$\boxed{\text{Lecture 13.1}}$

Last time:

- a is a primitive root mod p if its order mod p is $\phi(p) = p-1$.
- There are $\phi(\phi(p)) = \phi(p-1)$ of these primitive roots up to congruence.

The key utility of a primitive root a is that it <u>generates</u> the set of nonzero residue classes by exponentiation:

Lemma If a is a primitive root mod p, then $\{0, a, a^2, \ldots, a^{p-1}\}$ is a complete residue system mod p.

Exercise 1: Prove it.

Def Fix a primitive root a mod p. For any $b \in \mathbb{Z}$, $\gcd(b,p) = 1$, the **index** of b mod p is the unique number $1 \leq I(b) \leq p-1$ such that

$$b \equiv a^{I(b)} \pmod{p}.$$

$\boxed{\text{Ex}}$ $a = 2$ is a primitive root mod $p = 13$:

$$2^2 = 4 \not\equiv 1 \pmod{13}$$

$$2^3 = 8 \not\equiv 1 \pmod{13}$$

$$2^4 = 16 \not\equiv 1 \pmod{13}$$

$$2^6 \equiv -1 \pmod{13} \text{ by Q.R.}$$

and of course $2^{12} \equiv 1 \pmod{13}$ by FLT.

This means $2, 4, 8, 16, \ldots, 2^{12}$ is a complete list of nonzero congruence classes mod 13.

Here are the corresponding remainder classes:

I	1	2	3	4	5	6	7	8	9	10	11	12
$2^I \pmod{13}$	2	4	8	3	6	12	11	9	5	10	7	1

Powers of 2 Modulo 13

Rearranged by a :

b	1	2	3	4	5	6	7	8	9	10	11	12
$I(b)$	12	1	4	2	9	5	11	3	8	10	7	6

Table of Indices Modulo 13 for the Base 2

What patterns do you observe?

After staring at the data for awhile,

you might come up with:

$$I(ab) \equiv I(a) + I(b) \pmod{p-1}$$

$$I(a^k) \equiv kI(a) \pmod{p-1}.$$

Before trying to prove these, can you see where they might come from?

Recall that $I(b)$ in this example is defined by $\quad b \equiv 2^{I(b)} \pmod p$.

It's almost like we're taking the logarithm of b with base 2 (mod p of course):

$$b \equiv 2^{I(b)} \pmod{p}$$

$$\text{“}\log_2 b\text{''} \equiv \log_2\left(2^{I(b)}\right)$$

$$\equiv I(b)\log_2(2)$$

$$\equiv I(b) \pmod{p-1}$$

why?

$\boxed{\text{Theorem}}$ Fix a prime p and a primitive root g. Then for any $a, b \in \mathbb{Z}$ relatively prime to p and any $k \geq 1$,

(1) $I(ab) \equiv I(a) + I(b) \pmod{p-1}$

(1) $I(ab) \equiv I(a) + I(b) \pmod{p-1}$

(2) $I(a^k) \equiv k\,I(a) \pmod{p-1}$.

Pf: (1) Given

$$a \equiv g^{I(a)} \pmod{p}$$

$$b \equiv g^{I(b)} \pmod{p}$$

and $$ab \equiv g^{I(ab)} \pmod{p}$$

we have

$$g^{I(ab)} \equiv g^{I(a)} g^{I(b)}$$

$$\equiv g^{I(a)+I(b)} \pmod{p}$$

$$\Rightarrow \quad g^{I(ab)-I(a)-I(b)} \equiv 1 \pmod{p},$$

Since g is primitive, its order $p-1$

must divide $I(ab)-I(a)-I(b)$, so

$$I(ab) \equiv I(a) + I(b) \pmod{p-1}. \quad \square$$

Exercise 2: Prove (2).

$\boxed{\text{Ex}}$ 2 is also a primitive root mod

37 (check!) so every $a \in \mathbb{Z}$ not

divisible by 37 is congruent to some

2^k for $1 \le k \le 36$.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$I(a)$	36	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4	7	17

a	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
$I(a)$	35	25	22	31	15	29	10	12	6	34	21	14	9	5	20	8	19	18

Table of Indices Modulo 37 for the Base 2

To find $I(29^{14})$ for example,

$$I(29^{14}) \equiv 14\,I(29) \equiv 14 \cdot 21$$

$$\equiv 294$$

$$\equiv 6 \pmod{36}.$$

From the table, $I(27) = 0$, so

$$29^{14} \equiv 27 \pmod{37}.$$

We could have also solve this congruence $x \equiv 29^{14} \pmod{37}$ using successive squaring, but the index table can help us solve other congruences quickly.

e.g. $3x^{30} \equiv 4 \pmod{37}$

$\Longrightarrow I(3x^{30}) \equiv I(4) \pmod{36}$

$$\underbrace{I(3)}_{26} + 30\,I(x) \equiv \underbrace{I(4)}_{2} \pmod{36}$$

$$30\,I(x) \equiv -24 \equiv 12 \pmod{36}.$$

By the Linear Congruence Theorem, there are $\gcd(30, 36) = 6$ solutions to this congruence mod 36, namely

$$I(x) \equiv 4, 10, 16, 22, 28, 34 \pmod{36}$$

$$\Rightarrow x \equiv 16, 25, 9, 21, 12, 28 \pmod{37}.$$

$\boxed{\text{Discrete Logarithm Problem}}$ For fixed

a, g relatively prime to p, find k such that

$$g^k \equiv a \pmod{p}.$$

For large p, this is computational difficult to solve, which makes it useful for alternative cryptosystems to RSA.

When g is a primitive root mod p, the "brute force" method is to generate the table of indices relative

to g and use the Theorem.

In general, we have:

$\boxed{\text{Theorem}}$ Let a, g be relatively prime to

p and suppose $\gcd(n, p-1) = d$. Then

$$g^n \equiv a \pmod{p}$$

has d solutions if $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$

and no solutions otherwise.

$\boxed{\text{Ex}}$ Let's solve $x^5 \equiv$ [illegible]

Ex Let's solve $x \equiv 6 \pmod{101}$.

Here, $\gcd(5, 100) = 5$ so we expect all 5 solutions, but only if

$$6^{\frac{100}{5}} = 6^{20} \equiv 1 \pmod{101}.$$

This can be checked by successive squaring, and the 5 solutions to the original congruence can be found by brute force OR using indices.

First, check that none of

$$2^{2}, 2^{4}, 2^{5}, 2^{10}, 2^{20}, 2^{25}, 2^{50} \equiv 1 \pmod{101}.$$

-1 since $\left(\frac{2}{101}\right) = -1$

Let $I(a)$ be the index function "base 2".

Then $x^5 \equiv 6 \pmod{101}$

$$\Rightarrow \quad 5I(x) \equiv I(6) \equiv I(2) + I(3)$$

$$\equiv 1 + I(3) \pmod{100}.$$

We need $I(3)$ to proceed, but note

that $2^7 = 128 \equiv 27 \equiv 3^3 \pmod{101}$

$$\Rightarrow \quad 7 = 3I(3) \pmod{100}$$

$$-93 \equiv 3I(3) \pmod{100}$$

$$-31 \equiv I(3) \pmod{100}.$$

Then $5I(x) \equiv -30 \pmod{100}$ which

has $\gcd(5,100) = 5$ solutions:

$$I(x) \equiv 14, 34, 54, 74, 94 \pmod{100}.$$

Finally, the 5 solutions to

$$x^5 \equiv 6 \pmod{101}$$

are $x \equiv 2^{14}, 2^{34}, 2^{54}, 2^{74}, 2^{94}$

$$\equiv 22, 70, 85, 96, 30 \pmod{101}.$$

$\boxed{\text{Theorem}}$ Let $m = 2, 4, p^k$ or $2p^k$ for $k \geq 1$ and p prime. Then for any $a \in \mathbb{Z}$ relatively prime to m,

$$g^n \equiv a \pmod{m}$$

has $\gcd(n, \phi(m)) = d$ solutions if

$$a^{\frac{\phi(m)}{d}} \equiv 1 \pmod{m}$$

and no solutions otherwise.

Next time: Dirichlet's Theorem.