CS70 – Spring 2026

Lecture 10: Feb. 12

Last Lecture

- Arithmetic mod m : numbers are $\{0, 1, \ldots, m-1\}$

  $a \equiv b \pmod{m} \iff m \mid (a-b)$

  e.g. $27 \equiv 5 \pmod{11}$ $\quad -3 \equiv 7 \pmod{10}$

- 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. $3^{-1} = 10 \pmod{29}$; $\quad 3^{-1} = 19 \pmod{28}$; $\quad 3^{-1} = ?? \pmod{27}$

- 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 mod y))
```

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

Examples:

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

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

Computing inverses

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

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

NOT a modular equation!

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

$$ax + by = 1$$

and hence

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

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

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

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

Extended Euclidean Algorithm

```
function e_gcd(x,y)
    if y=0 then return(x,1,0)
    else
        (d,a,b) = e_gcd(y, x mod y)
        return (d, A, B)
```

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

What should A & B be?

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

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

From (1): $d = ay + b(x - y(x \operatorname{div} y))$

$= \underbrace{b}_{A}x + \underbrace{(a - (x \operatorname{div} y)b)}_{B}\, y$

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

```
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)
```

<u>Example</u>:

$$e\_gcd(35,12) \downarrow e\_gcd(12,11) \downarrow e\_gcd(11,1) \downarrow e\_gcd(1,0)$$

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:

$$e\_gcd(35,10) \rightarrow (5,1,-3) \qquad 5 = 1.35 + (-3).10$$

$$\downarrow \qquad\qquad \uparrow$$

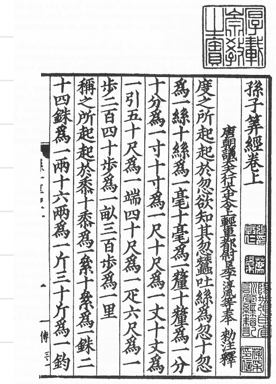
$$e\_gcd(10,5) \rightarrow (5,0,1) \qquad 5 = 0.10 + 1.5$$

$$\downarrow \qquad\qquad \uparrow$$

$$e\_gcd(5,0) \rightarrow (5,1,0) \qquad 5 = 1.5 + 0.0$$

Chinese Remainder Theorem

Method for solving systems of modular equations


孫子筭經卷上
唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勑注釋
度之所起起於忽欲知其忽蠶吐絲爲忽十忽
爲一絲十絲爲一毫十毫爲一氂十氂爲一分
十分爲一寸十寸爲一尺十尺爲一丈十丈爲
一引五十尺爲一端四十尺爲一疋六尺爲一
步二百四十步爲一畝三百步爲一里
稱之所起起於黍十黍爲一絫十絫爲一銖二
十四銖爲一兩十六兩爲一斤三十斤爲一鈞

Sunzi Suanjing
3rd-5th century

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

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

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

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

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

Proof:

<u>Example</u> : $x \equiv 2 \pmod{13}$ $[\gcd(13,10)=1]$

$x \equiv 7 \pmod{10}$

Construct $u_1 = n_2 (n_2^{-1} \bmod n_1) =$

$u_2 = n_1 (n_1^{-1} \bmod n_2) =$

Then $x = a_1 u_1 + a_2 u_2$

CRT: General Version

Let $n_1, n_2, \ldots, n_k$ 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

$$x \equiv a_1 \pmod{n_1}$$
$$\vdots$$
$$x \equiv a_k \pmod{n_k}$$

<u>Proof</u>: Same as before!

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 $\pmod N$ $\square$

<u>Applications</u>: If we're working mod N, we can instead just work mod n_i for each i, keeping the numbers small!

Example:

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

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

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

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

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

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

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

$$= 462 + 990 + 1680$$

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

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,

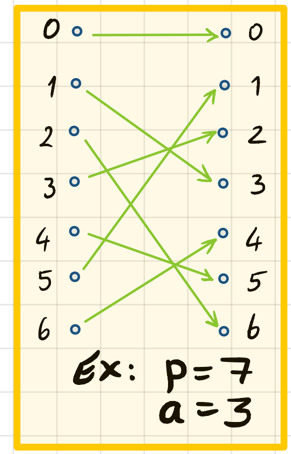
$$a^p \equiv a \pmod p \qquad \forall a \in \{0, 1, \dots, p-1\}$$

Theorem: For any prime p,

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

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

Last lecture: these numbers are all <u>different</u> so they cover $\{0, 1, \ldots, p-1\}$



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

$S' = \{a, 2a, \ldots (p-1)a \bmod p\}$

are the same set!

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

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

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

Euler's Totient Function

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

Examples: For prime p, $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$

$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$

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 $S := \{ax \bmod n : x \in \mathbb{Z}_n^*\}$

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

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

Thus $$\prod_{x \in \mathbb{Z}_n^*} x \equiv \prod_{x \in S} x \pmod{n}$$

$$\equiv a^{\varphi(n)} \prod_{x \in \mathbb{Z}_n^*} x \pmod{n}$$

So $a^{\varphi(n)} \equiv 1 \pmod{n}$ ✓

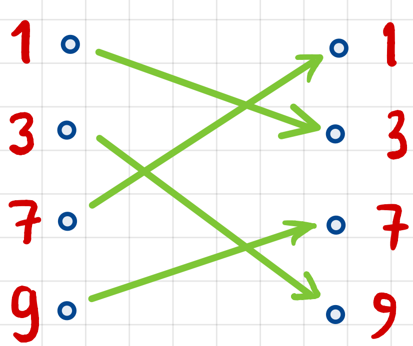
Euler's Theorem: For any $a \in \mathbb{Z}_n^*$, $a^{\varphi(n)} \equiv 1 \pmod{n}$

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

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

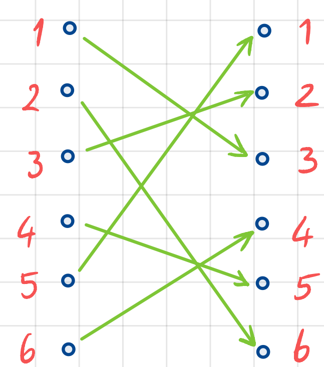
$7^4 \equiv 1 \pmod{10}$ $[7^4 = 2401]$

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



$\times 3 \pmod{10}$

c.f.



$\times 3 \pmod{7}$

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

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

<u>Proof of Claim</u>: Suppose for ※ 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 $x \equiv y \pmod n$ ※

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

$\square$