

CS70 — SPRING 2026

LECTURE 10: FEB. 12

Last Lecture

- Arithmetic mod m : numbers are $\{0, 1, \dots, m-1\}$
 $a \equiv b \pmod{m} \iff m \mid (a-b)$
e.g. $27 \equiv 5 \pmod{11}$ $-3 \equiv 7 \pmod{10}$
- Addition, subtraction, multiplication mod m
- Exponentiation by repeated squaring
- Inverse x^{-1} of $x \pmod{m}$: $x \cdot x^{-1} \equiv 1 \pmod{m}$
e.g. $3^{-1} = 10 \pmod{29}$; $3^{-1} = 19 \pmod{28}$; $3^{-1} = ?? \pmod{27}$
- x has an inverse $\pmod{m} \iff \gcd(x, m) = 1$
- Euclid's algorithm for computing gcd

Today

- Computing inverses : extended Euclid
- Chinese Remainder Theorem
- Fermat's Little Theorem

Next Lecture

- RSA Cryptosystem

Euclid's Algorithm

function gcd(x, y)

if $y = 0$ then output(x)

else output(gcd(y, $x \bmod y$))

{assume $x \geq y \geq 0$
& $x > 0$ }

Examples:

$$\begin{aligned} & \text{gcd}(35, 12) \\ &= \text{gcd}(12, 11) \\ &= \text{gcd}(11, 1) \\ &= \text{gcd}(1, 0) \\ &= 1 \quad \checkmark \end{aligned}$$

$$\begin{aligned} & \text{gcd}(72, 45) \\ &= \text{gcd}(45, 27) \\ &= \text{gcd}(27, 18) \\ &= \text{gcd}(18, 9) \\ &= \text{gcd}(9, 0) \\ &= 9 \quad \checkmark \end{aligned}$$

Computing inverses

Given positive integers x, y , suppose we could compute integers a, b such that

$$\gcd(x, y) = ax + by$$

← NOT a modular equation!

Then if $\gcd(x, y) = 1$ we get

$$ax + by = 1$$

and hence

$$by \equiv 1 \pmod{x}$$

So $b = y^{-1} \pmod{x}$ [and $a = x^{-1} \pmod{y}$]

E.g.: $1 = (-1 \times 35) + (3 \times 12)$

$$\Rightarrow 12^{-1} = 3 \pmod{35}$$

Extended Euclidean Algorithm

function e_gcd(x, y)

if $y = 0$ then return $(x, 1, 0)$

else

$(d, a, b) = \text{e_gcd}(y, x \bmod y)$

return (d, A, B)

$$\begin{aligned} \text{gcd}(x, 0) &= x \\ &= 1 \cdot x + 0 \cdot y \end{aligned}$$

$$d = \text{gcd}(x, y) = Ax + By$$

What should A & B be?

Know: $d = ay + b(x \bmod y)$ (1)

Want: $d = Ax + By$ (2)

From (1): $d = ay + b(x - y(x \text{div } y))$
 $= \underbrace{bx}_A + \underbrace{(a - (x \text{div } y)b)}_B y$

So set $A = b$, $B = a - (x \text{div } y)b$

```

function e_gcd(x, y)
  if y = 0 then return(x, 1, 0)
  else
    (d, a, b) = e_gcd(y, x mod y)
    return(d, b, a - (x div y) b)

```

$$\gcd(35, 12) = 1$$

$$12^{-1} = 3 \pmod{35}$$

Example:

e_gcd(35, 12)



e_gcd(12, 11)



e_gcd(11, 1)



e_gcd(1, 0)

(1, -1, 3)

(1, 1, -1)

(1, 0, 1)

(1, 1, 0)



$$1 = (-1) \cdot 35 + 3 \cdot 12$$

$$1 = 1 \cdot 12 + (-1) \cdot 11$$

$$1 = 0 \cdot 11 + 1 \cdot 1$$

$$1 = 1 \cdot 1 + 0 \cdot 0$$

Correctness & running time analysis as for basic gcd alg.

```

function e_gcd(x,y)
  if y=0 then return(x,1,0)
  else
    (d,a,b) = e_gcd(y, x mod y)
    return (d, b, a - (x div y) b)

```

Example:

e_gcd(35, 10)



e_gcd(10, 5)



e_gcd(5, 0)

(5, 1, -3)



(5, 0, 1)



(5, 1, 0)

$$5 = 1 \cdot 35 + (-3) \cdot 10$$

$$5 = 0 \cdot 10 + 1 \cdot 5$$

$$5 = 1 \cdot 5 + 0 \cdot 0$$

Chinese Remainder Theorem

Method for solving systems of modular equations

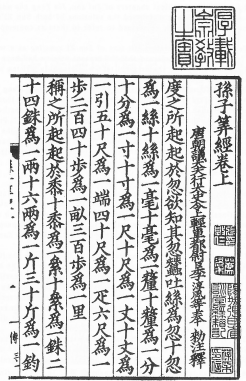
E.g.
$$\left. \begin{aligned} x &\equiv 2 \pmod{13} \\ x &\equiv 7 \pmod{10} \end{aligned} \right\}$$

Generally:

$$\left. \begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \end{aligned} \right\} \& \gcd(n_1, n_2) = 1$$

Goal: solve for $x \pmod{n_1, n_2}$

Theorem [CRT]: There is a unique $x \pmod{n_1, n_2}$
that satisfies the above equations



Sunzi Suanjing
3rd-5th century

Theorem [CRT]: Provided $\gcd(n_1, n_2) = 1$, there is a unique $x \pmod{n_1 n_2}$ that satisfies

$$x \equiv a_1 \pmod{n_1} \quad x \equiv a_2 \pmod{n_2} \quad (*)$$

Proof: Suppose we can construct numbers u_1, u_2 s.t.

$$u_1 \equiv \begin{cases} 1 \pmod{n_1} \\ 0 \pmod{n_2} \end{cases} \quad u_2 \equiv \begin{cases} 0 \pmod{n_1} \\ 1 \pmod{n_2} \end{cases}$$

Then $x = a_1 u_1 + a_2 u_2$ satisfies $(*)$!

To construct u_1 : $u_1 := n_2 (n_2^{-1} \pmod{n_1})$

To construct u_2 : $u_2 := n_1 (n_1^{-1} \pmod{n_2})$

Uniqueness ?

Sp. x & y are two solutions of $(*)$

Then $x \equiv y \pmod{n_1}$ $x \equiv y \pmod{n_2}$

So $n_1 \mid (x-y)$ and $n_2 \mid (x-y)$

$\Rightarrow n_1 n_2 \mid (x-y)$ because $\gcd(n_1, n_2) = 1$

So $x \equiv y \pmod{n_1 n_2}$ ✓

Example : $x \equiv 2 \pmod{13}$
 $x \equiv 7 \pmod{10}$

$$[\gcd(13, 10) = 1]$$

Construct $u_1 = n_2 (n_2^{-1} \pmod{n_1}) = 10 (10^{-1} \pmod{13}) = 10 \times 4$
 $= \boxed{40}$

$$u_2 = n_1 (n_1^{-1} \pmod{n_2}) = 13 (13^{-1} \pmod{10}) = 13 \cdot 7$$
$$= \boxed{91}$$

Then $x = a_1 u_1 + a_2 u_2$
 $= 2 \times 40 + 7 \times 91$
 $= 80 + 637$
 $= 717$
 $= 67 \pmod{130}$

CRT: General Version

Let $n_1, n_2, \dots, n_k$ be coprime (i.e., $\gcd(n_i, n_j) = 1 \ \forall i \neq j$)

Let $N = \prod_{i=1}^k n_i$.

Then there is a unique $x \pmod{N}$ that satisfies

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

$\vdots$

$$x \equiv a_k \pmod{n_k}$$

Proof: Same as before!

$$\text{Define } u_i := \frac{N}{n_i} \times \left(\left(\frac{N}{n_i} \right)^{-1} \pmod{n_i} \right)$$

Then $x = \sum_{i=1}^k a_i u_i$ is the solution $\pmod{N}$ $\square$

Applications: If we're working $\pmod{N}$, we can instead just work $\pmod{n_i}$ for each i , keeping the numbers small!

Example :

$$\left. \begin{array}{l} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 8 \pmod{11} \end{array} \right\} N = 5 \times 7 \times 11 = 385$$

$$u_1 = \frac{N}{n_1} \left(\left(\frac{N}{n_1} \right)^{-1} \pmod{n_1} \right) = 77 (77^{-1} \pmod{5})$$

$$= 77 (2^{-1} \pmod{5}) = 77 \times 3 = \boxed{231}$$

$$u_2 = \frac{N}{n_2} \left(\left(\frac{N}{n_2} \right)^{-1} \pmod{n_2} \right) = 55 (55^{-1} \pmod{7}) = 55 \times 6 = \boxed{330}$$

$$u_3 = \frac{N}{n_3} \left(\left(\frac{N}{n_3} \right)^{-1} \pmod{n_3} \right) = 35 (35^{-1} \pmod{11}) = 35 \times 6 = \boxed{210}$$

$$x = a_1 u_1 + a_2 u_2 + a_3 u_3$$

$$= (2 \times 231) + (3 \times 330) + (8 \times 210)$$

$$= 462 + 990 + 1680$$

$$\equiv 77 + 220 + 140 \pmod{385} \equiv \boxed{52 \pmod{385}}$$

Fermat's Little Theorem

"computing with exponents"



For any prime p ,

$$a^{p-1} \equiv 1 \pmod{p} \quad \forall a \in \{1, 2, \dots, p-1\}$$

Example: $1^6 \equiv 2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1 \pmod{7}$

$$431^{1008} \equiv 1 \pmod{1009}$$

$$6^{14} \equiv 6^2 = 36 \equiv 10 \pmod{13}$$

$$3^{244} \equiv 3^4 \equiv 81 \equiv 13 \pmod{17}$$

Corollary: For any prime p ,

$$a^p \equiv a \pmod{p} \quad \forall a \in \{0, 1, \dots, p-1\}$$

Theorem: For any prime p ,

$$a^{p-1} \equiv 1 \pmod{p} \quad \forall a \in \{1, 2, \dots, p-1\}$$

Proof: Consider the numbers $\{0, a, 2a, \dots, (p-1)a\} \pmod{p}$

Last lecture: these numbers are all different so they cover $\{0, 1, \dots, p-1\}$

Hence the sets $S = \{1, 2, \dots, p-1\}$

$S' = \{a, 2a, \dots, (p-1)a \pmod{p}\}$

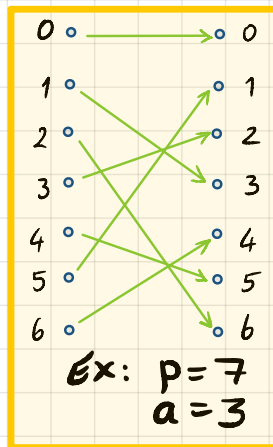
are the same set!

$$(p-1)! \equiv (p-1)! a^{p-1} \pmod{p} \quad \text{— multiply both sides by } [(p-1)!]^{-1} \pmod{p}$$
$$\Rightarrow 1 \equiv a^{p-1} \pmod{p}$$

$$\text{But } \left(\prod_{x \in S} x \right) \pmod{p} = 1 \times 2 \times \dots \times (p-1) \equiv (p-1)! \pmod{p}$$

$$\text{and } \left(\prod_{x \in S'} x \right) \pmod{p} = a \times 2a \times \dots \times (p-1)a \equiv (p-1)! a^{p-1} \pmod{p}$$

Since $(p-1)!$ has an inverse $\pmod{p}$, we conclude $a^{p-1} \equiv 1 \pmod{p}$



Euler's Totient Function

For positive integer n , let $\mathbb{Z}_n^*$ denote the set of integers $x \bmod n$ such that $\gcd(x, n) = 1$

Examples: For prime p , $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$
 $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$

Define $\varphi(n) = |\mathbb{Z}_n^*|$ (Euler's Totient Function)

For prime p , $\varphi(p) = p-1$

$\varphi(10) = 4$

Euler's Theorem: For any $a \in \mathbb{Z}_n^*$, $a^{\varphi(n)} \equiv 1 \pmod{n}$

Euler's Theorem: For any $a \in \mathbb{Z}_n^*$, $a^{\varphi(n)} \equiv 1 \pmod{n}$

Note: Fermat's Little Theorem is a special case (when n is prime)

Proof: Similar to proof of FLT.

For $a \in \mathbb{Z}_n^*$, consider the set $S := \{ax \pmod{n} : x \in \mathbb{Z}_n^*\}$

Claim: These numbers are all different, and all are in $\mathbb{Z}_n^*$

Hence S is the same as the set $\mathbb{Z}_n^*$!

$$\begin{aligned} \text{Thus } \prod_{x \in \mathbb{Z}_n^*} x &\equiv \prod_{x \in S} x \pmod{n} \\ &\equiv a^{\varphi(n)} \prod_{x \in \mathbb{Z}_n^*} x \pmod{n} \end{aligned}$$

$$\text{So } a^{\varphi(n)} \equiv 1 \pmod{n} \quad \checkmark$$

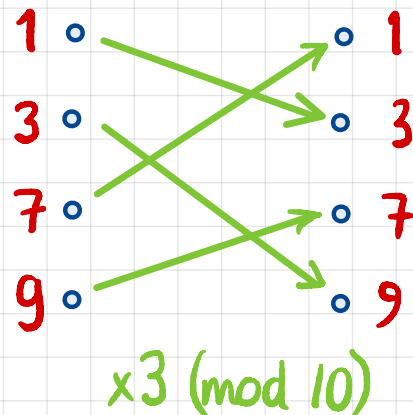
Euler's Theorem: For any $a \in \mathbb{Z}_n^*$, $a^{\varphi(n)} \equiv 1 \pmod{n}$

Note: Fermat's Little Theorem is a special case (when n is prime)

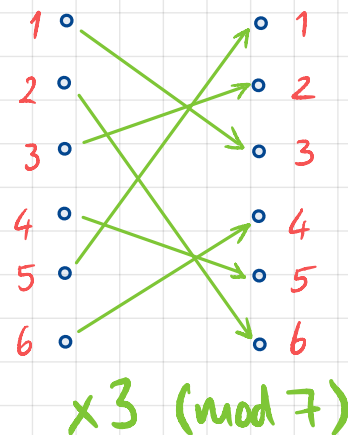
Example: $n = 10$ $\mathbb{Z}_n^* = \{1, 3, 7, 9\}$ $\varphi(n) = 4$

$$7^4 \equiv 1 \pmod{10} \quad [7^4 = 2401]$$

$$3^{71} \equiv 3^3 = 27 \equiv 7 \pmod{10}$$



c.f.



For $a \in \mathbb{Z}_n^*$, consider the set $S := \{ax \bmod n : x \in \mathbb{Z}_n^*\}$

Claim: These numbers are all different, and all are in $\mathbb{Z}_n^*$

Proof of Claim: Suppose for ~~$\times$~~ that $ax \equiv ay \bmod n$
for some $x, y \in \mathbb{Z}_n^*$ with $x \neq y$

Then $n \mid (ax - ay)$, i.e., $n \mid a(x - y)$

But $a \in \mathbb{Z}_n^*$ so $\gcd(a, n) = 1$

Hence $n \mid (x - y)$, so $x \equiv y \pmod{n}$ ~~$\times$~~

Also, $ax \bmod n \in \mathbb{Z}_n^*$ because $a, x \in \mathbb{Z}_n^*$
so $\gcd(ax, n) = 1$ $\square$