Last time:

Fix n, and let a be an integer with $\gcd(a, n) = 1$. The order of a $\pmod{n}$, written $|a|$ or $|a|_n$, is the smallest $k > 0$ such that $a^k \equiv 1 \pmod{n}$. (Book: $e_n(a) = |a|_n$)

Define

$$\psi_n(k) = \#\{1 \leqslant a < n \mid |a| = k\}.$$

Ex: Modulo 7, we have

a	1	2	3	4	5	6
$\|a\|$	1	3	6	3	6	2

So

$$\psi_7(1) = 1, \quad \psi_7(2) = 1, \quad \psi_7(3) = 2, \quad \psi_7(6) = 2.$$

Notice,

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

(every a rel. prime to p has *some* order, and that order divides $\phi(p) = p - 1$).

Last time:

Define

$$\psi_n(k) = \#\{1 \leqslant a < n \mid |a| = k\}.$$

Ex: Modulo 7, we have

a	1	2	3	4	5	6
$\|a\|$	1	3	6	3	6	2

So

$$\psi_7(1) = \underbrace{1}_{\phi(1)}, \quad \psi_7(2) = \underbrace{1}_{\phi(2)}, \quad \psi_7(3) = \underbrace{2}_{\phi(3)}, \quad \psi_7(6) = \underbrace{2}_{\phi(6)}.$$

Notice,

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

(every a rel. prime to p has *some* order, and that order divides $\phi(p) = p - 1$).

Last time, we showed

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

Claim: For all $d|(p-1)$, we have $\psi_p(d) = \phi(d)$.

Namely, there are $\phi(p-1)$ primitive roots (mod p) for all primes p.

Claim: For all $d|(p-1)$, we have $\psi_p(d) = \phi(d)$.
Namely, there are $\phi(p-1)$ primitive roots (mod p) for all primes p.

We essentially showed last time that $a^n \equiv_p 1$ iff $|a|_p$ divides n, i.e.

a is a solution to $x^n - 1 \equiv_p 0$
if and only if $|a|_p$ divides n.

(Proof: divide n by $|a|_p$, and show the remainder must be 0.)

Recall...

Theorem (Polynomial Roots Mod p Theorem)

Let p be prime in $\mathbb{Z}_{>0}$, and let

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x],$$

with $n \geqslant 1$ and $p \nmid a_n$. Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most p incongruent solutions.

Define $|a| = |a|_p$ as the smallest $k > 0$ such that $a^k \equiv 1 \pmod{p}$, and let $\psi_p(d) = \#\{1 \leqslant a < p \mid |a| = d\}$.

Claim: For all $d|(p-1)$, we have $\psi_p(d) = \phi(d)$.
Namely, there are $\phi(p-1)$ primitive roots (mod p) for all primes p.

Proof. (bijective) Count the solutions to

$$x^{p-1} - 1 \equiv_p 0$$

in two ways. **Know:** there are exactly most $p-1$ solutions
(Fermat says every non-multiple of p is a solution).

We have

$$X^m - 1 = (X-1)(X^{m-1} + \cdots + X^2 + X + 1). \qquad (*)$$

Fix a divisor $d|(p-1)$, and write $p - 1 = kd$.
Plug $X = x^d$ and $m - k$ into $(*)$:

$$\underbrace{x^{p-1} - 1}_{p-1 \text{ solns}} = (x^d)^k - 1 = \underbrace{(x^d - 1)}_{s \leqslant d \text{ sols}} \underbrace{((x^{(k-1)d} + \cdots + x^{2d} + x^d + 1)}_{\text{r} \leqslant (k-1)d \text{ solns (mod } p \text{ roots)}}.$$

$$d \geqslant s = (p-1) - r \geqslant (p-1) - \underbrace{(k-1)d}_{(p-1)-d} = d. \quad \text{So } \boxed{s = d}.$$

Define $|a| = |a|_p$ as the smallest $k > 0$ such that $a^k \equiv 1 \pmod{p}$, and let $\psi_p(d) = \#\{1 \leqslant a < p \mid |a| = d\}$.

Claim: For all $d|(p-1)$, we have $\psi_p(d) = \phi(d)$.
Namely, there are $\phi(p-1)$ primitive roots (mod p) for all primes p.

Proof. (So far: *Count the solutions to*

$$x^{p-1} - 1 \equiv_p 0$$

in two ways... Fix a divisor $d|(p-1)$*, and write* $p-1 = kd\ldots$)

So there are exactly d solutions to $x^d - 1 \equiv_p 0$.
Put another way, there are exactly d values a where $|a|$ divides d.

(We have $a^d \equiv_p 1$ iff $|a|_p$ divides d.)

So

$$\sum_{\ell|d} \phi(\ell) = d = \sum_{\ell|d} \psi(\ell).$$

(RHS: counting every a with order dividing d, one order at a time.)

(LHS: last time.)

Show $\phi(d) = \psi_p(d)$ by induction on d's prime factorization.

Discrete logarithm

We call g a primitive root (mod p) if $|g|_p = \phi(p) = p - 1$.
Last time: For p prime, we have $|a|_p = p - 1$ if and only if

$$\{1, 2, \ldots, p-1\} \equiv_p \{1, a, a^2, \ldots, a^{p-2}\}.$$

Example: The primitive roots modulo 13 are $2, 6, 7$, and 11:

$g^k \pmod{13}$:

g \ $\leftarrow k \rightarrow$	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	8	3	6	12	11	9	5	10	7	1
6	6	10	8	9	2	12	7	3	5	4	11	1
7	7	10	5	9	11	12	6	3	8	4	2	1
11	11	4	5	3	7	12	2	9	8	10	6	1

For a primitive root g, and $1 \leqslant b \leqslant p-1$, the exponential map is one-to-one! Define its inverse, the discrete logarithm (base g, mod p) or index, by

$$\mathrm{dlog}_g(b) \equiv_{p-1} k \quad \text{whenever} \quad g^k \equiv_p b.$$

$g^k \pmod{13}$:

g \ $\leftarrow k \rightarrow$	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	8	3	6	12	11	9	5	10	7	1
6	6	10	8	9	2	12	7	3	5	4	11	1
7	7	10	5	9	11	12	6	3	8	4	2	1
11	11	4	5	3	7	12	2	9	8	10	6	1

Fix p. For a primitive root g, and $1 \leqslant b \leqslant p-1$, define the discrete logarithm (base g, mod p) or index by

$$\boxed{\mathrm{dlog}_g(b) \equiv_{p-1} k \quad \text{whenever} \quad g^k \equiv_p b.}$$

$\mathrm{dlog}_g(b)$:

g \ $\leftarrow k \rightarrow$	1	2	3	4	5	6	7	8	9	10	11	12
2	12	1	4	2	9	5	11	3	8	10	7	6
6	12	5	8	10	9	1	7	3	4	2	11	6
7	12	11	8	10	3	7	1	9	4	2	5	6
11	12	7	4	2	3	11	5	9	8	10	1	6

Discrete logarithm

Fix p. For a primitive root g, and $1 \leqslant b \leqslant p-1$, define the discrete logarithm or index (base g, mod p) by

$$\boxed{\operatorname{dlog}_g(b) \equiv_{p-1} k \quad \text{whenever} \quad g^k \equiv_p b.}$$

(Book: $\operatorname{dlog}_g(b) = I(b)$)

Proposition

We have

$$\operatorname{dlog}_g(ab) \equiv_{p-1} \operatorname{dlog}_g(a) + \operatorname{dlog}_g(b)$$

and

$$\operatorname{dlog}_g(b^c) \equiv_{p-1} c \cdot \operatorname{dlog}_g(b)$$

(Why $p-1$?? In short, $\operatorname{dlog}_g(b)$ corresponds to an *exponent*, so lives in $\phi(p)$'s world!)

Proof. Raise g to one side and reduce...

Using logarithms to do computations

Fix $p = 37$. Then 2 is a primitive root.

The discrete logarithm values are given by the following.

b	1	2	3	4	5	6	7	8	9
$\mathrm{dlog}_2(b)$	36	1	26	2	23	27	32	3	16
b	10	11	12	13	14	15	16	17	18
$\mathrm{dlog}_2(b)$	24	30	28	11	33	13	4	7	17
b	19	20	21	22	23	24	25	26	27
$\mathrm{dlog}_2(b)$	35	25	22	31	15	29	10	12	6
b	28	29	30	31	32	33	34	35	36
$\mathrm{dlog}_2(b)$	34	21	14	9	5	20	8	19	18

Example: Use the logarithm table to compute the following $\pmod{37}$:

(1) $25 \cdot 16$ (2) 28^{32} (3) 9^{-1}

(4) x satisfying $20x \equiv 3$ (5) $3x^{30} \equiv 4$