Lecture 11.2

Last time:

- $\sigma(n) = \sum_{d \mid n} d$ is called the divisor sum function.

- σ and ϕ are multiplicative functions.

- $\sum_{d \mid n} \phi(d) = n$.

Primitive Roots

Recall that the order of a mod n

Recall that the order of $a \bmod n$

is the smallest $k \geq 1$ such that

$$a^k \equiv 1 \pmod{n}.$$

By a homework problem, if k is the order of $a \bmod n$, then $k \mid \phi(n)$.

When $n = p$ is prime, this means that

$$k \mid (p-1).$$

Def A primitive root $\bmod p$ is an integer a whose order $\bmod p$ is $p-1$.

Q: Do primitive roots always exist?

And if so, how many are there?

Here's a table of orders mod p for p = 5, 7 and 11.

$p = 5$
$1^1 \equiv 1 \pmod 5$
$2^4 \equiv 1 \pmod 5$
$3^4 \equiv 1 \pmod 5$
$4^2 \equiv 1 \pmod 5$

2 and 3 are primitive roots

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

3 and 5 are primitive roots

$p = 11$
$1^1 \equiv 1 \pmod{11}$
$2^{10} \equiv 1 \pmod{11}$
$3^5 \equiv 1 \pmod{11}$
$4^5 \equiv 1 \pmod{11}$
$5^5 \equiv 1 \pmod{11}$
$6^{10} \equiv 1 \pmod{11}$
$7^{10} \equiv 1 \pmod{11}$
$8^{10} \equiv 1 \pmod{11}$
$9^5 \equiv 1 \pmod{11}$
$10^2 \equiv 1 \pmod{11}$

2, 6, 7 and 8 are all prim. roots

roots

Here's some more data:

p	# primitive roots mod p
5	2
7	2
11	4
13	4
17	8
19	6
23	10
29	12
31	8
37	12

Try to guess the pattern before reading the theorem below.

Theorem Let p be a prime number. Then

(1) There are exactly $\phi(p-1)$ primitive roots mod p. In particular, a primitive root always exists mod p.

(2) If a is a primitive root mod p, then a^k is a primitive root mod p for all $k \geq 1$ with $\gcd(k, p-1) = 1$.

Pf: (1) For $p = 2$, $a = 1$ is a primitive root, so let's now assume $p > 2$.

Let k be a divisor of $\phi(p) = p - 1$.

By HW 5, Problem 2, the polynomial $x^k - 1$ has <u>exactly</u> k roots mod p.

Writing $p - 1 = q_1^{e_1} \cdots q_r^{e_r}$ for distinct primes q_i, this implies

- $x^{q_i^{e_i}} - 1$ has exactly $q_i^{e_i}$ roots;
- $x^{q_i^{e_i - 1}} - 1$ has exactly $q_i^{e_i - 1}$ roots;
- of the $q_i^{e_i}$ roots of the first polynomial,

$q_i^{e_i} - q_i^{e_i-1}$ of them have order equal to $q_i^{e_i}$.

For each $1 \leq i \leq r$, let a_i be a root of $x^{q_i^{e_i}} - 1$ which is not a root of $x^{q_i^{e_i-1}} - 1$, i.e. a_i has order $q_i^{e_i}$ mod p.

Set $a = a_1 \cdots a_r$. Then the order of a is the product of the orders of the a_i (see below), which is $q_1^{e_1} \cdots q_r^{e_r} = p-1$.

Hence a is a primitive root mod p.

To count the number of primitive roots,

let $\psi(k)$ be the arithmetic function

$$\psi(k) = \#\left\{ 0 < a < p \;\middle|\; \begin{array}{l}\text{the order of } a \\ \text{mod } p \text{ is } k\end{array} \right\}.$$

We are looking for $\psi(p-1)$, but the

whole function is useful because

the total number of roots of $x^{p-1}-1$

is $p-1 = \sum_{k \mid p-1} \psi(k)$.

We also know from Lecture 11 [illegible]

Lecture 11.1 that

$$p-1 = \sum_{k \mid p-1} \phi(k)$$

so it stands to reason $\psi = \phi$.

In particular, this would imply

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

as desired.

Let's prove $\psi(k) = \phi(k)$ for all k by induction.

First, $\phi(1) = 1$ while $\psi(1)$ is the

number of roots of $x-1 \bmod p$,

so $\psi(1) = 1$.

Next, suppose $\psi(d) = \phi(d)$ for all $d < k$.

Let $d_1 = 1, d_2, \ldots, d_{m-1}, d_m = k$ be the divisors of k.

Then $\sum_{d|k} \psi(d) = k = \sum_{d|k} \phi(d)$

can be written

$$\psi(1) + \psi(d_2) + \ldots + \psi(k) = \phi(1) + \phi(d_2) + \ldots + \phi(k)$$

but by induction, $\psi(d_i) = \phi(d_i)$ for each

$1 \leq i \leq m-1$

$1 = 1 = m-1$.

Cancelling these terms leaves $\Psi(k) = \phi(k)$.

In particular, $\Psi(p-1) = \phi(p-1)$. □

Exercise 1: Fill in this detail from the proof: if $a = a_1 \cdots a_r$ is relatively prime to p and the order of $a_i \bmod p$ is k_i, then the order of $a \bmod p$ is $k_1 \cdots k_r$.

Exercise 2: Prove (2).

Q: Fixing $a \in \mathbb{Z}$ and letting p vary, how often is a a primitive root mod p?

The question is already interesting for $a = 2$. Here's a list of the orders of 2 mod p, written $e_p(2)$, for $p < 100$:

$e_3 = 2$	$e_5 = 4$	$e_7 = 3$	$e_{11} = 10$	$e_{13} = 12$	$e_{17} = 8$
$e_{19} = 18$	$e_{23} = 11$	$e_{29} = 28$	$e_{31} = 5$	$e_{37} = 36$	$e_{41} = 20$
$e_{43} = 14$	$e_{47} = 23$	$e_{53} = 52$	$e_{59} = 58$	$e_{61} = 60$	$e_{67} = 66$
$e_{71} = 35$	$e_{73} = 9$	$e_{79} = 39$	$e_{83} = 82$	$e_{89} = 11$	$e_{97} = 48$

Conjecture (E. Artin) There are infinitely

many primes p for which 2 is a primitive root.

More generally, Artin conjectured that for $a \neq -1$, $a \neq b^2$, a is a primitive root mod p for infinitely many p.

What about composite moduli?

Def A primitive root mod n is an $a \in \mathbb{Z}$ whose order mod n is exactly $\phi(n)$.

The techniques we used above can also be used to prove:

Theorem Let $n \in \mathbb{N}$. Then

(1) There exists a primitive root mod n if and only if $n = 2, 4, p^k$ or $2p^k$ for an odd prime p and $k \geq 1$.

(2) If a primitive root mod n exists, there are $\phi(\phi(n))$ total primitive roots mod n.

Exercise 3: Prove it!

Next time: midterm review.

Next next time: the discrete logarithm problem.