Math 580/780I Notes 14

Primitive Roots:

• Definition. Let a be an integer, and let n be a positive integer with $\gcd(a, n) = 1$. The *order of* a *modulo* n is the least positive integer d such that $a^d \equiv 1 \pmod{n}$.

• **Comment:** With a and n as above, the order of a modulo n exists since $a^{\phi(n)} \equiv 1 \pmod{n}$. Furthermore, the order of a modulo n divides $\phi(n)$. To see this, consider integers x and y for which $dx + \phi(n)y = \gcd(d, \phi(n))$, where d is the order of a modulo n. Then it follows easily that $a^{\gcd(d,\phi(n))} \equiv 1 \pmod{n}$, and the definition of d implies that $d = \gcd(d, \phi(n))$. This in turn implies $d|\phi(n)$ as claimed.

• Definition. If an integer a has order $\phi(n)$ modulo a positive integer n, then we say that a is a *primitive root* modulo n.

• **Comment:** Given a positive integer n, it is *not* necessarily the case that there exists a primitive root modulo n. There exists a primitive root modulo n if and only if n is 2, 4, p^r, or $2p^r$ where p denotes an odd prime and r denotes a positive integer. The remainder of this section deals with the case where n is a prime, and in this case we establish the existence of a primitive root.

• **Theorem 19.** *There is a primitive root modulo* p *for every prime* p*. Furthermore, there are exactly* $\phi(p - 1)$ *incongruent primitive roots modulo* p*.*

• **Lemma.** *Let* n *denote a positive integer. Then*

$$\sum_{d|n} \phi(d) = n,$$

where the summation is over all positive divisors of n*.*

• **Proof of Lemma.** Write $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ where the p_j are distinct primes and the e_j are positive integers. Note that

$$\sum_{d|n} \phi(d) = \prod_{j=1}^{r} \big(1 + \phi(p_j) + \cdots + \phi(p_j^{e_j})\big).$$

Since,

$$1 + \phi(p_j) + \cdots + \phi(p_j^{e_j}) = 1 + (p_j - 1)(1 + p_j + \cdots + p_j^{e_j - 1}) = p_j^{e_j},$$

we deduce that

$$\sum_{d|n} \phi(d) = \prod_{j=1}^{r} p_j^{e_j} = n.$$

• Theorem 19 is an apparent consequence of the next more general theorem.

Theorem 20. *Let* p *be a prime, and let* d *be a positive divisor of* $p - 1$*. Then the number of incongruent integers of order* d *modulo* p *is* $\phi(d)$*.*

• **Proof of Theorem 20.** We first show that $x^d - 1 \equiv 0 \pmod{p}$ has exactly d incongruent solutions modulo p. By Lagrange's Theorem, it suffices to show that there is at least d incongruent solutions. Assume there are $< d$ incongruent solutions. Observe that $x^{p-1} - 1 = (x^d - 1)g(x)$ for some $g(x) \in \mathbb{Z}[x]$ for degree $p-1-d$. A number is a root of $x^{p-1}-1 \equiv 0 \pmod{p}$ if and only if it is a root of $x^d - 1 \equiv 0 \pmod{p}$ or $g(x) \equiv 0 \pmod{p}$. By Lagrange's Theorem, $g(x) \equiv 0 \pmod{p}$ has at most $p-1-d$ incongruent solutions modulo p. Hence, $x^{p-1}-1 \equiv 0 \pmod{p}$ has $< d + (p-1-d) = p-1$ incongruent solutions modulo p. This contradicts Fermat's Little Theorem. Hence, $x^d - 1 \equiv 0 \pmod{p}$ must have exactly d incongruent solutions modulo p.

Next, suppose a has order d' modulo p. We show that a is a root of $x^d - 1 \equiv 0 \pmod{p}$ if and only if $d'|d$. If $d'|d$, then $d = kd'$ for some integer k so that

$$a^d - 1 \equiv (a^{d'})^k - 1 \equiv 1 - 1 \equiv 0 \pmod{p}.$$

Hence, a is a root of $x^d - 1 \equiv 0 \pmod{p}$. Now suppose we know a is a root of $x^d - 1 \equiv 0 \pmod{p}$ and we want to prove $d'|d$. There are integers q and r such that $d = d'q + r$ and $0 \le r < d$. Since

$$1 \equiv a^d \equiv a^{d'q+r} \equiv (a^{d'})^q a^r \equiv a^r \pmod{p},$$

we deduce that $r = 0$ and, hence, $d'|d$ as desired.

We proceed to prove the theorem by induction. If $d = 1$, then the theorem is clear. Suppose the theorem holds for $d < D$. Then using the above information (including the Lemma), we have

$$\begin{aligned} D &= |\{a : a^D - 1 \equiv 0 \pmod{p}, 0 \le a < p\}| \\ &= \sum_{d'|D} |\{a : a \text{ has order } d', 0 \le a < p\}| \\ &= \sum_{\substack{d'|D \\ d'<D}} \phi(d') + |\{a : a \text{ has order } D, 0 \le a < p\}| \\ &= \sum_{d'|D} \phi(d') - \phi(D) + |\{a : a \text{ has order } D, 0 \le a < p\}| \\ &= D - \phi(D) + |\{a : a \text{ has order } D, 0 \le a < p\}|. \end{aligned}$$

The theorem follows.

- **Comment:** If g is a primitive root modulo p, then the numbers $1, g, g^2, \dots, g^{p-2}$ are incongruent modulo p. It follows that the numbers $1, g, g^2, \dots, g^{p-2}$ are congruent modulo p to the numbers $1, 2, \dots, p-1$ in some order.

- **Corollary.** *For all odd primes p, there are exactly $(p-1)/2$ non-zero incongruent squares modulo p.*

- **Proof.** If $x \equiv a^2 \pmod{p}$ for some integer a with $a \not\equiv 0 \pmod{p}$, then $x^{(p-1)/2} \equiv a^{p-1} \equiv 1 \pmod{p}$. Hence, Lagrange's Theorem implies that there are $\le (p-1)/2$ non-zero incongruent squares modulo p. On the other hand, if g is a primitive root modulo p, then the numbers $1, g^2, g^4, \dots, g^{p-3}$ form $(p-1)/2$ non-zero incongruent squares modulo p.

- **Example.** Illustrate the above by considering $p = 7$. Here, 3 is a primitive root, and the non-zero squares are 1, 2, and 4.

- **Comment:** It is not known whether 2 is a primitive root modulo p for infinitely many primes p. On the other hand, it is known that at least one of 2, 3, and 5 is a primitive root modulo p for infinitely many primes p.

Homework:

(1) What is the order of 2 modulo 7? What is the order of 3 modulo 7?

(2) Determine whether 2 is a primitive root modulo 19.

(3) What are the cubes modulo 7? What are the cubes modulo 11? What are the cubes modulo 47?

(4) What are the fifth powers modulo 7? What are the fifth powers modulo 11? What are the fifth powers modulo 47?

(5) Let a be an integer, and let p be a prime such that $p \nmid a$. Show that a is a square modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

(6) Let a be an integer, and let p be a prime such that $p \nmid a$. Show that if a is not a square modulo a prime p, then $a^{(p-1)/2} \equiv -1 \pmod{p}$.

(7) Let p and q be primes with $p = 2q + 1$. Let a be an integer. Explain why a is a primitive root modulo p if and only if

$$a^2 \not\equiv 1 \pmod{p} \quad \text{and} \quad a^q \not\equiv 1 \pmod{p}.$$

(8) Let p be a prime, and let $q_1, \ldots, q_r$ be the distinct primes dividing $p - 1$. Let a be an integer such that $p \nmid a$. Show that if

$$a^{(p-1)/q_j} \not\equiv 1 \pmod{p}, \text{ for each } j \in \{1, 2, \ldots, r\},$$

then a is a primitive root modulo p.

(9) Let p be a prime, let g be a primitive root modulo p, and let k be an integer. Prove that g^k is a primitive root modulo p if and only if $\gcd(k, p - 1) = 1$.