Lecture 5.1

Last time:

- The totient of $n \in \mathbb{N}$ is

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

- For any $x \in \mathbb{Z}$ relatively prime to n, $x^{\phi(n)} \equiv 1 \pmod{n}$.

- Special case: for p prime, $\gcd(x,p) = 1$,

$$x^{p-1} \equiv 1 \pmod{p}.$$

A Formula for $\phi(n)$

Last time, we observed some patterns in the values of $\phi(n)$. Let's prove two of them.

Lemma Let p and q be distinct primes.

(a) $\phi(pq) = (p-1)(q-1)$.

(b) For any $k \geq 1$, $\phi(p^k) = p^{k-1}(p-1)$.

Pf: (b) The proofs of both parts can be done with clever counting.

For $\phi(p^k)$, instead of counting what's relatively prime to p^k, let's count what's not.

These are just the multiples of p:

$$0, p, 2p, \ldots, (p^{k-1}-1)p$$

The total number of integers $0 \le a \le p^k - 1$ is p^k, so

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

(a) By definition,

$$\phi(pq) = \#\{0 < a < pq \mid \gcd(a, pq) = 1\}.$$

call this set A

On the other hand, $(p-1)(q-1) = \phi(p)\phi(q)$

can be counted by the set

$$B = \{(b,c) \in \mathbb{Z} \mid 0 < b < p,\ 0 < c < q\}.$$

To show $\phi(pq) = \phi(p)\phi(q)$, let's show these sets are in bijection.

Define a function

$$f : A \longrightarrow B$$

$$a \longmapsto (a \bmod p,\ a \bmod q).$$

We want to show f is a bijection.

We want to show f is a bijection.

- f is 1-to-1: Suppose (a,a) and (b,b) are the same in B.

  That is, $a \equiv b \pmod{p}$

  and $a \equiv b \pmod{q}$.

  Then p and q both divide $b-a$,

  but since $\gcd(p,q) = 1$, pq also

  divides $b-a \Rightarrow a \equiv b \pmod{pq}$.

- f is onto: for any $(b,c) \in B$,

We need some $a \in A$ with

$$a \equiv b \pmod{p} \quad \text{and} \quad a \equiv c \pmod{q}.$$

First, all solutions to the linear congruence $x \equiv b \pmod{p}$ are:

$$x = b + py \quad \text{for} \quad y \in \mathbb{Z}.$$

For such a solution $a = b + py$, the second congruence becomes

$$b + py \equiv c \pmod{q}$$

or

$$py \equiv c - b \pmod{q}$$

which has a unique solution mod q since $\gcd(p,q) = 1$. Such a solution $0 \leq y < q$ gives us a solution

$$0 \leq a = b + py < pq$$

to both congruences.

Now, since f is a bijection,

$$\phi(pq) = \#A = \#B = \phi(p)\phi(q). \quad \square$$

Part (a) actually generalizes easily

to any relatively prime moduli:

Theorem (Sun Tzu) For any $m, n \in \mathbb{N}$ which are relatively prime, the "linear system"

$$x \equiv b \pmod{m}$$
$$x \equiv c \pmod{n}$$

has a unique solution $0 \leq x < mn$.

Exercise 1: Rewrite our proof above for any $(m, n) = 1$. Do you

think the Theorem holds without this gcd hypothesis?

Remark: In the West, the Theorem is often called the Chinese Remainder Theorem, which many people find insensitive. I encourage you all to refer to it as Sun Tzu's Thm., the Remainder Thm., or at worst the CRT. Or we can come up with a better name as a class...

Ex Consider the linear system

$$x \equiv 8 \pmod{11}$$
$$x \equiv 3 \pmod{19}.$$

A solution exists by the Remainder Theorem, so let's find one.

First, $x = 8$ is a solution to the first congruence, and all solutions are of the form $x = 8 + 11k$, $k \in \mathbb{Z}$.

Then the second congruence becomes

Thus the second congruence becomes

$$8 + 11k \equiv 3 \pmod{19}$$

or $$11k \equiv -5 \pmod{19}.$$

↑ or 14 if you prefer

We know one solution is of the form $k_0 = -5u$ where

$$11u + 19v = 1.$$

To find u, use the gcd algorithm:

$$\begin{aligned} 19 &= 11 \cdot 1 + 8 \\ 11 &= 8 \cdot 1 + 3 \end{aligned} \Bigg| \rightsquigarrow 11(7) - 19(4) = 1$$

$$\left.\begin{aligned} 8 &= 3 \cdot 2 + 2 \\ 3 &= 2 \cdot 1 + 1 \end{aligned}\right|$$

So $u = 7$ and $k_0 = -35$.

(check: $11k_0 \equiv -5 \pmod{19}$)

Finally, $x_0 = 8 + 11k_0 = -377$ is the unique solution mod $11 \cdot 19 = 209$ to the original linear system, but it's better to write

$$x = -377 \equiv 41 \pmod{209}.$$

All solutions to the linear system are:

$x \equiv 41 + 209j, \quad j \in \mathbb{Z}.$

Exercise 2: Describe all solutions to the linear system

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 5 \pmod 6 \\ x &\equiv 0 \pmod 7 \end{aligned}$$

Primes Revisited

Q: How many primes are there?

Theorem There are infinitely many primes.

Pf: If there were finitely many, say $p_1, \dots, p_r$, we could multiply them and add 1 to get a new number:

$$n = p_1 \cdots p_r + 1.$$

By FTA, n has a prime factorization and in particular must be divisible by at least one of the p_i.

But for any p_i on the list,

$$n = p_1 \cdots p_i \cdots p_n + 1$$

$$\equiv 0 + 1 \equiv 1 \pmod{p_i}$$

so $p_i \nmid n$, a contradiction. □

Harder Q: How are the prime numbers distributed among all natural numbers?

Ex We know that after 2, all primes fall into one of the two

odd congruence classes mod 4:

$$p \equiv 1 \pmod 4 \quad \text{or} \quad p \equiv 3 \pmod 4.$$

For example:

$1 \pmod 4$	$3 \pmod 4$
5	3
13	7
17	11
29	19
37	23
41	31

Do you see any patterns?

Questions we can ask:

- Are there infinitely many primes

Are there infinitely many primes on each list?

- Does one list grow faster than the other?

Next time: some answers.