# M 328K: Lecture 7

Katherine Ho

September 17, 2024

## 1 Last Time

1. $ax \equiv b \pmod{n}$ If $d = \gcd(a, n)$, then
   (a) If $d \nmid b$, then no solutions
   (b) If $d \mid b$, then there are exsactly $d$ distinct solutions mod $n$
   (c) If $\gcd(a, n) = 1$, there is a unique solution mod $n$.
2. $9x \equiv 21 \pmod{30}$
   $d = \gcd(9, 30) = 3$
   First divide by $d$ to solve congruence
   $$3x \equiv 7 \pmod{10}$$
   This applies to point 1(c) and has a unique solution mod 10.
   Euclidean Algorithm: $x = -21$ is a solution. There are infinitely many solutions adding multiples of 10 to the solution.
   $$-21 + 10k \quad \text{is also a solution}$$
   They are all congruent to each other mod 10. Infinitely many integer solutions to $3x \equiv 7 \pmod{10}$ are
   $$\ldots, -21, -11, -1, 9, 19, 29, 39, \ldots$$
   This list also includes all solutions to original congruence, but not all the same mod 30.

## 2 Today

Consider $ax \equiv 1 \pmod{n}$. This has a (unique) solution iff $\gcd(a, n) = 1$.
A solution is called a multiplicative inverse of a modulo n. We will write it as $x \equiv a^{-1} \pmod{n}$ so $aa^{-1} \equiv 1 \pmod{n}$. Note that $a^{-1} \neq \frac{1}{a}$.
Recall. $4x \equiv 3 \pmod{19}$.
Note.

$$4^{-1} \equiv 3 \pmod{19} \quad \text{Since}$$
$$4 \cdot 5 \equiv 20 \equiv 1 \pmod{19}$$

Multiply $4x \equiv 3 \pmod{19}$ by $4^{-1} \pmod{19}$ to get

$$5 \cdot 4x \equiv 5 \cdot 3 \pmod{19}$$
$$x \equiv 15 \pmod{19}$$

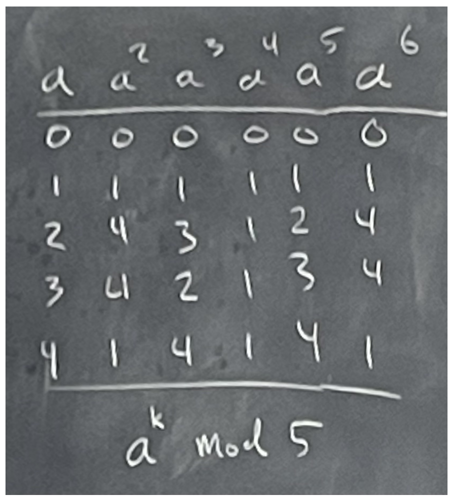
**Example 2.0.1.** *Find* $7^{-1} \pmod{17}$. *Solve* $7x \equiv 1 \pmod{17} \Leftrightarrow 7x - 17y = 1$.
*EA:*

$$\begin{aligned} 17 &= 7 \cdot 2 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 1 &= 7 - 3 \cdot 2 \\ 1 &= 7 - (17 - 7 \cdot 2) \\ &= 17(-2) + 7 \cdot 5 \end{aligned}$$

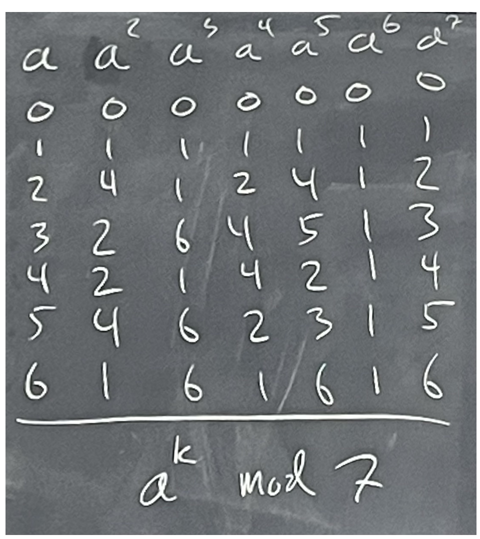
$$\boxed{x = 5}$$

# 3 Stuff

$a^k \pmod{5}$




$a^k \pmod{7}$



## 3.1 Fermat's Little Theorem

**Theorem 3.1.** *Let $p$ be prime and $a \in \mathbb{Z}$ such that $p \nmid a$. Then*

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

*ie.*

$$p \mid (a^{p-1} - 1)$$

*Proof (Idea).* $p = 5$

$$\begin{aligned} 0,1,2,3,4,5 &\pmod 5 \\ 0,2,4,1,3 &\pmod 5 \\ &0,3,1,4,2 \end{aligned}$$

□

Claim: The integers $0, a, 2a, \ldots, (p-1)a \pmod p$ are the same as the integers $0, 1, 2, \ldots, (p-1)$ but maybe in a different order.

*Proof of Claim.* If claim is false, then $ia \equiv ja \pmod p$ for some $i, j$. Then $p \mid a(i-j)$.

□

Now Consider

$$\begin{aligned} &a(2a)(3a)\ldots((p-1)(a)) \\ &= a^{p-1}(1)(2)(3)\ldots(p-1) \\ &= a^{p-1}(p-1)! \end{aligned}$$

On the other hand, by the claim,

$$\begin{aligned} a(2a)(3a)\ldots((p-1)a) &\equiv (1)(2)(3)\ldots(p-1) \pmod p \\ a^{p-1}(p-1)! &\equiv (p-1)! \pmod p \end{aligned}$$

By HW,

$$\gcd((p-1)!, p) = 1$$

So we can cancel:

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

## 3.2 Example

$p = 23$. $6^{22} = 1 \pmod{23}$.
ie.

$$23 | (6^{22} - 1)$$

## 3.3 Primality Test

$n = 10^{100} + 37$
Compute

$$\begin{aligned} 2^{n-1} = 2^{10^{100}+36} &\not\equiv 1 \pmod n \\ &\equiv 367\ldots396 \pmod n \end{aligned}$$

So n is not prime.
Note: This will never show n is prime. It can be true that $a^{n-1} \equiv 1 \pmod{n}$ even if n is composite.
Test 117 with $a = 2$.

$$\begin{aligned} 2^{116} &= 2^{64} \cdot 2^{32} \cdot 2^{16} \cdot 2^{4} \\ &\equiv 16 \cdot 22 \cdot 16 \cdot 16 \\ &\equiv 22 \\ &\not\equiv 1 \pmod{117} \end{aligned}$$

So 117 is composite.