Lecture 4.1

Last time:

- Solutions to a linear congruence

$$ax \equiv c \pmod{n}$$

exist if and only if $d = \gcd(a,n)$ divides c.

- In this case, one solution is $x_0 = \frac{cu}{d}$ for any $u \in \mathbb{Z}$ satisfying

$$au + nv = d$$

and the rest are

$$x \equiv x_0 + \frac{nk}{d} \pmod{n}$$

for $0 \leq k < d$.

Power Congruences

Once we can solve linear congruences, what's next?

Ex Let $f(x) = x^2 + 1$. Then $f(x) = 0$ has different solution sets over different arithmetic systems.

- Over the real numbers, $x^2+1=0$ has no solutions. Why?

- However, over the complex numbers, there

are 2: $x = i$ and $x = -i$.

- $x^2 + 1 \equiv 0 \pmod 2$ has a unique solution mod 2, $x \equiv 1 \pmod 2$.

This is because

$$x^2 + 1 \equiv (x-1)^2 \pmod 2.$$

- $x^2 + 1 \equiv 0 \pmod 3$ has no solutions:

$$0^2 = 0 \not\equiv -1 \pmod 3$$

$$1^2 = 1 \not\equiv -1 \pmod 3$$

$$2^2 = 4 \not\equiv -1 \pmod 3.$$

- $x^2 + 1 \equiv 0 \pmod 5$ has 2 solutions:

$$x^2+1 \equiv x^2-4 \equiv (x-2)(x+2) \pmod 5$$

$$\rightsquigarrow x \equiv 2, 3 \pmod 5.$$

- $x^2+1 \equiv 0 \pmod 7$ has no solutions

(check it!)

- $x^2+1 \equiv 0 \pmod{10}$ has 2 solutions:

$$x \equiv 3, 7 \pmod{10}$$

- $x^2+1 \equiv 0 \pmod{13}$ has 2 solutions

(check it!)

Exercise 1: Do you see a pattern? If so, try to prove it!

Theorem Let $f(x)$ be a polynomial of degree $d \geq 1$ with integer coefficients. Then for any prime p,

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

has at most d solutions mod p.

Pf: See Theorem 8.2 in the textbook.

WARNING: This is not true for composite moduli, e.g. $f(x) = ax - c \pmod{n}$ where $\gcd(a,n) > 1$.

Ex Fix $n \geq 2$ and consider the values of x^n for $0 < x < n$. Here are some examples:

$\underline{n=2}$: $1^2 = 1$

$\underline{n=3}$: $1^3 = 1$, $2^3 = 8 \equiv 2 \pmod{3}$

Okay, we can skip $x = 0$ and 1.

$n = 4$: $2^4 = 16 \equiv 0$, $3^4 = 81 \equiv 1$

$n = 5$: $2^5 = 32 \equiv 2$, $3^5 = 243 \equiv 3$,

$4^5 = 1024 \equiv 4$

For prime moduli, there appears to be a pattern... Let's investigate another:

$n = 7$: $2^7 = 128 \equiv 2$

$3^7 = 2187 \equiv 3$

$4^7 = (2^7)^2 \equiv 2^2 \equiv 4$

$5^7 = 78125 \equiv 5$.

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

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

Ex The number

$$6^{22} - 1 = 23 \cdot 5722682775750745$$

is hard to factor by sight. However,

$$6^{23} \equiv 6 \pmod{23}$$

and since $\gcd(6, 23) = 1$, we can cancel a factor of 6 to obtain

$$6^{22} \equiv 1 \pmod{23}$$

$6 \equiv 1 \pmod{23}$.

i.e. $23 \mid 6^{22} - 1$.

In fact, this cancellation is always possible:

Corollary For p prime and any $x \in \mathbb{Z}$ with $\gcd(x, p) = 1$, $x^{p-1} \equiv 1 \pmod{p}$.

Ex This theorem also helps us solve other polynomial congruences, such as

$$x^{103} \equiv 4 \pmod{11}.$$

By the Corollary, $x^{10} \equiv 1 \pmod{11}$ so

$$x^{103} = x^{100} x^3 \equiv 1^2 x^3 \equiv x^3 \pmod{11}$$

and the solutions to $x^3 \equiv 4 \pmod{11}$ can be found by hand:

$$x \equiv 5 \pmod{11}.$$

Exercise 2: Describe how to solve a polynomial congruence

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

for small primes p.

Def A **complete residue system mod n** is a set of n integers $a_1, \ldots, a_n$ belonging to n distinct congruence classes mod n.

Ex Main example: $0, 1, \ldots, n-1$.

To prove the prime power theorem, we need:

Lemma Let p be prime and $a \in \mathbb{Z}$ be

relatively prime to p. Then

$$a, 2a, \ldots, (p-1)a, pa$$

is a complete residue system mod p.

Pf: We know $1, 2, \ldots, p-1$ are coprime to p, so by HW3, Problem 2a, $a, 2a, \ldots, (p-1)a$ are coprime to p as well.

Suppose $ia \equiv ja \pmod{p}$ for some $1 \leq i, j < p$.

Then $0 \equiv (i-j)a \pmod{p}$ and since p is prime and $p \nmid a$, we must have $p \mid i-j$.

This forces $i = j$, so $a, 2a, \ldots, (p-1)p, pa$ are incongruent mod p. $\square$

Pf of Fermat's Little Thm.: 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 $a^p \equiv 0^p \equiv 0 \equiv a \pmod{p}$. □

WARNING: The converse of the Theorem is false. For example, one can check that $x^{561} \equiv x \pmod{561}$ for all $x \in \mathbb{Z}$. However, $561 = 3 \cdot 11 \cdot 17$.

Nevertheless, this is helpful for detecting

composite moduli.

Ex $2^{14} = 16384 \equiv 4 \pmod{15}$ so 15 is not prime. (We already knew this.)

Ex For $n = 2^{1048576} + 1 = 2^{2^{20}} + 1$,

$$3^{n-1} = 3^{2^{2^{20}}} \not\equiv 1 \pmod{n}$$

so n is not prime. However, no prime factors of n are known.

A composite number n such that

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

for all $a \in \mathbb{Z}$ is called a Fermat pseudoprime and there are, unfortunately, infinitely many such numbers, including

$$561, 1105, 1729, \ldots$$

However, one can still use FLT to test for primes probabilistically:

(1) As $N \longrightarrow \infty$, the proportion of Fermat pseudoprimes $\leq N$ decreases.

Therefore the likelihood of the following test failing decreases.

(2) Choose $a_1, \ldots, a_k$ and compute

$$a_1^{n-1}, \ldots, a_k^{n-1} \pmod{n}.$$

If any are $\not\equiv 1$, n is composite.

If all are $\equiv 1$, the likelihood of n being prime increases with k.

Next time: powers and composite moduli.