M 328K: Lecture 8

Katherine Ho

September 19, 2024

1 Last Time

1.1 Fermat's Little Theorem

Let p be prime, $a \in \mathbb{Z}$, $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}$$

$$ax \equiv 1 \pmod{n} \quad \text{has a solution whenever} \quad \gcd(a, n) = 1$$

$$\begin{aligned} 4x &\equiv 3 \pmod{19} \\ 4^{17}(4x) &\equiv 4^{17} \cdot 3 \pmod{19} \\ 4^{18}x &\equiv 5 \cdot 3 \pmod{19} \\ x &\equiv 15 \pmod{19} \end{aligned}$$

Note: Definitely need p to be prime.

Example 1.1.1.

$$3^9 \equiv 3 \pmod{10}$$

2 Generalization to composite modulus

2.1 Euler Totient Function (Euler's Phi Function)

Definition 2.1.1. *The Euler totient function ϕ is the function ϕ $\mathbb{N} \to \mathbb{N}$ defined by*

$$\phi(n) = \#\{a \mid 1 \leq a \leq n-1, \gcd(a, n) = 1\}$$

Example 2.1.1.

$$\begin{aligned} \phi(1) &= 1 \\ \phi(2) &= 1 \\ \phi(3) &= 2 \\ \phi(4) &= 2 \\ \phi(20) &= 8 \end{aligned}$$

Proposition 2.1.1. *If p is prime, then*

$$\phi(p) = p - 1$$

Proposition 2.1.2. *If p is prime and $k > 1$, then*

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

Exclude all multiples of p between 1 and p^k:

$$p, 2p, 3p, \ldots, (p^{k-1})p, p^{k-1}p$$

Note: $\phi(n) = n - 1$ iff n is prime. Intuition: ϕ is how close n is to being prime.

2.2 Euler's Theorem

Theorem 2.2.1 (Euler's Theorem)**.** *Let* $\gcd(a, n) = 1$*. Then*

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

Note: If $n = p$ *is prime, then* $\phi(n) = p - 1$*, so we get*

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof of Euler's Theorem. Let $0 < b_1 < b_2 < \cdots < b_{\phi(n)}$ be the integers between 1 and n that are coprime to n. The claim: The integers $ab_1, ab_2, \ldots, ab_{\phi(n)}$ are the same as $b_1, b_2, \ldots, b_{\phi(n)} \pmod{n}$ but maybe in a different order.

Example 2.2.1. $n = 10$*;* $a - 3$

$$\begin{array}{ccccc} b_1 & b_2 & b_3 & b_4 & \\ 1 & 3 & 7 & 9 & \\ ab_1 & ab_2 & ab_3 & ab_4 & \pmod{10} \\ 3 & 9 & 1 & 7 & \end{array}$$

Proof is same from HW.
So

$$\begin{aligned} (ab_1)(ab_2) &\equiv b_1 b_2 \ldots b_{\phi(n)} \pmod{n} \\ a^{\phi(n)}(b_1 b_2 \ldots b_{\phi(n)}) &\equiv b_1 b_2 \ldots b_{\phi(n)} \end{aligned}$$

Since each b_i *is coprime to* n*, we can cancel to get*

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

□

2.3 More on ϕ

$$\begin{aligned} \phi(p) &= p - 1 \quad \text{for } p \text{ prime} \\ \phi(p^k) &= p^k - p^{k-1} \end{aligned}$$

Theorem 2.3.1. *Let* a, b *be coprime positive integers. Then,*

$$\phi(a, b) = \phi(a) \cdot \phi(b)$$

"ϕ *is multiplicative."*

WARNING*: We need* $\gcd(a, b) = 1$*. Ex.* $\phi(4) = 2$*,* $\phi(2)\phi(2) = 1$

Corollary 2.3.1. *If* $n = p_1^{r_1} \ldots p_k^{r_k}$*, then*

$$\phi(n) = \phi(p_1^{r_1}) \ldots \phi(p_k^{r_k}) = (p^{r_1} - p^{r_{k-1}}) \ldots (p^{r_k} - p^{r_{k-1}})$$

To prove this, we first need to understand how to solve this problem from 4th century China:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

We will solve this using the Chinese Remainder Theorem.

Theorem 2.3.2 (Chinese Remainder Theorem). *Suppose* $\gcd(n_1, n_2) = 1$ *for pos integers* n_1 *and* n_2*. Then for any* $a_1, a_2 \in \mathbb{Z}$*, the system*

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$

has a unique solution $0 \leq x < n_1 n_2$*.*

Proof (Existence). By Bezout, there exist $m_1, m_2 \in \mathbb{Z}$ such that

$$n_1 m_1 + n_2 m_2 = 1$$

Now let $x = a_2 n_1 m_1 + a_1 n_2 m_2$. Then reducing $\pmod{n_1}$, we have

$$\begin{aligned} x = a_2 n_1 m_1 + a_1 n_2 m_2 &\equiv a_1 n_2 m_2 \pmod{n_1} \\ &\equiv a_1(1 - n_1 m_1) \pmod{n - 1} \\ &\equiv a_1 - a_1 n_1 m_1 \pmod{n - 1} \\ &\equiv a_1 \pmod{n_1} \end{aligned}$$

By the same argument,

$$x \equiv a_2 \pmod{n_2}$$

Take $x \pmod{n_1 n_2}$ to be a solution between 0 and $n_1 n_2$. ☐

Example 2.3.1. *Going back to this problem,*

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

First use Bezout:

$$\begin{aligned} 3 \cdot 2 + 5(-1) = 1 \\ x = 3(6) + 2(-5) \pmod{15} = 8 \end{aligned}$$

$$\begin{aligned} x \equiv 8 \pmod{15} \\ x \equiv 2 \pmod 7 \\ 15 \cdot 1 + 7(-2) = 1 \\ x = 2(15) + 8(-14) \pmod{105} \\ -82 \pmod{105} = 23 \end{aligned}$$

Relationship with ϕ: To show

$$\phi(ab) = \phi(a)\phi(b)$$

when $\gcd(a, b) = 1$, we need to count two things:

$$\{x \mid 0 \leq x < ab, \gcd(x, ab) = 1\}$$

Size: $\phi(ab)$

$$\{(y_1, y_2) \mid 0 \leq y_1 < a, \gcd(y_1, a) = 1, 0 \leq y_2 < b, \gcd(y_2, b) = 1\}$$

Size: $\phi(a)\phi(b)$