2^{4} \equiv 3$	$3^{4} \equiv 3$	$2^{4} \equiv 16$	$3^{4} \equiv 12$	$5^{4} \equiv 4$
	$2^{5} \equiv 4$	$3^{5} \equiv 5$	$2^{5} \equiv 6$	$3^{5} \equiv 9$	$2^{5} \equiv 9$	$3^{5} \equiv 13$	$5^{5} \equiv 20$
	$2^{6} \equiv 1$	$3^{6} \equiv 1$	$2^{6} \equiv 12$	$3^{6} \equiv 1$	$2^{6} \equiv 18$	$3^{6} \equiv 16$	$5^{6} \equiv 8$
			$2^{7} \equiv 11$	$3^{7} \equiv 3$	$2^{7} \equiv 13$	$3^{7} \equiv 2$	$5^{7} \equiv 17$
			$2^{8} \equiv 9$	$3^{8} \equiv 9$	$2^{8} \equiv 3$	$3^{8} \equiv 6$	$5^{8} \equiv 16$
			$2^{9} \equiv 5$	$3^{9} \equiv 1$	$2^{9} \equiv 6$	$3^{9} \equiv 18$	$5^{9} \equiv 11$
			$2^{10} \equiv 10$	$3^{10} \equiv 3$	$2^{10} \equiv 12$	$3^{10} \equiv 8$	$5^{10} \equiv 9$
			$2^{11} \equiv 7$	$3^{11} \equiv 9$	$2^{11} \equiv 1$	$3^{11} \equiv 1$	$5^{11} \equiv 22$
			$2^{12} \equiv 1$	$3^{12} \equiv 1$	$2^{12} \equiv 2$	$3^{12} \equiv 3$	$5^{12} \equiv 18$
					$2^{13} \equiv 4$	$3^{13} \equiv 9$	$5^{13} \equiv 21$
					$2^{14} \equiv 8$	$3^{14} \equiv 4$	$5^{14} \equiv 13$
					$2^{15} \equiv 16$	$3^{15} \equiv 12$	$5^{15} \equiv 19$
					$2^{16} \equiv 9$	$3^{16} \equiv 13$	$5^{16} \equiv 3$
					$2^{17} \equiv 18$	$3^{17} \equiv 16$	$5^{17} \equiv 15$
					$2^{18} \equiv 13$	$3^{18} \equiv 2$	$5^{18} \equiv 6$
					$2^{19} \equiv 3$	$3^{19} \equiv 6$	$5^{19} \equiv 7$
					$2^{20} \equiv 6$	$3^{20} \equiv 18$	$5^{20} \equiv 12$
					$2^{21} \equiv 12$	$3^{21} \equiv 8$	$5^{21} \equiv 14$
					$2^{22} \equiv 1$	$3^{22} \equiv 1$	$5^{22} \equiv 1$

Some observations on the table.

1) In all cases, $a^{p-1} \equiv 1 \pmod{p}$. We already knew this had to occur, by Fermat's Theorem.

2) For each prime p in the table, we can find some integer b (not divisible by p) such that $b^{i} \not\equiv 1 \pmod{p}$ for $0 < i < p-1$. In other words, $p-1$ is the *smallest* positive integer j such that $b^{j} \equiv 1 \pmod{p}$.

   We call b a primitive root mod p.

   2 is a primitive root mod 5, and also mod 13.
   3 is a primitive root mod 7.
   5 is a primitive root mod 23.

   It can be proven that there exists a primitive root mod p for *every* prime p. (However, the proof isn't easy; we shall omit it here.)

3) For each primitive root b in the table, $b^{0}, b^{1}, b^{2}, \ldots, b^{p-2}$ are all distinct in Z_p, and they constituted all the nonzero elements of Z_p.

   Again, this is always true, and easy to prove. We know that b has an inverse since $b \not\equiv 0 \pmod{p}$. If

   $$b^{i} \equiv b^{k} \pmod{p} \quad \text{for } 0 \le i < k \le p-2,$$

   then

   $$b^{i}(b^{-1})^{i} \equiv b^{k}(b^{-1})^{i} \;\Rightarrow\; b^{i}b^{-i} \equiv b^{k}b^{-i} \;\Rightarrow\; 1 \equiv b^{k-i} \pmod{p}$$

   and $0 < k-i \le k \le p-2$, which contradicts b being primitive.

4) For each prime in the table, we can find nonzero integers a that are not primitive roots mod p. In each case, if k is the smallest positive integer with $a^k \equiv 1 \pmod{p}$, then k divides $p-1$.

Once more, this always holds, and is easy to show. If it k does not divide $p-1$, write $p-1 = qk + r$, with $1 \le r < k$. ($r \ne 0$ since k does not divide $p-1$.) Then

$$a^{p-1} \equiv a^{qk+r} \Rightarrow a^{p-1} \equiv (a^k)^q a^r \Rightarrow 1 \equiv 1^q a^r \Rightarrow a^r \equiv 1 \pmod{p}$$

which contradicts k being the *smallest* positive integer with $a^k \equiv 1 \pmod{p}$.

The smallest positive integer k with $a^k \equiv 1 \pmod{p}$ is called the *order of a* mod p. I will write the order of a as $o(a)$. (Recall it depends on p).

We have shown that $o(a)$ divides $p-1$ for all $a \not\equiv 0 \pmod{p}$. Note a is a primitive root if and only if $o(a) = p-1$.

5) In the table, whenever b is a primitive element mod p, then every integer x with $x \not\equiv 0 \pmod{p}$ is a power of b, i.e., $x \equiv b^k$ for some integer k.

Again, this is true in general, and follows immediately from (3).

However, given x, we have no practical way to find k, assuming p is large.

Computing k involves finding a discrete logarithm, and finding discrete logarithms with a large prime base is (as far as anyone knows) too difficult to be practical. (Much of public key cryptography would collapse if an efficient algorithm for discrete logs were discovered.)

6) If b is a primitive root mod p, then $o(b^k) = (p-1) / \gcd(p-1,k)$.

$$\begin{aligned} \text{Let}\quad d &= \gcd\,(p-1,k), \\ p-1 &= ud \\ k &= vd. \end{aligned}$$

If $(b^k)^m \equiv 1$, then $b^{km} \equiv 1$, so $(p-1) \mid km$ and $(p-1)/d \mid (k/d)m$.

Since $(p-1)/d$ and k/d are relatively prime, we conclude $(p-1)/d \mid m$. In other words, $(p-1)/\gcd(p-1,k)$ divides m. In particular, $(p-1)/\gcd(p-1,k)$ divides $o(b^k)$.

$(b^k)^{(p-1)/d} \equiv (b^{vd})^{(p-1)/d} \equiv b^{(p-1)v} \equiv 1 \pmod{p}$, so $o(b^k)$ divides $(p-1)/d = (p-1)/\gcd(p-1,k)$.

So $o(b^k) = (p-1)/\gcd(p-1,k)$.

7) If b is any primitive root mod p, then the set of all primitive roots mod p is exactly $\{b^k \mid \gcd(p-1,k) = 1\}$. The number of primitive roots mod p is $\varphi(p-1)$.

For example, consider the case $p = 13$ in the table.

$\varphi(p-1) = \varphi(12) = \varphi(2^2 3) = 12(1-1/2)(1-1/3) = 4.$

If b is a primitive root mod 13, then the complete set of primitive roots is $\{b^1, b^5, b^7, b^{11}\}$. We see from the table that 2 is a primitive root mod 13.. The complete set of primitive roots mod 13 is $\{2^1, 2^5, 2^7, 2^{11}\} = \{2, 6, 11, 7\}$.