Primitive Roots of Primes

In this section, we prove that every prime has a primitive root.

Definition: Let $f(x)$ be a polynomial with integer coefficients. We say that an integer c is a root of $f(x)$ modulo m if $f(c) \equiv 0 \pmod{m}$.

Exercise: Show that, if $f(c) \equiv 0 \pmod{m}$ and $d \equiv c \pmod{m}$, then $f(d) \equiv 0 \pmod{m}$.

ex: Let $f(x) = x^2 + x + 1$. Then, $f(x)$ has exactly two incongruent roots modulo 7, namely $x \equiv 2 \pmod{7}$ and $x \equiv 4 \pmod{7}$.

ex: $f(x) = x^2 + 2$ has no roots modulo 5.

ex: Let $h(x) = x^{p-1} - 1$ where p is a prime. By Fermat's little theorem, $h(x)$ has exactly $p-1$ incongruent roots modulo p, namely $x \equiv 1, 2, 3, \ldots, p-1 \pmod{p}$.

Theorem 9.6: Lagrange's Theorem

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree n, $n \geq 1$, with integer coefficients and with leading coefficient a_n not divisible by p. Then, $f(x)$ has at most n incongruent roots modulo p.

Proof: We use mathematical induction on n.

Let $n = 1$.

Then, $f(x) = a_1 x + a_0$ with $p \nmid a_1$.

The roots of $f(x) \equiv 0 \pmod{p}$ are the roots of the linear congruence

$$a_1 x + a_0 \equiv 0 \pmod{p}$$

$$\Rightarrow \quad a_1 x \equiv -a_0 \pmod{p}.$$

Since $\gcd(a_1, p) = 1$, by Theorem 4.10, this linear congruence has a unique solution modulo p.

Hence, the result holds for $n = 1$.

Next, suppose the result holds for all polynomials of degree $n-1$.

Let $f(x)$ be a polynomial of degree n with leading coefficient not divisible by p.

We use the method of contradiction. We assume that $f(x)$ has $n+1$ incongruent roots modulo p and then derive a contradiction.

Let $c_0, c_1, c_2, \cdots, c_n$ be $n+1$ incongruent solutions of $f(x)$ modulo p.

Then,

$$f(c_k) \equiv 0 \pmod{p} \text{ for } 0 \leq k \leq n.$$

Then,

$$f(x) - f(c_0) = a_n (x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1 (x - c_0)$$

$$= a_n (x - c_0)(x^{n-1} + x^{n-2} c_0 + \cdots + x c_0^{n-2} + c_0^{n-1})$$

$$+ a_{n-1}(x - c_0)(x^{n-2} + x^{n-3} c_0 + \cdots + x c_0^{n-3} + c_0^{n-2})$$

$$+ \cdots + a_1 (x - c_0)$$

$$= (x - c_0) g(x)$$

where $g(x)$ is a polynomial of degree $n-1$ with leading coefficient a_n.

We show that $c_1, c_2, \cdots, c_n$ are roots of $g(x)$ modulo p.

Let $k \in \mathbb{Z}$ be such that $1 \leq k \leq n$.

Then, we have

$$(c_k - c_0) g(c_k) = f(c_k) - f(c_0)$$
$$\equiv 0 - 0 \pmod{p}$$
$$(\because f(c_i) \equiv 0 \ \forall\ 0 \le i \le n)$$
$$\equiv 0 \pmod{p}$$

Since $\gcd(c_k - c_0, p) = 1$, it follows that

$$g(c_k) \equiv 0 \pmod{p} \text{ for any } 1 \le k \le n.$$

This is impossible since $g(x)$ is a polynomial of degree $n-1$ and has a leading coefficient not divisible by p, and then by the induction hypothesis it has at most $n-1$ incongruent roots.

Hence the theorem follows.

<u>Theorem 9.7</u>: Let p be a prime and let d be a divisor of $p-1$. Then, the polynomial $x^d - 1$ has exactly d incongruent roots modulo p.

Proof: Write $p-1 = de$. Then,

$$x^{p-1} - 1 = x^{de} - 1 = (x^d)^e - 1^e$$

$$= (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1)$$
$$= (x^d - 1)\, g(x)$$

From Fermat's little theorem, $x^{p-1} - 1$ has $p-1$ incongruent roots modulo p.
Therefore, by the above equality, any root of $x^{p-1} - 1$ modulo p is either a root of $x^d - 1$ modulo p or a root of $g(x)$ modulo p.

By the Lagrange's theorem, $g(x)$ has at most $d(e-1) = de - d = p-1-d$ roots modulo p.
$\therefore$ $x^d - 1$ should have at least $(p-1)-(p-1-d)$ $= d$ incongruent roots modulo p.

On the other hand, by Lagrange's theorem, $x^d - 1$ has at most d incongruent roots modulo p.

Consequently, $x^d - 1$ has exactly d incongruent roots modulo p.

ex: Let $p = 7$ and $d = 3$. Then, $d \mid (p-1)$. The three incongruent roots of $x^3 - 1$ modulo 7 are 1, 2 and 4.

Lemma 9.1: Let p be a prime and let d be a positive divisor of $p-1$. Then, the number of positive integers less than p of order d modulo p does not exceed $\varphi(d)$.

Proof: For each d dividing $p-1$, let

$$F(d) = \#\text{positive integers of order } d \text{ modulo } p \text{ that are less than } p.$$

$$= \#\{x \in \mathbb{Z}^+ \mid \text{ord}_p x = d,\ x < p\}$$

We wish to show that $F(d) \leq \varphi(d)$.
If $F(d) = 0$, then $F(d) \leq \varphi(d)$.
Suppose $F(d) > 0$.
Then, $\exists\, a \in \mathbb{Z}$ such that $\text{ord}_p a = d$.

Then, by Theorem 9.2, the integers

$$a, a^2, \cdots, a^d$$

are incongruent modulo p because, for $1 \leq i < j \leq d$, $i \not\equiv j \pmod d$.
Moreover, each of these integers is a root of $x^d - 1$ modulo p because, for any $k \in \mathbb{Z}^+$,

$$(a^k)^d \equiv (a^d)^k \equiv 1^k \equiv 1 \pmod p$$

By Theorem 9.7, $x^d - 1$ has exactly d

incongruent roots, so every root modulo p should be congruent to one of these powers of a.

By Theorem 9.4,

$$\operatorname{ord}_p(a^k) = \operatorname{ord}_p a \quad (= d)$$
$$\Longleftrightarrow$$
$$\gcd(d, k) = 1.$$

There are $\varphi(d)$ such integers k with $1 \le k \le d$.

$$\therefore F(d) = \varphi(d).$$

It follows that, if there is at least one element of order d modulo p, then

$$F(d) \le \varphi(d).$$

This completes the proof.

ex: Let $p = 7$. The divisors of $7-1=6$ are $1, 2, 3$ and 6. Let's count $F(d)$ for each d where $d = 1, 2, 3$ and 4.

$1 \equiv 1 \pmod 7$

$2^1 \equiv 2 \pmod 7$, $2^2 \equiv 4 \pmod 7$, $2^3 \equiv 1 \pmod 7$

$3^1 \equiv 3 \pmod 7$, $3^2 \equiv 2 \pmod 7$, $3^3 \equiv 6 \pmod 7$, $3^4 \equiv 4 \pmod 7$

$3^5 \equiv 5 \pmod 7$, $3^6 \equiv 1 \pmod 7$

$4^1 \equiv 4 \pmod 7$, $4^2 \equiv 2 \pmod 7$, $4^3 \equiv 1 \pmod 7$

$5^1 \equiv 5 \pmod 7$, $5^2 \equiv 4 \pmod 7$, $5^3 \equiv 6 \pmod 7$, $5^4 \equiv 2 \pmod 7$
$5^5 \equiv 3 \pmod 7$, $5^6 \equiv 1 \pmod 7$

$6^1 \equiv 6 \pmod 7$, $6^2 \equiv 1 \pmod 7$

It follows that

$$F(1) = 1 = \varphi(1)$$
$$F(2) = 1 = \varphi(2)$$
$$F(3) = 2 = \varphi(3)$$
$$F(6) = 2 = \varphi(6).$$

Theorem 9.8: Let p be a prime and d be a divisor of $p-1$. Then the number of incongruent integers of order d modulo p is equal to $\varphi(d)$.

Proof: Let $F(d)$ be defined as in Lemma 9.1:

$$F(d) = \#\{x \in \mathbb{Z}^+ : \operatorname{ord}_p x = d,\ x < p\}$$

If $\gcd(p, a) = 1$, then, by Fermat's little theorem, $a^{p-1} \equiv 1 \pmod p$.

$\therefore$ order of every a such that $1 \le a \le p-1$ divides $p-1$.

Therefore, it follows that

$$p-1 = \sum_{d|(p-1)} F(d)$$

By Theorem 7.7, we get

$$p-1 = \sum_{d|(p-1)} \varphi(d)$$

$$\therefore \sum_{d|(p-1)} F(d) = \sum_{d|(p-1)} \varphi(d)$$

But, by Lemma 9.1, $F(d) \leq \varphi(d)$.

$\therefore$ $F(d) = \varphi(d)$ for all $d|(p-1)$.

$\therefore$ the number of incongruent integers of order d modulo p is $\varphi(d)$.

<u>Corollary 9.8.1:</u> Every prime has a primitive root.

Proof: By Theorem 9.8, there are $\varphi(p-1)$ incongruent integers of order $p-1$ modulo p, where p is prime.

$\therefore$ by definition of a primitive root, p has $\varphi(p-1)$ primitive roots and the result follows.

ex: Let $p=11$. There should be $\varphi(11-1)=\varphi(10)=4$ primitive roots of 11. It can be shown that the primitive roots of 11 are 2, 6, 7 and 8.