Primitive Roots

Lemma : (10.2)

If f is a polynomial of degree n, then

$$f(x) \equiv 0 \mod p$$

has at most n solutions

Proof. Let $f(n)$ be a polynomial of degree n

$$f(n) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

For $n = 1$, the polynomial has one solution since $(a_1, p) = 1$

$$a_1 x + a_0 \equiv 0 \mod p$$

Suppose that the lemma is true for polynomials of degree $n-1$. Let $f(n)$ be a polynomial of degree n. Either $f(x) \equiv 0 \mod p$ has no solutions, or it has at least one. If $f(x) \equiv 0 \mod p$ has no solutions, then it has at most n solutions. In the second case, suppose that r is a solution, that is $f(r) \equiv 0 \mod p$. Then, because $x - r$ is a factor of $x^t - r^t$ for $t = 0, 1, \ldots, n$, we have

$$\begin{aligned} f(x) &\equiv f(x) - f(r) \\ &\equiv a_n (x^n - r^n) + a_{n-1} \left(x^{n-1} - r^{n-1}\right) + \cdots + a_1 (x - r) \\ &\equiv (x - r) g(x) \mod p \end{aligned}$$

Where $g(x)$ is of degree $n - 1$. Suppose that s is also a solution of $f(x) \equiv 0 \mod p$. Then,

$$f(s) = (s - r) g(s) \equiv 0 \mod p$$

Since p is a prime, it follows that $s \equiv r \mod p$ or $g(s) \equiv 0 \mod p$. From the induction assumption, the second congruence has at most $n - 1$ solutions, so in total there are at most n solutions. □

Note that Lemma 10.2 is not true if the modulus is not prime. For example, the polynomial equation

$$x^2 + x \equiv 0 \mod 6$$

Has the solutions $x = 0, 2, 3$, and 5

Lemma : (10.3)

If $d \mid p - 1$, then $x^d \equiv 1 \mod p$ has exactly d solutions.

Proof. From Fermat's Theorem, we have that the congruence

$$x^{p-1} \equiv 1 \mod p$$

has exactly $p - 1$ solutions, which are

$$1, \quad 2, \quad \ldots, \quad p - 1$$

However, notice that we have

$$\begin{aligned} x^{p-1}-1 &= \left(x^d-1\right)\left(x^{p-1-d}+x^{p-1-2d}+\cdots+1\right) \\ &= \left(x^d-1\right)h\left(x\right) \end{aligned}$$

From Lemma 10.2, $h\left(x\right) \equiv 0 \mod p$ has at most $p-1-d$ solutions. Hence $x^d \equiv 1 \mod p$ has at least d solutions. By Lemma 10.2, $x^d \equiv 1 \mod p$ also has at most d solutions. Therefore, we see that $x^d \equiv 1 \mod p$ has exactly d solutions. □

Theorem : (10.6)

Every prime p has $\phi\left(p-1\right)$ primitive roots.

Proof. Theorem 10.2 says that each of the integers

$$1, \quad 2, \quad \ldots, \quad p-1$$

has an order that is a divisor of $p-1$. For each divisor t of $p-1$, let $\psi\left(t\right)$ denote the number of integer that have order t. This can be restated as

$$\sum_{t|p-1} \psi\left(t\right) = p-1$$

From Theorem 9.4, we have that

$$\sum_{t|p-1} \psi\left(t\right) = \sum_{t|p-1} \phi\left(t\right)$$

If we can show that $\psi\left(t\right) \leq \phi\left(t\right)$ for each t, it will follow from

$$\sum_{t|p-1} \psi\left(t\right) = \sum_{t|p-1} \phi\left(t\right)$$

that $\psi\left(t\right) = \phi\left(t\right)$ for each t. In particular, the number of primitive roots of p will be

$$\psi\left(p-1\right) = \phi\left(p-1\right)$$

If $\psi\left(t\right) = 0$, then $\psi\left(t\right) < \phi\left(t\right)$ and we are done. If $\psi\left(t\right) \neq 0$, then there is an integer with order t, call it a. By Lemma 10.3, $x^t \equiv 1 \mod p$ has exactly t solutions. Furthermore, the integers $a, a^2, \ldots, a^t$ satisfy the congruence. By Theorem 10.4, no two powers have the same least residue. Therefore, they give all the solutions to $x^t \equiv 1 \mod p$. From Lemma 10.1, the numbers in $a, a^2, \ldots, a^t$ that have order t are those powers of a^k with $(k,t) = 1$. There are $\phi\left(t\right)$ such numbers k. Hence $\psi\left(t\right) = \phi\left(t\right)$ in this case. That is, there are $\phi\left(p-1\right)$ primitive roots. □

Theorem 10.6 does not actually help us to find a primitive root. We do not have an efficient way to find primitive roots, since they behave pseudo-randomly. They can also be composite, for example, 6 is the smallest for 41.

Theorem

The only positive integers with primitive roots are 1, 2, 4, p^e, and $2p^e$, where p is an odd prime.