Lecture 4.2

Last time:

- A **complete residue system mod n** is a set of n integers $a_1, \ldots, a_n$ that fall into the n distinct congruence classes, $x \equiv 0, 1, \ldots, n-1 \pmod{n}$.

- If p is prime and $\gcd(a,p) = 1$, then $a, 2a, \ldots, (p-1)a, pa$ is a complete res. system mod p.

Let's start by proving

Theorem (Fermat's Little Theorem) For any prime p and any integer x,

$$x^p \equiv x \pmod{p}.$$

Pf: Multiplying together the nonzero terms in the complete residue system

$$a, 2a, (p-1)a, pa \equiv 0$$

and collecting powers of a together, we get:

$$a \cdot 2a \cdots (p-1)a = 1 \cdot 2 \cdots (p-1)\, a^{p-1}.$$

There's our a^{p-1}. On the other hand, since $a, 2a, \ldots, (p-1)a, pa$ are congruent to $0, 1, 2, \ldots, p-1$ in some order, and certainly $pa \equiv 0 \pmod{p}$, we see

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1).$$

This means

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

Finally, since p is prime, we cancel out $1, 2, \ldots, p-1$ (Lecture 3.2, Exercise 1) to get $a^{p-1} \equiv 1 \pmod{p}$.

This proves the Corollary, which is equivalent to the $\gcd(a,p)=1$ case of the Theorem.

If $\gcd(a,p) > 1$, then $a \equiv 0 \pmod{p}$ and hence $a^p \equiv 0^p \equiv 0 \equiv a \pmod{p}$. $\square$

Power Congruences and Composite Moduli

FLT is very false for composite moduli:

$$5^5 \equiv (-1)^4 5 \equiv 5 \pmod{6}$$

$$2^8 = 64 \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \pmod{9}.$$

Q: Which congruences

$$x^8 \equiv 1 \pmod{n},$$

if any, can we say anything about?

Ex Let's look at $x^8 \pmod{n}$ for small values of n, 8 and all x relatively prime to n.

$n = 4$:

$$1^2 \equiv 1 \pmod{4}$$

$$3^2 \equiv 1 \pmod{4}$$

$$1^3 \equiv 1 \pmod{4}$$

$$3^3 \equiv 3 \pmod{4}$$

Remember $1^q \equiv 1 \pmod{n}$ for any q,

so let's just consider $2 \leq x \leq n-1$.

$n=6$: $5^2 \equiv 1 \pmod{6}$

$5^3 \equiv 5 \pmod{6}$

$5^4 \equiv 1 \pmod{6}$

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

$n=8$: let's skip for now

$n=9$: $2^2 \equiv 4 \pmod{9}$

$2^3 \equiv 8 \pmod{9}$

$2^4 \equiv 7 \pmod{9}$

$2^5 \equiv 5 \pmod{9}$

$2^6 \equiv 1 \pmod{9}$

$4^6 \equiv 1 \pmod 9$

$5^6 \equiv 1 \pmod 9$

$7^6 \equiv 1 \pmod 9$

$8^6 \equiv 1 \pmod 9$

$\underline{n=10}$: $3^2 \equiv 9 \pmod{10}$

$3^3 \equiv 7 \pmod{10}$

$3^4 \equiv 1 \pmod{10}$

$7^4 \equiv 1 \pmod{10}$

$9^4 \equiv 1 \pmod{10}$

Including the primes $p = 3, 5, 7, 11,$ here is a list of the smallest g such that $x^g \equiv 1 \pmod n$ for all $(x,n) = 1$:

n	φ
3	2
4	2
5	4
6	2
7	6
9	6
10	4
11	10

This sequence has a special name.

Def For any $n \in \mathbb{N}$, the totient

of n is the number

$$\phi(n) = \{ 0 < a < n \mid (a,n) = 1 \}.$$

Ex If p is prime, $\phi(p) = p-1$.

The following generalizes FLT.

Theorem (Euler) For any $n \in \mathbb{N}$ and $x \in \mathbb{Z}$ with $\gcd(x,n) = 1$,

$$x^{\phi(n)} \equiv 1 \pmod{n}.$$

Pf: Let $a_1, \ldots, a_{\phi(n)}$ be the natural numbers between 1 and $n-1$

which are relatively prime to n.

Mimicking our proof of FLT, let's show $a_1x, \ldots, a_{\phi(n)}x$ are distinct mod n.

Suppose $a_ix \equiv a_jx \pmod{n}$ for some $1 \leq i, j \leq \phi(n)$.

Then since $(x,n) = 1$, $a_i \equiv a_j \pmod{n}$.

Thus $a_i = a_j$, proving the claim.

Now consider

$$a_1x \cdots a_{\phi(n)}x = a_1 \cdots a_{\phi(n)}x^{\phi(n)}.$$

Since each x and each a_i are

relatively prime to n, we must have

$a_i x \equiv a_j \pmod{n}$ for one of the

a_j, $1 \le j \le \phi(n)$.

This implies

$$a_1 x \cdots a_{\phi(n)} x \equiv a_1 \cdots a_{\phi(n)} \pmod{n}.$$

Putting these together gives

$$a_1 \cdots a_{\phi(n)} \equiv a_1 \cdots a_{\phi(n)} x^{\phi(n)} \pmod{n}.$$

Since $(a_1 \cdots a_{\phi(n)}, n) = 1$, we can

cancel to obtain $x^{\phi(n)} \equiv 1 \pmod{n}$. □

Ex Let's compute $4^{49} \pmod{15}$.

First,

$$\begin{aligned}\phi(15) &= \#\{1 \le a \le 14 \mid (a,15) = 1\} \\ &= \#\{1, 2, 4, 7, 8, 11, 13, 14\} \\ &= 8.\end{aligned}$$

So $$\begin{aligned}4^{49} &= 4^{8 \cdot 6 + 1} = (4^8)^6 \cdot 4 \\ &\equiv 1^6 \cdot 4 \\ &\equiv 4 \pmod{15}.\end{aligned}$$

Ex What are all solutions to

$$x^{16} + x^9 + 4x - 11 \equiv 0 \pmod{15}?$$

For starters, if $(x, 15) = 1$,

$$x^{16} = (x^8)^2 \equiv 1^2 \equiv 1 \pmod{15}$$

and likewise,

$$x^9 = x^8 \cdot x \equiv 1 \cdot x \equiv x \pmod{15}.$$

So $x^{16} + x^9 + 4x - 11 \equiv 1 + x + 4x - 11$

$$\equiv 5x - 10 \pmod{15}.$$

This becomes a linear problem and since

$\gcd(5, 15) = 5$, there are 5 solutions.

One is $x_0 = 2$ (easy to spot, or use

gcd algorithm) and the full set is:

$$x \equiv 2 + 3k \pmod{15}, \quad 0 \le k < 4$$

or $x \equiv 2, 5, 8, 11, 14 \pmod{15}$.

For the degree 16 congruence, this gives the solutions $x \equiv 2, 8, 11, 14$.

On the other hand,

$$\begin{aligned} 5^4 = 25^2 &\equiv 10^2 \equiv (-5)^2 \\ &\equiv 5^2 \\ &\equiv 10 \pmod{15} \end{aligned}$$

so for the degree 16 congruence,

$$5^{16} + 5^9 + 4\cdot 5 - 11 \equiv (5^4)^4 + (5^4)^2 \cdot 5 + 9$$

$$\equiv (5^2)^4 + (5^2)^2 \cdot 5 + 9$$

$$\equiv (5^4)^2 + 5^4 \cdot 5 + 9$$

$$\equiv (5^2)^2 + 5^2 \cdot 5 + 9$$

$$\equiv 5^2 + 10 \cdot 5 + 9$$

$$\equiv (5+10)\cdot 5 + 9$$

$$\equiv 0 + 9 \pmod{15}.$$

Thus $x \equiv 15 \pmod{15}$ is not a solution.

Exercise 1: Find any other solutions to $x^{16} + x^9 + 4x - 11 \equiv 0 \pmod{15}$,

if possible.

Next time: more on $\phi(n)$.