Number Theory for Cryptography

密碼學與應用

海洋大學資訊工程系

丁培毅

Congruence

- **Modulo Operation:**
  - **Question:** What is 12 mod 9?
  - **Answer:** 12 mod 9 ≡ 3 or 12 ≡ 3 (mod 9)

    "12 is congruent to 3 modulo 9"

Congruence

- **Modulo Operation:**
  - **Question:** What is 12 mod 9?
  - **Answer:** 12 mod 9 ≡ 3 or 12 ≡ 3 (mod 9)

    "12 is congruent to 3 modulo 9"

- **Definition:** Let a, r, $m \in Z$ (where Z is the set of all integers) and $m > 0$. We write
  - $a \equiv r \pmod{m}$ if m divides $a - r$ (i.e. m | a-r)
  - m is called the *modulus*
  - r is called the *remainder*
  - $a = q \cdot m + r \qquad 0 \leq r < m$

Congruence

- **Modulo Operation:**
  - **Question:** What is 12 mod 9?
  - **Answer:** 12 mod 9 ≡ 3 or 12 ≡ 3 (mod 9)

    "12 is congruent to 3 modulo 9"
- **Definition:** Let a, r, $m \in Z$ (where Z is the set of all integers) and $m > 0$. We write
  - $a \equiv r \pmod{m}$ if m divides $a - r$ (i.e. m | a-r)
  - m is called the *modulus*
  - r is called the *remainder*
  - $a = q \cdot m + r \qquad 0 \leq r < m$
- **Example:** $a = 42$ and $m=9$
  - $42 = 4 \cdot 9 + 6$ therefore $42 \equiv 6 \pmod{9}$

Greatest Common Divisor

- GCD of a and b is the largest positive integer dividing both a and b

Greatest Common Divisor

- GCD of a and b is the largest positive integer dividing both a and b
- gcd(a, b) or (a,b)

Greatest Common Divisor

- GCD of a and b is the largest positive integer dividing both a and b
- gcd(a, b) or (a,b)
- ex. gcd(6, 4) = 2, gcd(5, 7) = 1

Greatest Common Divisor

- GCD of a and b is the largest positive integer dividing both a and b
- gcd(a, b) or (a,b)
- ex. gcd(6, 4) = 2, gcd(5, 7) = 1
- Euclidean algorithm
  - ex. gcd(482, 1180)

Greatest Common Divisor

- GCD of a and b is the largest positive integer dividing both a and b
- gcd(a, b) or (a,b)
- ex. gcd(6, 4) = 2, gcd(5, 7) = 1
- Euclidean algorithm
  - ex. gcd(482, 1180)

    $1180 = 2 \cdot 482 + 216$

Greatest Common Divisor

- GCD of a and b is the largest positive integer dividing both a and b
- gcd(a, b) or (a,b)
- ex. gcd(6, 4) = 2, gcd(5, 7) = 1
- Euclidean algorithm
  - ex. gcd(482, 1180)

$$1180 = 2 \cdot 482 + 216$$
$$482 = 2 \cdot 216 + 50$$

Greatest Common Divisor

- GCD of a and b is the largest positive integer dividing both a and b
- gcd(a, b) or (a,b)
- ex. gcd(6, 4) = 2, gcd(5, 7) = 1
- Euclidean algorithm
  - ex. gcd(482, 1180)

$$1180 = 2 \cdot 482 + 216$$
$$482 = 2 \cdot 216 + 50$$
$$216 = 4 \cdot 50 + 16$$

Greatest Common Divisor

- GCD of a and b is the largest positive integer dividing both a and b
- gcd(a, b) or (a,b)
- ex. gcd(6, 4) = 2, gcd(5, 7) = 1
- Euclidean algorithm
  - ex. gcd(482, 1180)

$$1180 = 2 \cdot 482 + 216$$
$$482 = 2 \cdot 216 + 50$$
$$216 = 4 \cdot 50 + 16$$
$$50 = 3 \cdot 16 + \mathbf{2}$$

Greatest Common Divisor

- GCD of a and b is the largest positive integer dividing both a and b
- gcd(a, b) or (a,b)
- ex. gcd(6, 4) = 2, gcd(5, 7) = 1
- Euclidean algorithm
  - ex. gcd(482, 1180)

$$1180 = 2 \cdot 482 + 216$$
$$482 = 2 \cdot 216 + 50$$
$$216 = 4 \cdot 50 + 16$$
$$50 = 3 \cdot 16 + \boldsymbol{2}$$
$$16 = 8 \cdot 2 + 0$$

Greatest Common Divisor

- GCD of a and b is the largest positive integer dividing both a and b
- gcd(a, b) or (a,b)
- ex. gcd(6, 4) = 2, gcd(5, 7) = 1
- Euclidean algorithm
  - ex. gcd(482, 1180)

$$1180 = 2 \cdot 482 + 216$$
$$482 = 2 \cdot 216 + 50$$
$$216 = 4 \cdot 50 + 16$$
$$50 = 3 \cdot 16 + 2$$
$$16 = 8 \cdot 2 + 0$$

gcd

Greatest Common Divisor

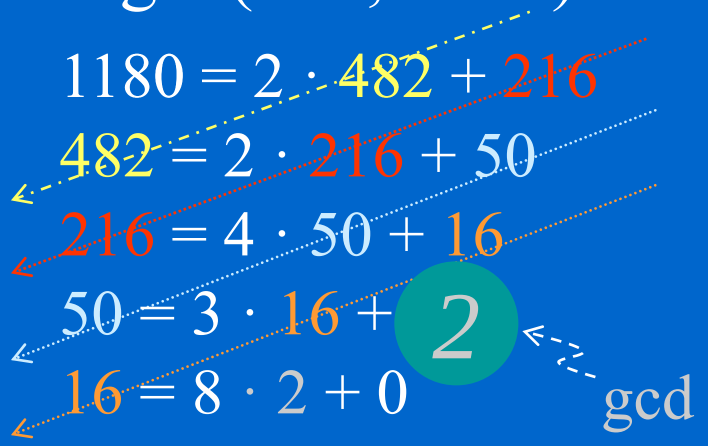
- GCD of a and b is the largest positive integer dividing both a and b
- gcd(a, b) or (a,b)
- ex. gcd(6, 4) = 2, gcd(5, 7) = 1
- Euclidean algorithm   remainder→divisor → dividend → ignore
  - ex. gcd(482, 1180)

$$1180 = 2 \cdot 482 + 216$$
$$482 = 2 \cdot 216 + 50$$
$$216 = 4 \cdot 50 + 16$$
$$50 = 3 \cdot 16 + 2$$
$$16 = 8 \cdot 2 + 0$$

gcd

Greatest Common Divisor

- ✧ GCD of a and b is the largest positive integer dividing both a and b
- ✧ gcd(a, b) or (a,b)
- ✧ ex. gcd(6, 4) = 2, gcd(5, 7) = 1
- ✧ Euclidean algorithm remainder→divisor → dividend → ignore
  - ✶ ex. gcd(482, 1180)



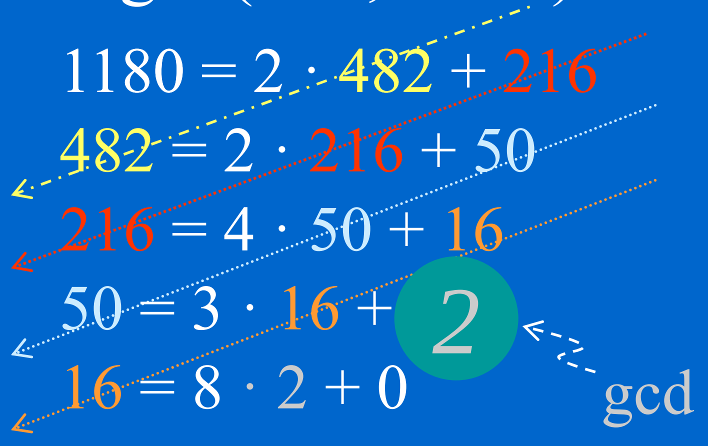
$$1180 = 2 \cdot 482 + 216$$
$$482 = 2 \cdot 216 + 50$$
$$216 = 4 \cdot 50 + 16$$
$$50 = 3 \cdot 16 + \boxed{2}$$
$$16 = 8 \cdot 2 + 0$$

gcd

Greatest Common Divisor

- GCD of a and b is the largest positive integer dividing both a and b
- gcd(a, b) or (a,b)
- ex. gcd(6, 4) = 2, gcd(5, 7) = 1
- Euclidean algorithm
  - ex. gcd(482, 1180)

remainder→divisor → dividend → ignore



$$1180 = 2 \cdot 482 + 216$$
$$482 = 2 \cdot 216 + 50$$
$$216 = 4 \cdot 50 + 16$$
$$50 = 3 \cdot 16 + \boxed{2}$$
$$16 = 8 \cdot 2 + 0$$

Why does it work?

Let d = gcd(482, 1180)

$d \mid 482$ and $d \mid 1180 \Rightarrow d \mid 216$

because $216 = 1180 - 2 \cdot 482$

$d \mid 216$ and $d \mid 482 \Rightarrow d \mid 50$

$d \mid 50$ and $d \mid 216 \Rightarrow d \mid 16$

$d \mid 16$ and $d \mid 50 \Rightarrow d \mid 2$

$2 \mid 16 \Rightarrow d = 2$

Greatest Common Divisor (cont'd)

- Euclidean Algorithm: calculating GCD

  gcd(1180, 482)

Greatest Common Divisor (cont’d)

- Euclidean Algorithm: calculating GCD

gcd(1180, 482)

1180

Greatest Common Divisor (cont’d)

- Euclidean Algorithm: calculating GCD

gcd(1180, 482)

482 | 1180

Greatest Common Divisor (cont'd)

- Euclidean Algorithm: calculating GCD

gcd(1180, 482)

482	1180	2

Greatest Common Divisor (cont’d)

- Euclidean Algorithm: calculating GCD

gcd(1180, 482)

482	1180	2
	964	

Greatest Common Divisor (cont’d)

- Euclidean Algorithm: calculating GCD

gcd(1180, 482)

482	1180 964	2
	216	

Greatest Common Divisor (cont'd)

✧ Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482	1180	2
		964	
		216	

Greatest Common Divisor (cont'd)

- Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482	1180	2
	432	964	
		216	

Greatest Common Divisor (cont’d)

- ✧ Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482	1180	2
	432	964	
	50	216	

Greatest Common Divisor (cont'd)

✧ Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482	1180	2
	432	964	
	50	216	4

Greatest Common Divisor (cont'd)

✧ Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482	1180	2
	432	964	
	50	216	4
		200	

Greatest Common Divisor (cont’d)

- Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482 432	1180 964	2
	50	216 200	4
		16	

Greatest Common Divisor (cont’d)

- Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482	1180	2
	432	964	
3	50	216	4
		200	
		16	

Greatest Common Divisor (cont’d)

✧ Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482	1180	2
	432	964	
3	50	216	4
	48	200	
		16	

Greatest Common Divisor (cont’d)

✧ Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482	1180	2
	432	964	
3	50	216	4
	48	200	
	2	16	

Greatest Common Divisor (cont'd)

- ✧ Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482	1180	2
	432	964	
3	50	216	4
	48	200	
	2	16	8

Greatest Common Divisor (cont’d)

✧ Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482 432	1180 964	2
3	50 48	216 200	4
	2	16 16	8

Greatest Common Divisor (cont'd)

✧ Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482	1180	2
	432	964	
3	50	216	4
	48	200	
	2	16	8
		16	
		0	

Greatest Common Divisor (cont’d)

✧ Euclidean Algorithm: calculating GCD

gcd(1180, 482)

2	482 432	1180 964	2
3	50 48	216 200	4
	2	16 16	8
		0	

Greatest Common Divisor (cont'd)

- ✧ Euclidean Algorithm: calculating GCD

gcd(1180, 482)

(輾轉相除法)

2	482 432	1180 964	2
3	50 48	216 200	4
	2	16 16	8
		0	

Greatest Common Divisor (cont’d)

- Def: gcd(a, b) = 1 means a and b are relatively prime

Greatest Common Divisor (cont'd)

- Def: gcd(a, b) = 1 means a and b are relatively prime
- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$

Greatest Common Divisor (cont'd)

- Def: gcd(a, b) = 1 means a and b are relatively prime
- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$
  - Constructive proof: Using Extended Euclidean Algorithm to find x and y

Greatest Common Divisor (cont'd)

- Def: gcd(a, b) = 1 means a and b are relatively prime
- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$
  - Constructive proof: Using Extended Euclidean Algorithm to find x and y

$d = 2 = 50 - 3 \cdot 16$

Greatest Common Divisor (cont'd)

- Def: gcd(a, b) = 1 means a and b are relatively prime
- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$
  - Constructive proof: Using Extended Euclidean Algorithm to find x and y

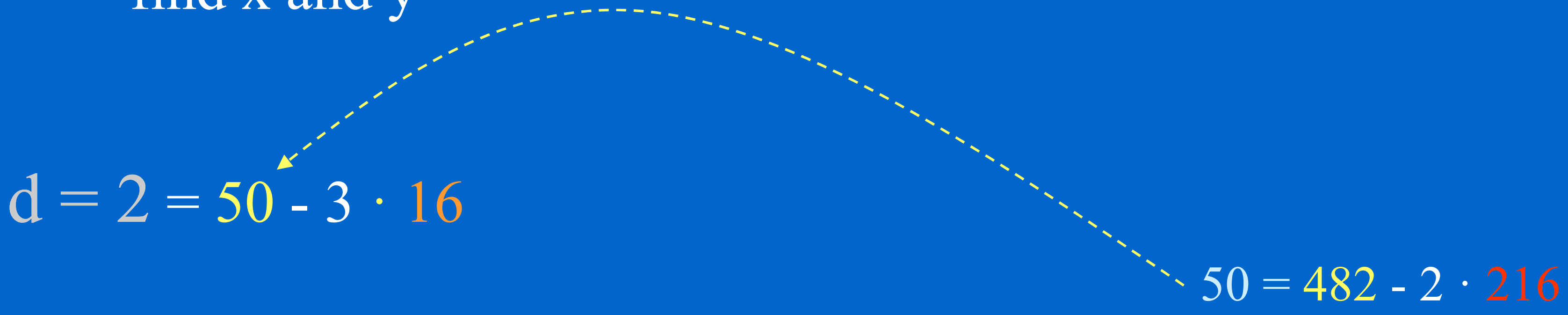
$d = 2 = 50 - 3 \cdot 16$

$50 = 482 - 2 \cdot 216$

Greatest Common Divisor (cont’d)

- Def: $\gcd(a, b) = 1$ means a and b are relatively prime

- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let $d = \gcd(a,b)$. Then there exist integers x, y, $\gcd(x, y) = 1$ such that $a \cdot x + b \cdot y = d$
  - Constructive proof: Using Extended Euclidean Algorithm to find x and y



$d = 2 = 50 - 3 \cdot 16$

$50 = 482 - 2 \cdot 216$

Greatest Common Divisor (cont'd)

- Def: gcd(a, b) = 1 means a and b are relatively prime
- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$
  - Constructive proof: Using Extended Euclidean Algorithm to find x and y

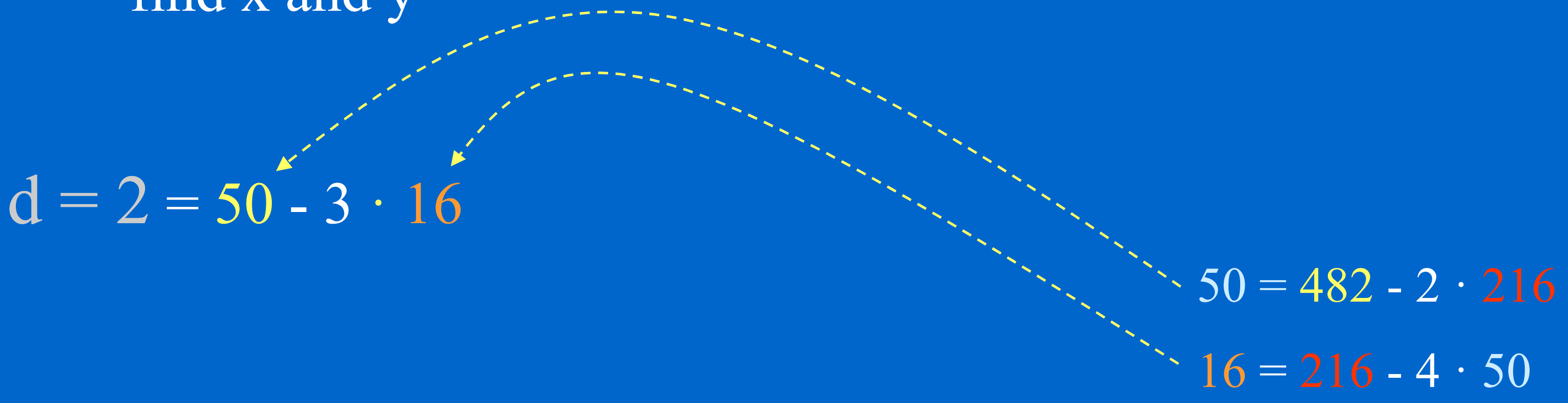
$d = 2 = 50 - 3 \cdot 16$

$50 = 482 - 2 \cdot 216$

$16 = 216 - 4 \cdot 50$

Greatest Common Divisor (cont’d)

- Def: gcd(a, b) = 1 means a and b are relatively prime
- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$
  - Constructive proof: Using Extended Euclidean Algorithm to find x and y



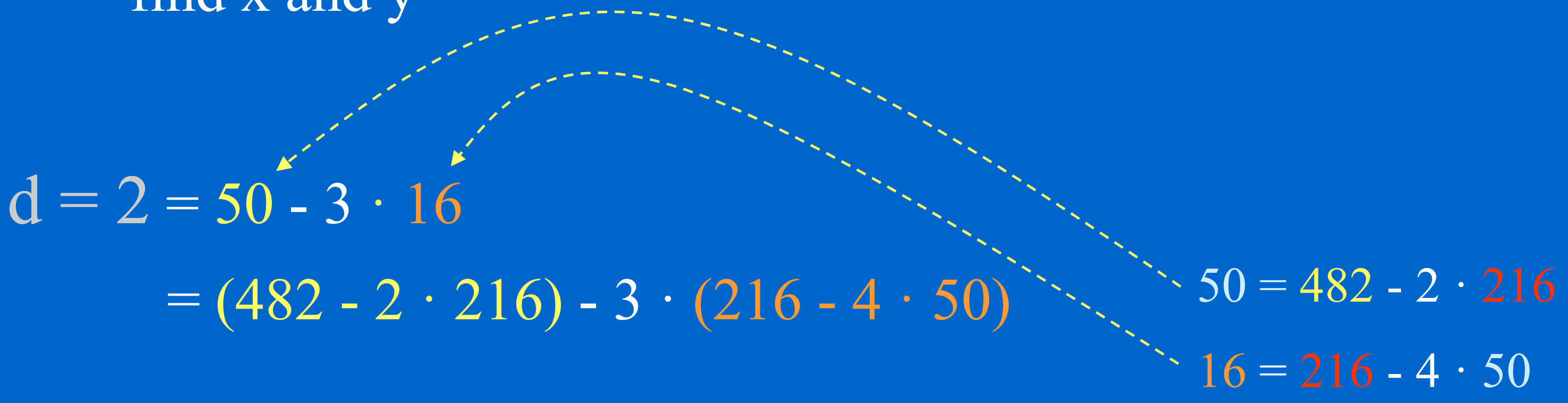
$d = 2 = 50 - 3 \cdot 16$

$50 = 482 - 2 \cdot 216$

$16 = 216 - 4 \cdot 50$

Greatest Common Divisor (cont'd)

- Def: gcd(a, b) = 1 means a and b are relatively prime
- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$
  - Constructive proof: Using Extended Euclidean Algorithm to find x and y



$d = 2 = 50 - 3 \cdot 16$

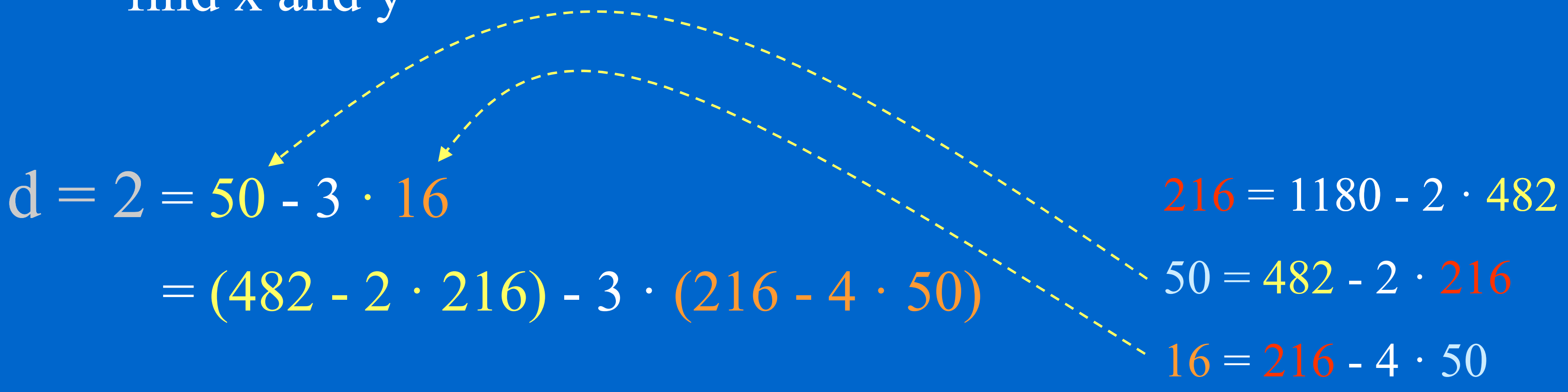
$= (482 - 2 \cdot 216) - 3 \cdot (216 - 4 \cdot 50)$

$50 = 482 - 2 \cdot 216$

$16 = 216 - 4 \cdot 50$

Greatest Common Divisor (cont’d)

- Def: gcd(a, b) = 1 means a and b are relatively prime
- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$
  - Constructive proof: Using Extended Euclidean Algorithm to find x and y



$$d = 2 = 50 - 3 \cdot 16$$

$$= (482 - 2 \cdot 216) - 3 \cdot (216 - 4 \cdot 50)$$

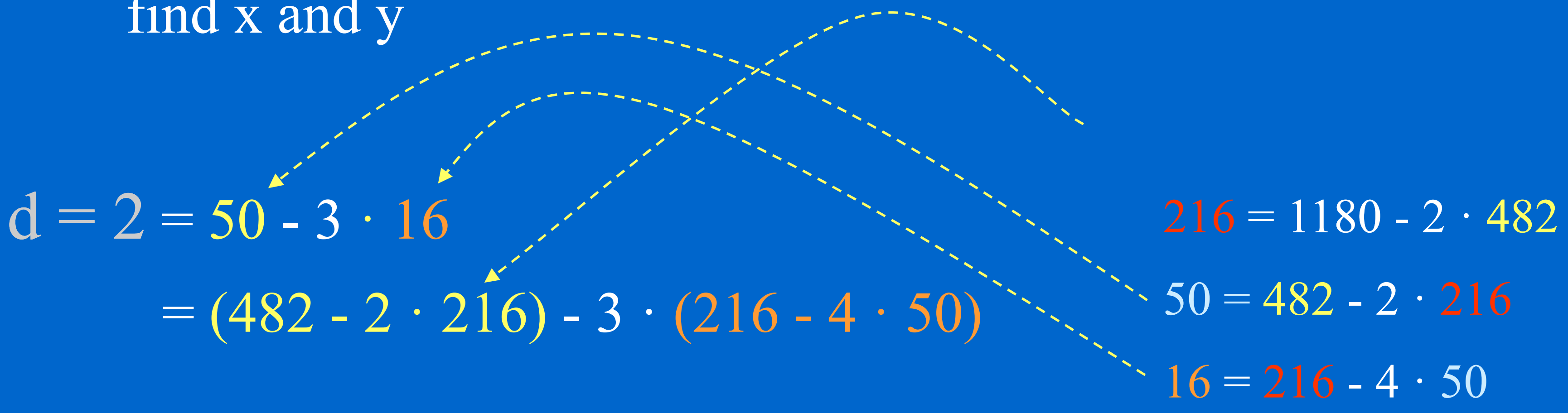
$$216 = 1180 - 2 \cdot 482$$

$$50 = 482 - 2 \cdot 216$$

$$16 = 216 - 4 \cdot 50$$

Greatest Common Divisor (cont'd)

- Def: gcd(a, b) = 1 means a and b are relatively prime
- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$
  - Constructive proof: Using Extended Euclidean Algorithm to find x and y



$$d = 2 = 50 - 3 \cdot 16$$

$$= (482 - 2 \cdot 216) - 3 \cdot (216 - 4 \cdot 50)$$

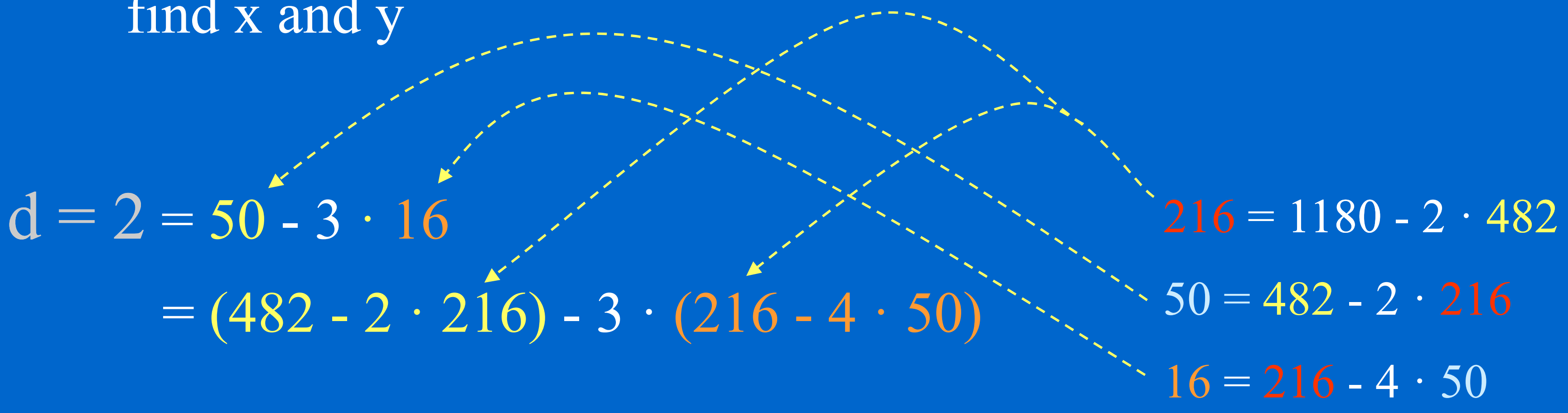
$216 = 1180 - 2 \cdot 482$

$50 = 482 - 2 \cdot 216$

$16 = 216 - 4 \cdot 50$

Greatest Common Divisor (cont’d)

- Def: gcd(a, b) = 1 means a and b are relatively prime
- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$
  - Constructive proof: Using Extended Euclidean Algorithm to find x and y



$d = 2 = 50 - 3 \cdot 16$

$= (482 - 2 \cdot 216) - 3 \cdot (216 - 4 \cdot 50)$

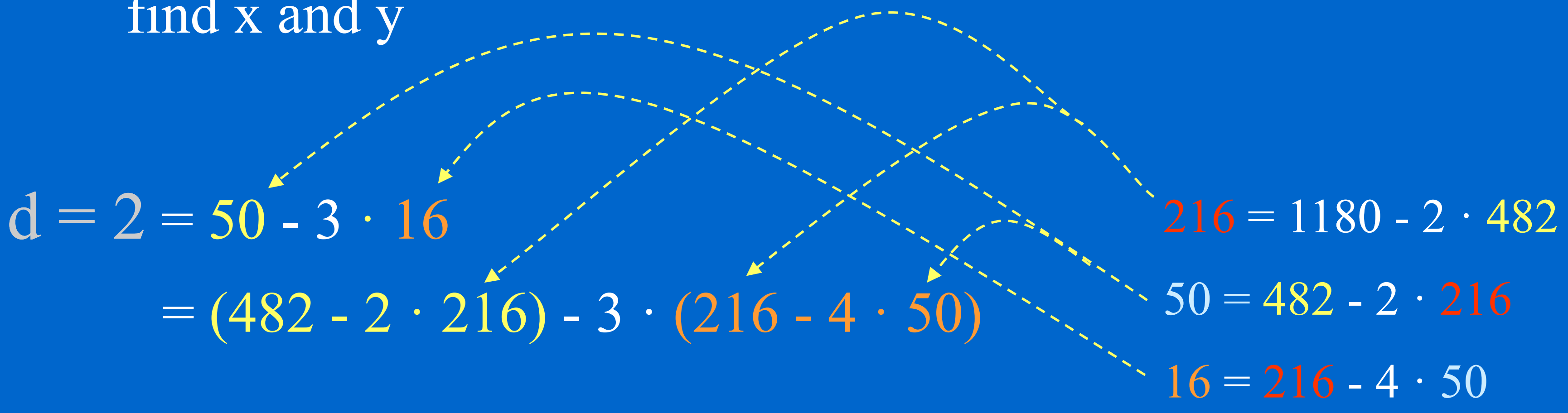
$216 = 1180 - 2 \cdot 482$

$50 = 482 - 2 \cdot 216$

$16 = 216 - 4 \cdot 50$

Greatest Common Divisor (cont’d)

- Def: gcd(a, b) = 1 means a and b are relatively prime
- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$
  - Constructive proof: Using Extended Euclidean Algorithm to find x and y



$$d = 2 = 50 - 3 \cdot 16$$

$$= (482 - 2 \cdot 216) - 3 \cdot (216 - 4 \cdot 50)$$

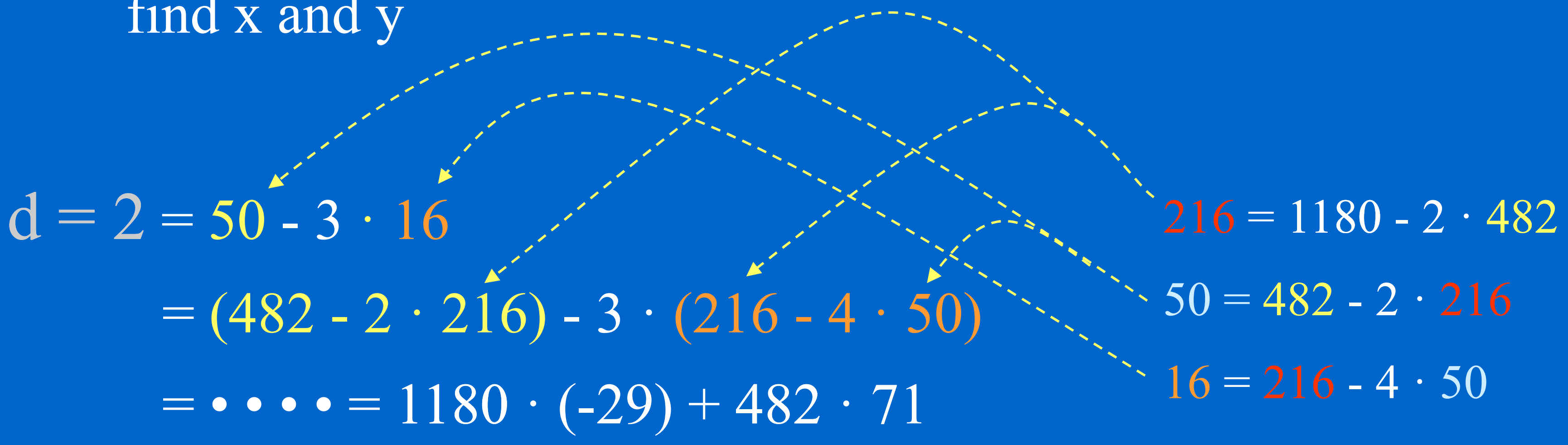
$$216 = 1180 - 2 \cdot 482$$

$$50 = 482 - 2 \cdot 216$$

$$16 = 216 - 4 \cdot 50$$

Greatest Common Divisor (cont’d)

- Def: gcd(a, b) = 1 means a and b are relatively prime
- Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$
  - Constructive proof: Using Extended Euclidean Algorithm to find x and y



$$d = 2 = 50 - 3 \cdot 16$$

$$= (482 - 2 \cdot 216) - 3 \cdot (216 - 4 \cdot 50)$$

$$= \bullet \bullet \bullet \bullet = 1180 \cdot (-29) + 482 \cdot 71$$

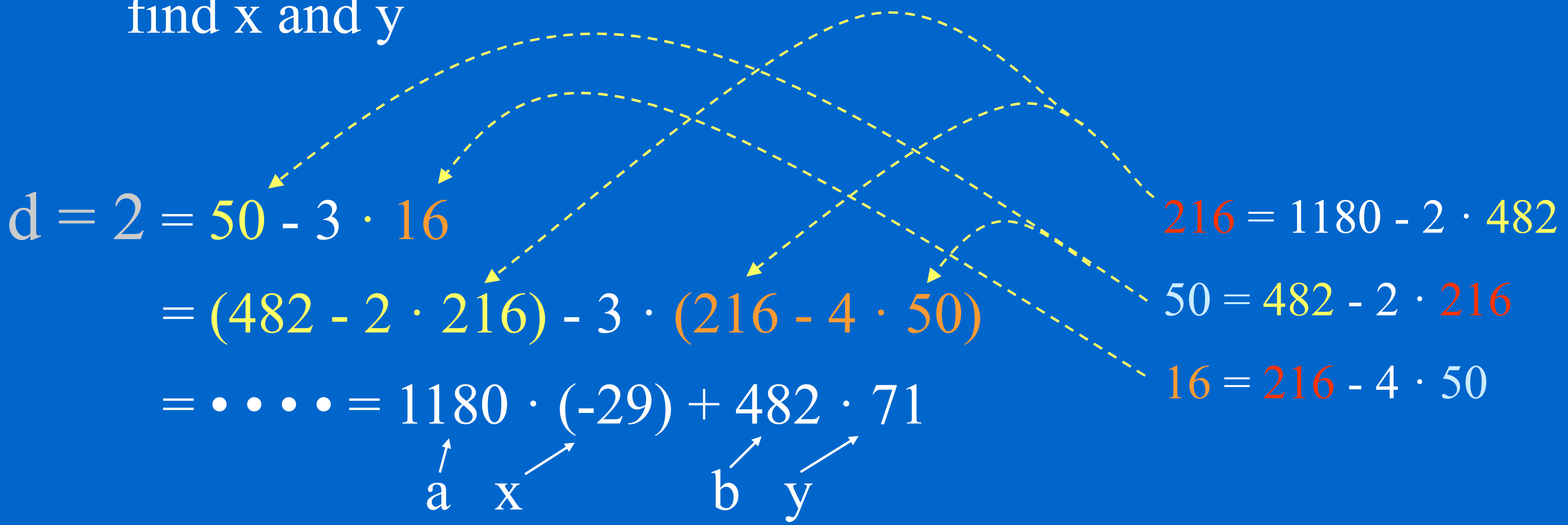
$$216 = 1180 - 2 \cdot 482$$

$$50 = 482 - 2 \cdot 216$$

$$16 = 216 - 4 \cdot 50$$

Greatest Common Divisor (cont'd)

- ✧ Def: gcd(a, b) = 1 means a and b are relatively prime
- ✧ Theorem: Let a and b be two integers, with at least one of a, b nonzero, and let d = gcd(a,b). Then there exist integers x, y, gcd(x, y) = 1 such that $a \cdot x + b \cdot y = d$
  - ✶ Constructive proof: Using Extended Euclidean Algorithm to find x and y



$$d = 2 = 50 - 3 \cdot 16$$

$$= (482 - 2 \cdot 216) - 3 \cdot (216 - 4 \cdot 50)$$

$$= \bullet \bullet \bullet \bullet = \underset{a}{1180} \cdot \underset{x}{(-29)} + \underset{b}{482} \cdot \underset{y}{71}$$

$$216 = 1180 - 2 \cdot 482$$

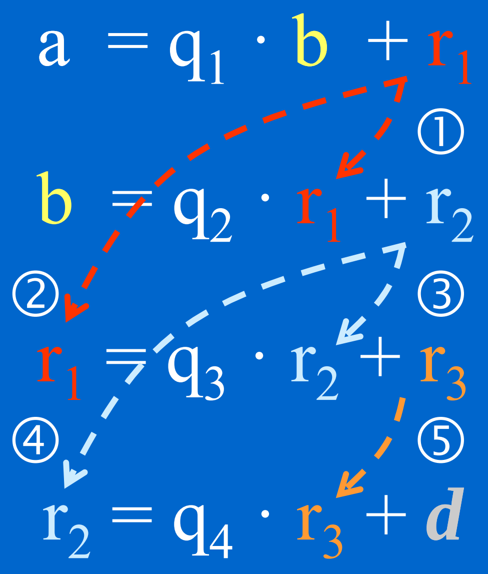
$$50 = 482 - 2 \cdot 216$$

$$16 = 216 - 4 \cdot 50$$

Extended Euclidean Algorithm

Let gcd(a, b) = d

- ✧ Looking for s and t, gcd(s, t) = 1 s.t. $a \cdot s + b \cdot t = d$
- ✧ When d = 1, $t \equiv b^{-1} \pmod{a}$



$a = q_1 \cdot b + r_1$

$b = q_2 \cdot r_1 + r_2$

$r_1 = q_3 \cdot r_2 + r_3$

$r_2 = q_4 \cdot r_3 + \boldsymbol{d}$

$r_3 = q_5 \cdot d + 0$

Ex.

$1180 = 2 \cdot 482 + 216$

$1180 - 2 \cdot 482 = 216$

$482 = 2 \cdot 216 + 50$

$482 - 2 \cdot (1180 - 2 \cdot 482) = 50$

$-2 \cdot 1180 + 5 \cdot 482 = 50$

$216 = 4 \cdot 50 + 16$

$(1180 - 2 \cdot 482) -$

$4 \cdot (-2 \cdot 1180 + 5 \cdot 482) = 16$

$9 \cdot 1180 - 22 \cdot 482 = 16$

$50 = 3 \cdot 16 + \boldsymbol{2}$

$(-2 \cdot 1180 + 5 \cdot 482) -$

$3 \cdot (9 \cdot 1180 - 22 \cdot 482) = 2$

$-29 \cdot 1180 + 71 \cdot 482 = 2$

Greatest Common Divisor (cont’d)

- The above proves only the existence of integers x and y

Greatest Common Divisor (cont'd)

- The above proves only the existence of integers x and y
- How about gcd(x, y)?

Greatest Common Divisor (cont'd)

- The above proves only the existence of integers x and y
- How about gcd(x, y)?

$$d = a \cdot x + b \cdot y$$

$$d = \gcd(a, b)$$

Greatest Common Divisor (cont'd)

- The above proves only the existence of integers x and y
- How about gcd(x, y)?

$$\begin{aligned} d &= a \cdot x + b \cdot y \\ d &= \gcd(a, b) \end{aligned} \quad \Rightarrow \quad 1 = a/d \cdot x + b/d \cdot y$$

Greatest Common Divisor (cont’d)

- The above proves only the existence of integers x and y
- How about gcd(x, y)?

$\in Z$

$$\begin{aligned} d &= a \cdot x + b \cdot y \\ d &= \gcd(a, b) \end{aligned} \quad \Rightarrow \quad 1 = a/d \cdot x + b/d \cdot y$$

Greatest Common Divisor (cont'd)

- The above proves only the existence of integers x and y
- How about gcd(x, y)?

$$\begin{aligned} d &= a \cdot x + b \cdot y \\ d &= \gcd(a, b) \end{aligned} \quad \Rightarrow \quad 1 = \overset{\in Z}{a/d} \cdot x + \overset{\in Z}{b/d} \cdot y$$

If $\gcd(x, y) = r$, $r \geq 1$ then

Greatest Common Divisor (cont'd)

- ✶ The above proves only the existence of integers x and y
- ✶ How about gcd(x, y)?

$$\begin{array}{l} d = a \cdot x + b \cdot y \\ d = \gcd(a, b) \end{array} \Rightarrow \quad 1 = \overset{\in Z}{a/d} \cdot x + \overset{\in Z}{b/d} \cdot y$$

If $\gcd(x, y) = r$, $r \geq 1$ then

$r \mid x$ and $r \mid y$

Greatest Common Divisor (cont'd)

- The above proves only the existence of integers x and y
- How about gcd(x, y)?

$$\in Z$$

$$\begin{matrix} d = a \cdot x + b \cdot y \\ d = \gcd(a, b) \end{matrix} \quad \Rightarrow \quad 1 = a/d \cdot x + b/d \cdot y$$

If $\gcd(x, y) = r$, $r \geq 1$ then

$$r \mid x \text{ and } r \mid y \quad \Rightarrow \quad r \mid a/d \cdot x + b/d \cdot y$$

Greatest Common Divisor (cont'd)

- ✶ The above proves only the existence of integers x and y
- ✶ How about gcd(x, y)?

$$\in Z$$

$$\left.\begin{array}{l} d = a \cdot x + b \cdot y \\ d = \gcd(a, b) \end{array}\right. \Rightarrow \quad 1 = a/d \cdot x + b/d \cdot y$$

If $\gcd(x, y) = r$, $r \geq 1$ then

$$r \mid x \text{ and } r \mid y \;\Rightarrow\; r \mid a/d \cdot x + b/d \cdot y$$

which means that $r \mid 1$ i.e. $r = 1$

Greatest Common Divisor (cont'd)

- ✶ The above proves only the existence of integers x and y
- ✶ How about gcd(x, y)?

$\in Z$

$$\begin{aligned} d &= a \cdot x + b \cdot y \\ d &= \gcd(a, b) \end{aligned} \quad \Rightarrow \quad 1 = a/d \cdot x + b/d \cdot y$$

If $\gcd(x, y) = r$, $r \geq 1$ then

$$r \mid x \text{ and } r \mid y \quad \Rightarrow \quad r \mid a/d \cdot x + b/d \cdot y$$

which means that $r \mid 1$ i.e. $r = 1$

$\gcd(x, y) = 1$ ¶

Greatest Common Divisor (cont'd)

- ★ The above proves only the existence of integers x and y
- ★ How about gcd(x, y)?

$\in Z$

$$\left.\begin{array}{l} d = a \cdot x + b \cdot y \\ d = \gcd(a, b) \end{array}\right. \quad \Rightarrow \quad 1 = a/d \cdot x + b/d \cdot y$$

If $\gcd(x, y) = r$, $r \geq 1$ then

$$r \mid x \text{ and } r \mid y \;\Rightarrow\; r \mid a/d \cdot x + b/d \cdot y$$

which means that $r \mid 1$ i.e. $r = 1$

$\gcd(x, y) = 1$ ¶

Note: gcd(x, y) = 1 but (x, y) is not unique

e.g. $d = a\,x + b\,y = a\,(x-k\cdot b) + b\,(y+k\cdot a)$

when k increases, $x-k\cdot b$ decreases and become negative

Greatest Common Divisor (cont'd)

Lemma: gcd(a,b) = gcd(x,y) = gcd(a,y) = gcd(x,b) = 1 ⇔ ∃ a, b, x, y s.t. $1 = a x + b y$

Greatest Common Divisor (cont'd)

Lemma: gcd(a,b) = gcd(x,y) = gcd(a,y) = gcd(x,b) = 1 ⇔

∃ a, b, x, y s.t. $1 = a x + b y$

pf:

(⇒) following the previous theorem

Greatest Common Divisor (cont’d)

Lemma: gcd(a,b) = gcd(x,y) = gcd(a,y) = gcd(x,b) = 1 ⇔ ∃ a, b, x, y s.t. $1 = a\,x + b\,y$

pf:

(⇒) following the previous theorem

(⇐) let d = gcd(a, b), $d \geq 1$

Greatest Common Divisor (cont'd)

Lemma: gcd(a,b) = gcd(x,y) = gcd(a,y) = gcd(x,b) = 1 $\Leftrightarrow$

$\exists$ a, b, x, y s.t. $1 = a\,x + b\,y$

pf:

($\Rightarrow$) following the previous theorem

($\Leftarrow$) let $d = \gcd(a, b)$, $d \geq 1$

$\Rightarrow d \mid a$ and $d \mid b$

Greatest Common Divisor (cont’d)

Lemma: $\gcd(a,b) = \gcd(x,y) = \gcd(a,y) = \gcd(x,b) = 1 \Leftrightarrow$

$\exists\ a, b, x, y$ s.t. $1 = a x + b y$

pf:

$(\Rightarrow)$ following the previous theorem

$(\Leftarrow)$ let $d = \gcd(a, b)$, $d \geq 1$

$\Rightarrow d \mid a$ and $d \mid b$

$\Rightarrow d \mid a x + b y$

Greatest Common Divisor (cont’d)

Lemma: gcd(a,b) = gcd(x,y) = gcd(a,y) = gcd(x,b) = 1 ⇔

$\exists$ a, b, x, y s.t. $1 = a\,x + b\,y$

pf:

(⇒) following the previous theorem

(⇐) let $d = \gcd(a, b)$, $d \geq 1$

$\Rightarrow d \mid a$ and $d \mid b$

$\Rightarrow d \mid a\,x + b\,y \qquad = 1$

Greatest Common Divisor (cont'd)

Lemma: gcd(a,b) = gcd(x,y) = gcd(a,y) = gcd(x,b) = 1 ⇔

$\exists$ a, b, x, y s.t. $1 = a x + b y$

pf:

(⇒) following the previous theorem

(⇐) let $d = \gcd(a, b)$, $d \geq 1$

$\Rightarrow d \mid a$ and $d \mid b$

$\Rightarrow d \mid a x + b y \quad = 1$

$\Rightarrow d = 1$

Greatest Common Divisor (cont'd)

Lemma: $\gcd(a,b) = \gcd(x,y) = \gcd(a,y) = \gcd(x,b) = 1 \Leftrightarrow$

$\exists$ a, b, x, y s.t. $1 = a x + b y$

pf:

($\Rightarrow$) following the previous theorem

($\Leftarrow$) let $d = \gcd(a, b)$, $d \geq 1$

$\Rightarrow d \mid a$ and $d \mid b$

$\Rightarrow d \mid a x + b y \quad = 1$

$\Rightarrow d = 1$

similarly, $\gcd(a, y)=1$, $\gcd(x, b)=1$, and $\gcd(x, y)=1$

Operations under mod n

- ✧ Proposition:

  Let a,b,c,d,n be integers with $n \neq 0$, suppose

  $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

Operations under mod n

✧ Proposition:

Let a,b,c,d,n be integers with n ≠ 0, suppose

a ≡ b (mod n) and c ≡ d (mod n) then

a + c   b + d (mod n)

Operations under mod n

✧ Proposition:

Let a,b,c,d,n be integers with $n \neq 0$, suppose

$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

$$a + c \qquad b + d \pmod{n}$$

pf. $\begin{cases} a = k_1\, n + b \\ c = k_2\, n + d \end{cases}$

Operations under mod n

✧ Proposition:

Let a,b,c,d,n be integers with $n \neq 0$, suppose

$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

$$a + c \qquad b + d \pmod{n}$$

pf. $\begin{cases} a = k_1\, n + b \\ c = k_2\, n + d \end{cases}$

$\Rightarrow (a+c) = (k_1+k_2)\, n + (b+d)$

Operations under mod n

✧ Proposition:

Let a,b,c,d,n be integers with $n \neq 0$, suppose

$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

$$a + c \qquad b + d \pmod{n}$$

pf. $\begin{cases} a = k_1\, n + b \\ c = k_2\, n + d \end{cases}$

$\Rightarrow (a+c) = (k_1+k_2)\, n + (b+d)$

$\Rightarrow a+c \equiv b+d \pmod{n}$

Operations under mod n

✧ Proposition:

Let a,b,c,d,n be integers with $n \neq 0$, suppose

$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

$$a + c \qquad b + d \pmod{n}$$

$$a - c \qquad b - d \pmod{n}$$

$$a \cdot c \qquad b \cdot d \pmod{n}$$

Operations under mod n

✧ Proposition:

Let a,b,c,d,n be integers with $n \neq 0$, suppose
$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

$$a + c \qquad b + d \pmod{n}$$

$$a - c \qquad b - d \pmod{n}$$

$$a \cdot c \qquad b \cdot d \pmod{n}$$

✧ Proposition:

Let a,b,c,n be integers with $n \neq 0$ and $\gcd(a,n) = 1$.

Operations under mod n

- ✧ Proposition:

  Let a,b,c,d,n be integers with n ≠ 0, suppose

  a ≡ b (mod n) and c ≡ d (mod n) then

  $a + c \quad b + d \pmod{n}$

  $a - c \quad b - d \pmod{n}$

  $a \cdot c \quad b \cdot d \pmod{n}$

- ✧ Proposition:

  Let a,b,c,n be integers with n ≠ 0 and gcd(a,n) =1.

  If a · b ≡ a · c (mod n) then b ≡ c (mod n)

Operations under mod n

✧ What is the multiplicative inverse of a (mod n)?

i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

Operations under mod n

✧ What is the multiplicative inverse of a (mod n)?

i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

Existence of a^{-1} and k ⇔ gcd(a,n)=1

Operations under mod n

- ✧ What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  $\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

  Extended Euclidean Algo.

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

Operations under mod n

✧ What is the multiplicative inverse of a (mod n)?

i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

$\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

$\Rightarrow a^{-1} \equiv s \pmod{n}$

T

Operations under mod n

✧ What is the multiplicative inverse of a (mod n)?

i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

$\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

$\Rightarrow a^{-1} \equiv s \pmod{n}$

T

➢

➢

Operations under mod n

- What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  $\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

T

Operations under mod n

✧ What is the multiplicative inverse of a (mod n)?

i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

$\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

$\Rightarrow a^{-1} \equiv s \pmod{n}$

T

➢

➢

➢

Operations under mod n

- What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  $\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

T

Operations under mod n

- What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  $\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

T

Operations under mod n

✧ What is the multiplicative inverse of a (mod n)?

i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

$\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

$\Rightarrow a^{-1} \equiv s \pmod{n}$

T

➢

➢

➢

Operations under mod n

- ✧ What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  gcd(a, n) = 1 ⇒ ∃ integer s and t such that $a \cdot s + n \cdot t = 1$

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

T

➢

➢

➢

Operations under mod n

- ✧ What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  $\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

- ✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = 1$, $x \equiv ?$

  $x \equiv a^{-1} \cdot b \equiv s \cdot b \pmod{n}$

Operations under mod n

- ✧ What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  $\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

- ✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = 1$, $x \equiv ?$

  $x \equiv a^{-1} \cdot b \equiv s \cdot b \pmod{n}$

- ✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

Operations under mod n

- ✧ What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  $\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

- ✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = 1$, $x \equiv ?$

  $x \equiv a^{-1} \cdot b \equiv s \cdot b \pmod{n}$

- ✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

Are there any solutions?

Operations under mod n

- ✧ What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  $\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

- ✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = 1$, $x \equiv ?$

  $x \equiv a^{-1} \cdot b \equiv s \cdot b \pmod{n}$

Are there any solutions?

- ✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

  if $d \nmid b$

Operations under mod n

- ✧ What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  $\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

- ✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = 1$, $x \equiv ?$

  $x \equiv a^{-1} \cdot b \equiv s \cdot b \pmod{n}$

- ✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

  Are there any solutions?

  if $d \nmid b$ $\quad a\,x = b + k\,n$

Operations under mod n

✧ What is the multiplicative inverse of a (mod n)?

$$\text{i.e.}\quad a \cdot a^{-1} \equiv 1 \pmod{n} \qquad \text{or} \qquad a \cdot a^{-1} = 1 + k \cdot n$$

$$\gcd(a, n) = 1 \;\Rightarrow\; \exists \text{ integer } s \text{ and } t \text{ such that } a \cdot s + n \cdot t = 1$$

$$\Rightarrow a^{-1} \equiv s \pmod{n}$$

✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = 1$, $x \equiv ?$

$$x \equiv a^{-1} \cdot b \equiv s \cdot b \pmod{n}$$

Are there any solutions?

✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

if $d \nmid b$ $\quad a\, x = b + k\, n \;\Rightarrow\; d\, a'\, x = b + k\, d\, n'$

Operations under mod n

- What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  $\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

- $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = 1$, $x \equiv ?$

  $x \equiv a^{-1} \cdot b \equiv s \cdot b \pmod{n}$

- $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

  Are there any solutions?

  if $d \nmid b$ $\quad a\,x = b + k\,n \Rightarrow d\,a'\,x = b + k\,d\,n' \Rightarrow b = d\,(a'\,x - k\,n')$

Operations under mod n

✧ What is the multiplicative inverse of a (mod n)?

i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

$\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

$\Rightarrow a^{-1} \equiv s \pmod{n}$

✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = 1$, $x \equiv ?$

$x \equiv a^{-1} \cdot b \equiv s \cdot b \pmod{n}$

Are there any solutions?

✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

if $d \nmid b$ $\quad a\,x = b + k\,n \Rightarrow d\,a'\,x = b + k\,d\,n' \Rightarrow b = d\,(a'\,x - k\,n')$

$\Rightarrow d \mid b$ contradiction

Operations under mod n

✧ What is the multiplicative inverse of a (mod n)?

$$\text{i.e. } a \cdot a^{-1} \equiv 1 \pmod{n} \quad \text{or} \quad a \cdot a^{-1} = 1 + k \cdot n$$

$$\gcd(a, n) = 1 \Rightarrow \exists \text{ integer } s \text{ and } t \text{ such that } a \cdot s + n \cdot t = 1$$

$$\Rightarrow a^{-1} \equiv s \pmod{n}$$

✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = 1$, $x \equiv ?$

$$x \equiv a^{-1} \cdot b \equiv s \cdot b \pmod{n}$$

Are there any solutions?

✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

$$\text{if } d \nmid b \quad a\,x = b + k\,n \Rightarrow d\,a'\,x = b + k\,d\,n' \Rightarrow b = d\,(a'\,x - k\,n')$$

$$\Rightarrow d \mid b \quad \text{contradiction} \Rightarrow \text{no solution}$$

Operations under mod n

- What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  $\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

- $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = 1$, $x \equiv ?$

  $x \equiv a^{-1} \cdot b \equiv s \cdot b \pmod{n}$

Are there any solutions?

- $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

  if $d \nmid b$ $\quad a\,x = b + k\,n \Rightarrow d\,a'\,x = b + k\,d\,n' \Rightarrow b = d\,(a'\,x - k\,n')$

  $\Rightarrow d \mid b$ contradiction $\Rightarrow$ no solution

  if $d \mid b$

Operations under mod n

- ✧ What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

  $\gcd(a, n) = 1 \Rightarrow \exists$ integer s and t such that $a \cdot s + n \cdot t = 1$

  $\Rightarrow a^{-1} \equiv s \pmod{n}$

- ✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = 1$, $x \equiv ?$

  $x \equiv a^{-1} \cdot b \equiv s \cdot b \pmod{n}$

- ✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

  Are there any solutions?

  if $d \nmid b$ $\quad a\,x = b + k\,n \Rightarrow d\,a'\,x = b + k\,d\,n' \Rightarrow b = d\,(a'\,x - k\,n')$

  $\Rightarrow d \mid b$ contradiction $\Rightarrow$ no solution

  if $d \mid b$ $\quad (a/d) \cdot x \equiv (b/d) \pmod{n/d}$ $\quad \gcd(a/d,n/d) = 1$

  $x_0 \equiv (b/d) \cdot (a/d)^{-1} \pmod{n/d}$

Operations under mod n

- What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

Are there any solutions?

- $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

  if $d \nmid b$ $\quad a\,x = b + k\,n \;\Rightarrow\; d\,a'\,x = b + k\,d\,n' \;\Rightarrow\; b = d\,(a'\,x - k\,n')$

  $\Rightarrow\; d \mid b$ contradiction $\Rightarrow$ no solution

  if $d \mid b$ $\quad (a/d) \cdot x \equiv (b/d) \pmod{n/d}$ $\quad \gcd(a/d, n/d) = 1$

  $x_0 \equiv (b/d) \cdot (a/d)^{-1} \pmod{n/d}$

Operations under mod n

✧ What is the multiplicative inverse of a (mod n)?

i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

Are there any solutions?

✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

if $d \nmid b$ $\quad a\,x = b + k\,n \;\Rightarrow\; d\,a'\,x = b + k\,d\,n' \;\Rightarrow\; b = d\,(a'\,x - k\,n')$

$\Rightarrow d \mid b$ contradiction $\Rightarrow$ no solution

if $d \mid b$ $\quad (a/d) \cdot x \equiv (b/d) \pmod{n/d}$ $\quad \gcd(a/d, n/d) = 1$

$x_0 \equiv (b/d) \cdot (a/d)^{-1} \pmod{n/d}$

Operations under mod n

✧ What is the multiplicative inverse of a (mod n)?

i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

Are there any solutions?

✧ $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

if $d \nmid b$ $\quad a\,x = b + k\,n \Rightarrow d\,a'\,x = b + k\,d\,n' \Rightarrow b = d\,(a'\,x - k\,n')$

$\Rightarrow d \mid b$ contradiction $\Rightarrow$ no solution

if $d \mid b$ $\quad (a/d) \cdot x \equiv (b/d) \pmod{n/d}$ $\quad \gcd(a/d, n/d) = 1$

$x_0 \equiv (b/d) \cdot (a/d)^{-1} \pmod{n/d}$

Operations under mod n

- What is the multiplicative inverse of a (mod n)?

  i.e. $a \cdot a^{-1} \equiv 1 \pmod{n}$ or $a \cdot a^{-1} = 1 + k \cdot n$

Are there any solutions?

- $a \cdot x \equiv b \pmod{n}$, $\gcd(a, n) = d > 1$, $x \equiv ?$

  if $d \nmid b$ $\quad a\,x = b + k\,n \Rightarrow d\,a'\,x = b + k\,d\,n' \Rightarrow b = d\,(a'\,x - k\,n')$

  $\Rightarrow d \mid b$ contradiction $\Rightarrow$ no solution

  if $d \mid b$ $\quad (a/d) \cdot x \equiv (b/d) \pmod{n/d}$ $\quad \gcd(a/d, n/d) = 1$

  $x_0 \equiv (b/d) \cdot (a/d)^{-1} \pmod{n/d}$

Matrix inversion under mod n

- A square matrix is invertible mod n if and only if its determinant and n are relatively prime

Matrix inversion under mod n

- ✧ A square matrix is invertible mod n if and only if its determinant and n are relatively prime
- ✧ ex: in real field R

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Matrix inversion under mod n

- A square matrix is invertible mod n if and only if its determinant and n are relatively prime
- ex: in real field R

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

In a finite field Z (mod n)? we need to find the inverse for ad-bc (mod n) in order to calculate the inverse of the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \equiv (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \pmod{n}$$

Group

- A group G is a finite or infinite set of elements and a binary operation × which together satisfy

Group

- A group G is a finite or infinite set of elements and a binary operation × which together satisfy

  1. Closure: $\forall\ a,b \in G \quad a \times b = c \in G$ 封閉性

Group

- A group G is a finite or infinite set of elements and a binary operation × which together satisfy

  1. Closure: $\forall\ a,b \in G \quad a \times b = c \in G$ 封閉性
  2. Associativity: $\forall\ a,b,c \in G \quad (a \times b) \times c = a \times (b \times c)$ 結合性

Group

✧ A group G is a finite or infinite set of elements and a binary operation × which together satisfy

1. Closure: $\forall\ a,b \in G$ $\quad a \times b = c \in G$ 封閉性
2. Associativity: $\forall\ a,b,c \in G$ $\quad (a \times b) \times c = a \times (b \times c)$ 結合性
3. Identity: $\forall\ a \in G$ $\quad 1 \times a = a \times 1 = a$ 單位元素

Group

- A group G is a finite or infinite set of elements and a binary operation × which together satisfy

1. Closure:	$\forall\ a,b \in G$	$a \times b = c \in G$	封閉性
2. Associativity:	$\forall\ a,b,c \in G$	$(a \times b) \times c = a \times (b \times c)$	結合性
3. Identity:	$\forall\ a \in G$	$1 \times a = a \times 1 = a$	單位元素
4. Inverse:	$\forall\ a \in G$	$a \times a^{-1} = 1 = a^{-1} \times a$	反元素

Group

- A group G is a finite or infinite set of elements and a binary operation × which together satisfy

1. Closure:	$\forall a,b \in G$	$a \times b = c \in G$	封閉性
2. Associativity:	$\forall a,b,c \in G$	$(a \times b) \times c = a \times (b \times c)$	結合性
3. Identity:	$\forall a \in G$	$1 \times a = a \times 1 = a$	單位元素
4. Inverse:	$\forall a \in G$	$a \times a^{-1} = 1 = a^{-1} \times a$	反元素

- Abelian group 交換群 $\forall a,b \in G$ $a \times b = b \times a$

Group

- A group G is a finite or infinite set of elements and a binary operation × which together satisfy

1. Closure:	$\forall$ a,b $\in$G	a × b = c $\in$G	封閉性
2. Associativity:	$\forall$ a,b,c $\in$G	(a × b) × c = a × (b × c)	結合性
3. Identity:	$\forall$ a $\in$G	1 × a = a × 1 = a	單位元素
4. Inverse:	$\forall$ a $\in$G	a × a^{-1} = 1 = a^{-1} × a	反元素

- Abelian group 交換群 $\forall$ a,b $\in$G a × b = b × a

- Cyclic group G of order m: a group defined by an element g $\in$ G such that g, g^2, g^3, …. g^m are all distinct elements in G (thus cover all elements of G) and g^m = 1, the element g is called a generator of G. Ex: Z_n^* (or Z/nZ)

Group

- A group G is a finite or infinite set of elements and a binary operation × which together satisfy

1. Closure:	$\forall$ a,b $\in$G	a × b = c $\in$G	封閉性
2. Associativity:	$\forall$ a,b,c $\in$G	(a × b) × c = a × (b × c)	結合性
3. Identity:	$\forall$ a $\in$G	1 × a = a × 1 = a	單位元素
4. Inverse:	$\forall$ a $\in$G	a × a^{-1} = 1 = a^{-1} × a	反元素

- Abelian group 交換群 $\forall$ a,b $\in$G a × b = b × a

means g × g × g × … × g

- Cyclic group G of order m: a group defined by an element g $\in$ G such that g, g^2, g^3, …. g^m are all distinct elements in G (thus cover all elements of G) and $g^m = 1$, the element g is called a generator of G. Ex: Z_n^* (or Z/nZ)

Group (cont'd)

- The **order of a group**: the number of elements in a group G, denoted by |G|. If the order of a group is a finite number, the group is said to be a finite group, note $g^{|G|} = 1$ (the identity element).

Group (cont'd)

- The **order of a group**: the number of elements in a group G, denoted by |G|. If the order of a group is a finite number, the group is said to be a finite group, note $g^{|G|} = 1$ (the identity element).
- The **order of an element g** of a finite group G is the smallest power m such that $g^{m} = 1$ (the identity element), denoted by $\mathrm{ord}_G(g)$

Group (cont’d)

- The **order of a group**: the number of elements in a group G, denoted by |G|. If the order of a group is a finite number, the group is said to be a finite group, note $g^{|G|} = 1$ (the identity element).

- The **order of an element g** of a finite group G is the smallest power m such that $g^{m} = 1$ (the identity element), denoted by $ord_G(g)$

- ex: $\mathbf{Z_n}$: additive group modulo n is the set {0, 1, …, n-1}

  binary operation: + (mod n)

  identity: 0

  inverse: -x ≡ n-x (mod n) Algorithm

Group (cont'd)

- The **order of a group**: the number of elements in a group G, denoted by |G|. If the order of a group is a finite number, the group is said to be a finite group, note $g^{|G|} = 1$ (the identity element).
- The **order of an element g** of a finite group G is the smallest power m such that $g^m = 1$ (the identity element), denoted by $\mathrm{ord}_G(g)$
- ex: $\mathbf{Z_n}$: additive group modulo n is the set {0, 1, …, n-1}

  binary operation: + (mod n)
  identity: 0
  inverse: -x ≡ n-x (mod n) Algorithm

size of Z_n is n,
$\underbrace{g+g+\ldots+g}_{} \equiv 0 \pmod{n}$

Group (cont'd)

- The **order of a group**: the number of elements in a group G, denoted by |G|. If the order of a group is a finite number, the group is said to be a finite group, note $g^{|G|} = 1$ (the identity element).
- The **order of an element g** of a finite group G is the smallest power m such that $g^m = 1$ (the identity element), denoted by $\mathrm{ord}_G(g)$
- ex: $\mathbf{Z_n}$: additive group modulo n is the set {0, 1, …, n-1}

  binary operation: + (mod n)

  identity: 0

  inverse: $-x \equiv n-x \pmod{n}$ Algorithm

  size of Z_n is n,

  $\underbrace{g+g+\ldots+g}_{} \equiv 0 \pmod{n}$
- ex: $\mathbf{Z_n^*}$: multiplicative group modulo n is the set {i:0<i<n, gcd(i,n)=1}

  binary operation: × (mod n)

  identity: 1

  inverse: x^{-1} can be found using extended Euclidean Algorithm

Group (cont'd)

- The **order of a group**: the number of elements in a group G, denoted by |G|. If the order of a group is a finite number, the group is said to be a finite group, note $g^{|G|} = 1$ (the identity element).
- The **order of an element g** of a finite group G is the smallest power m such that $g^m = 1$ (the identity element), denoted by $\mathrm{ord}_G(g)$
- ex: $\mathbf{Z_n}$: additive group modulo n is the set {0, 1, …, n-1}

  binary operation: + (mod n)
  identity: 0
  inverse: -x ≡ n-x (mod n) Algorithm

  size of Z_n is n,
  $\underbrace{g+g+\ldots+g}_{} \equiv 0 \pmod n$

- ex: $\mathbf{Z_n^*}$: multiplicative group modulo n is the set {i:0<i<n, gcd(i,n)=1}

  binary operation: × (mod n)
  identity: 1
  inverse: x^{-1} can be found using extended Euclidean Algorithm

  size of Z_n^* is $\phi(n)$,
  $g^{\phi(n)} \equiv 1 \pmod n$

Ring Z_m

- ✧ **Definition:** The ring Z_m consists of

Ring Z_m

- **Definition:** The ring Z_m consists of
  - The set $Z_m = \{0, 1, 2, \ldots, m\text{-}1\}$

Ring Z_m

- **Definition:** The ring Z_m consists of
  - The set $Z_m = \{0, 1, 2, \ldots, m\text{-}1\}$
  - Two operations "+ (mod m)" and "× (mod m)" for all $a, b \in Z_m$ such that they satisfy the properties on the next slide

Ring Z_m

- **Definition:** The ring Z_m consists of
  - The set $Z_m = \{0, 1, 2, \ldots, m\text{-}1\}$
  - Two operations "+ (mod m)" and "× (mod m)" for all $a, b \in Z_m$ such that they satisfy the properties on the next slide

- **Example:** $m = 9$ $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$$6 + 8 = 14 \equiv 5 \pmod 9$$

$$6 \times 8 = 48 \equiv 3 \pmod 9$$

Properties of the ring Z_m

- Consider the ring $Z_m = \{0, 1, \ldots, m\text{-}1\}$

Properties of the ring Z_m

- Consider the ring $Z_m = \{0, 1, \ldots, m\text{-}1\}$
  - The additive identity "0": $a + 0 \equiv a \pmod{m}$
  - The additive inverse of a: $-a = m - a$ s.t. $a + (-a) \equiv 0 \pmod{m}$
  - Addition is closed i.e if $a, b \in Z_m$ then $a + b \in Z_m$
  - Addition is associative $(a + b) + c \equiv a + (b + c) \pmod{m}$

Properties of the ring Z_m

- Consider the ring $Z_m = \{0, 1, \ldots, m\text{-}1\}$
  - The additive identity "0": $a + 0 \equiv a \pmod{m}$
  - The additive inverse of a: $-a = m - a$ s.t. $a + (-a) \equiv 0 \pmod{m}$
  - Addition is closed i.e if $a, b \in Z_m$ then $a + b \in Z_m$
  - Addition is associative $(a + b) + c \equiv a + (b + c) \pmod{m}$
  - Addition is commutative $a + b \equiv b + a \pmod{m}$

Properties of the ring Z_m

- Consider the ring $Z_m = \{0, 1, \ldots, m\text{-}1\}$
  - The additive identity “0”: $a + 0 \equiv a \pmod{m}$
  - The additive inverse of a: $-a = m - a$ s.t. $a + (-a) \equiv 0 \pmod{m}$
  - Addition is closed i.e if $a, b \in Z_m$ then $a + b \in Z_m$
  - Addition is associative $(a + b) + c \equiv a + (b + c) \pmod{m}$
  - Addition is commutative $a + b \equiv b + a \pmod{m}$

  - Multiplicative identity “1”: $a \times 1 \equiv a \pmod{m}$
  - The multiplicative inverse of a exists only when $\gcd(a,m) = 1$ and denoted as a^{-1} s.t. $a^{-1} \times a \equiv 1 \pmod{m}$
  - Multiplication is closed i.e. if $a, b \in Z_m$ then $a \times b \in Z_m$
  - Multiplication is associative $(a \times b) \times c \equiv a \times (b \times c) \pmod{m}$

Properties of the ring Z_m

- Consider the ring $Z_m = \{0, 1, \ldots, m\text{-}1\}$
  - The additive identity "0": $a + 0 \equiv a \pmod{m}$
  - The additive inverse of a: $-a = m - a$ s.t. $a + (-a) \equiv 0 \pmod{m}$
  - Addition is closed i.e if $a, b \in Z_m$ then $a + b \in Z_m$
  - Addition is associative $(a + b) + c \equiv a + (b + c) \pmod{m}$
  - Addition is commutative $a + b \equiv b + a \pmod{m}$

  - Multiplicative identity "1": $a \times 1 \equiv a \pmod{m}$
  - The multiplicative inverse of a exists only when $\gcd(a,m) = 1$ and denoted as a^{-1} s.t. $a^{-1} \times a \equiv 1 \pmod{m}$
  - Multiplication is closed i.e. if $a, b \in Z_m$ then $a \times b \in Z_m$
  - Multiplication is associative $(a \times b) \times c \equiv a \times (b \times c) \pmod{m}$
  - Multiplication is commutative $a \times b \equiv b \times a \pmod{m}$

Properties of the ring Z_m

- Consider the ring $Z_m = \{0, 1, \ldots, m\text{-}1\}$
  - The additive identity “0”: $a + 0 \equiv a \pmod{m}$
  - The additive inverse of a: $-a = m - a$ s.t. $a + (-a) \equiv 0 \pmod{m}$
  - Addition is closed i.e if $a, b \in Z_m$ then $a + b \in Z_m$
  - Addition is associative $(a + b) + c \equiv a + (b + c) \pmod{m}$
  - Addition is commutative $a + b \equiv b + a \pmod{m}$

  - Multiplicative identity “1”: $a \times 1 \equiv a \pmod{m}$
  - The multiplicative inverse of a exists only when $\gcd(a,m) = 1$ and denoted as a^{-1} s.t. $a^{-1} \times a \equiv 1 \pmod{m}$ **might or might not exist**
  - Multiplication is closed i.e. if $a, b \in Z_m$ then $a \times b \in Z_m$
  - Multiplication is associative $(a \times b) \times c \equiv a \times (b \times c) \pmod{m}$
  - Multiplication is commutative $a \times b \equiv b \times a \pmod{m}$

Some remarks on the ring Z_m

- A ring is an Abelian group under addition and an Abelian semigroup under multiplication..

Some remarks on the ring Z_m

- A ring is an Abelian group under addition and an Abelian semigroup under multiplication..

- A semigroup is defined for a **set** and an associative **binary operator**. No other restrictions are placed on a semigroup; thus a semigroup need not have an **identity** element and its elements need not have **inverses** within the semigroup.

Some remarks on the ring Z_m (cont'd)

- Roughly speaking a ring is a mathematical structure in which we can add, subtract, multiply, and even sometimes divide. (A ring in which every element has multiplicative inverse is called a field.)

Some remarks on the ring Z_m (cont'd)

- Roughly speaking a ring is a mathematical structure in which we can add, subtract, multiply, and even sometimes divide. (A ring in which every element has multiplicative inverse is called a field.)
    - **Example:** Is the division 4/15 (mod 26) possible?

      In fact, $4/15 \bmod 26 \equiv 4 \times 15^{-1} \pmod{26}$

      Does $15^{-1} \pmod{26}$ exist ?

      It exists if $\gcd(15, 26) = 1$.

      $15^{-1} \equiv 7 \pmod{26}$ therefore,

      $4/15 \bmod 26 \equiv 4 \times 7 \equiv 28 \equiv 2 \bmod 26$

Some remarks on the group Z_m *and* Z_m^*

- The modulo operation can be applied whenever we want

Some remarks on the group Z_m *and* Z_m^*

✧ The modulo operation can be applied whenever we want

in Z_m

(a + b) (mod m) ≡ [(a (mod m)) + ((b mod m))] (mod m)

Some remarks on the group Z_m *and* $Z_m{}^*$

✧ The modulo operation can be applied whenever we want

in Z_m

$$(\boldsymbol{a} + \boldsymbol{b})\ (\mathbf{mod}\ \boldsymbol{m}) \equiv [(\boldsymbol{a}\ (\mathbf{mod}\ \boldsymbol{m})) + ((\boldsymbol{b}\ \mathbf{mod}\ \boldsymbol{m}))\ ]\ (\mathbf{mod}\ \boldsymbol{m})$$

in Z_m^*

$$(\boldsymbol{a} \times \boldsymbol{b})\ (\mathbf{mod}\ \boldsymbol{m}) \equiv [(\boldsymbol{a}\ (\mathbf{mod}\ \boldsymbol{m})) \times ((\boldsymbol{b}\ \mathbf{mod}\ \boldsymbol{m}))\ ]\ (\mathbf{mod}\ \boldsymbol{m})$$

$$\boldsymbol{a}^{\boldsymbol{b}}\ (\mathbf{mod}\ \boldsymbol{m}) \equiv (\boldsymbol{a}\ (\mathbf{mod}\ \boldsymbol{m}))^{\boldsymbol{b}}\ (\mathbf{mod}\ \boldsymbol{m})$$

Some remarks on the group Z_m *and* Z_m^*

- The modulo operation can be applied whenever we want

in Z_m

$$(a + b) \pmod{m} \equiv [(a \pmod{m}) + ((b \bmod m))\ ] \pmod{m}$$

in Z_m^*

$$(a \times b) \pmod{m} \equiv [(a \pmod{m}) \times ((b \bmod m))\ ] \pmod{m}$$

$$a^b \pmod{m} \equiv (a \pmod{m})^b \pmod{m}$$

- Question? $a^b \pmod{m} \overset{?}{\equiv} a^{\boxed{(b \bmod m)}} \pmod{m}$

Exponentiation in Z_m

- Example: $3^8 \pmod 7 \equiv ?$

Exponentiation in Z_m

- Example: $3^8 \pmod 7 \equiv ?$

$$3^8 \pmod 7 \equiv 6561 \pmod 7 \equiv 2 \text{ since } 6561 \equiv 937 \times 7 + 2$$

Exponentiation in Z_m

- Example: $3^8 \pmod 7 \equiv ?$

$$3^8 \pmod 7 \equiv 6561 \pmod 7 \equiv 2 \text{ since } 6561 \equiv 937 \times 7 + 2$$

or

$$\begin{aligned} 3^8 \pmod 7 &\equiv 3^4 \times 3^4 \pmod 7 \equiv 3^2 \times 3^2 \times 3^2 \times 3^2 \pmod 7 \\ &\equiv (3^2 \pmod 7)\times(3^2 \pmod 7)\times(3^2 \pmod 7)\times(3^2 \pmod 7) \\ &\equiv 2 \times 2 \times 2 \times 2 \pmod 7 \equiv 16 \pmod 7 \equiv 2 \end{aligned}$$

Exponentiation in Z_m

- Example: $3^8 \pmod 7 \equiv ?$

  $3^8 \pmod 7 \equiv 6561 \pmod 7 \equiv 2$ since $6561 \equiv 937 \times 7 + 2$

  or

  $$3^8 \pmod 7 \equiv 3^4 \times 3^4 \pmod 7 \equiv 3^2 \times 3^2 \times 3^2 \times 3^2 \pmod 7$$
  $$\equiv (3^2 \pmod 7)) \times (3^2 \pmod 7)) \times (3^2 \pmod 7)) \times (3^2 \pmod 7))$$
  $$\equiv 2 \times 2 \times 2 \times 2 \pmod 7 \equiv 16 \pmod 7 \equiv 2$$

- The cyclic group Z_m^* and the modulo arithmetic is of central importance to modern public-key cryptography. In practice, the order of the integers involved in PKC are in the range of $[2^{160}, 2^{1024}]$. Perhaps even larger.

Exponentiation in Z_m (cont'd)

- How do we do the exponentiation efficiently?

Exponentiation in Z_m (cont'd)

- ✧ How do we do the exponentiation efficiently?
- ✧ 3^{1234} (mod 789)   many ways to do this

Exponentiation in Z_m (cont’d)

- How do we do the exponentiation efficiently?
- $3^{1234} \pmod{789}$ many ways to do this

  a. do 1234 times multiplication and then calculate remainder

Exponentiation in Z_m (cont'd)

- How do we do the exponentiation efficiently?
- 3^{1234} (mod 789) many ways to do this
  - a. do 1234 times multiplication and then calculate remainder
  - b. repeat 1234 times (multiplication by 3 and calculate remainder)

Exponentiation in Z_m (cont'd)

- How do we do the exponentiation efficiently?
- $3^{1234} \pmod{789}$ many ways to do this

  a. do 1234 times multiplication and then calculate remainder

  b. repeat 1234 times (multiplication by 3 and calculate remainder)

  c. repeated $\lfloor \log 1234 \rfloor$ times (square, multiply and calculate remainder)

Exponentiation in Z_m (cont'd)

✧ How do we do the exponentiation efficiently?

✧ 3^{1234} (mod 789)   many ways to do this

a. do 1234 times multiplication and then calculate remainder

b. repeat 1234 times (multiplication by 3 and calculate remainder)

c. repeated $\lfloor \log 1234 \rfloor$ times (square, multiply and calculate remainder)

ex. first tabulate

3^2 9 (mod 789)

$3^4 \equiv 9^2 \equiv 81$

$3^8 \equiv 81^2 \equiv 249$

$3^{16} \equiv 249^2 \equiv 459$

$3^{32} \equiv 459^2 \equiv 18$

$3^{64} \equiv 18^2 \equiv 324$

$3^{128} \equiv 324^2 \equiv 39$

$3^{256} \equiv 39^2 \equiv 732$

$3^{512} \equiv 732^2 \equiv 93$

$3^{1024} \equiv 93^2 \equiv 759$

Exponentiation in Z_m (cont'd)

- How do we do the exponentiation efficiently?
- 3^{1234} (mod 789)   many ways to do this

a. do 1234 times multiplication and then calculate remainder

b. repeat 1234 times (multiplication by 3 and calculate remainder)

c. repeated $\lfloor \log 1234 \rfloor$ times (square, multiply and calculate remainder)

ex. first tabulate

3^2 9 (mod 789)

$3^4 \equiv 9^2 \equiv 81$

$3^8 \equiv 81^2 \equiv 249$

$3^{16} \equiv 249^2 \equiv 459$

$3^{32} \equiv 459^2 \equiv 18$

$3^{64} \equiv 18^2 \equiv 324$

$3^{128} \equiv 324^2 \equiv 39$

$3^{256} \equiv 39^2 \equiv 732$

$3^{512} \equiv 732^2 \equiv 93$

$3^{1024} \equiv 93^2 \equiv 759$

$1234 = 1024 + 128 + 64 + 16 + 2$ $(10011010010)_2$

Exponentiation in Z_m (cont'd)

- ✧ How do we do the exponentiation efficiently?
- ✧ 3^{1234} (mod 789) many ways to do this

a. do 1234 times multiplication and then calculate remainder

b. repeat 1234 times (multiplication by 3 and calculate remainder)

c. repeated $\lfloor \log 1234 \rfloor$ times (square, multiply and calculate remainder)

ex. first tabulate

3^2 9 (mod 789)	$3^{32} \equiv 459^2 \equiv 18$	$3^{512} \equiv 732^2 \equiv 93$
$3^4 \equiv 9^2 \equiv 81$	$3^{64} \equiv 18^2 \equiv 324$	$3^{1024} \equiv 93^2 \equiv 759$
$3^8 \equiv 81^2 \equiv 249$	$3^{128} \equiv 324^2 \equiv 39$	
$3^{16} \equiv 249^2 \equiv 459$	$3^{256} \equiv 39^2 \equiv 732$	

$1234 = 1024 + 128 + 64 + 16 + 2$ $(10011010010)_2$

$3^{1234} \equiv 3^{(1024+128+64+16+2)} \equiv (((759 \bullet 39) \bullet 324) \bullet 459) \bullet 9 \equiv 105 \pmod{789}$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod{m}$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod{m}$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

- ✧ Method 1:

$$x$$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod m$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

✧ Method 1:

$$x^{b_2}$$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod m$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

✧ Method 1:

$$\begin{tikzcd} x^{b_2} \arrow[r, bend right, "\text{square}"'] & x^{2} \end{tikzcd}$$

Exponentiation in Z_m (cont'd)

calculate x^y (mod m) where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

✧ Method 1:

$$\begin{tikzcd} x^{b_2} \arrow[r, Rightarrow] \arrow[rr, bend right, "\text{square}"'] & (x^{b_2}) & x^{2} \end{tikzcd}$$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod{m}$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

✧ Method 1:

$$x^{b_2} \Longrightarrow (x^{b_2}) \cdot (x^2)^{b_1}$$

square

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod{m}$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

✧ Method 1:

$$\begin{tikzcd} x^{b_2} \arrow[r, Rightarrow] \arrow[rr, bend right, "\text{square}"'] & (x^{b_2}) \cdot & (x^{2})^{b_1} \arrow[r, bend right, "\text{square}"'] & x^{4} \end{tikzcd}$$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod{m}$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

✧ Method 1:

$$\begin{tikzcd}
x^{b_2} \arrow[r, Rightarrow] \arrow[r, bend right, "\text{square}"'] & (x^{b_2}) \cdot (x^2)^{b_1} \arrow[r, Rightarrow] \arrow[rr, bend right, "\text{square}"'] & \left(x^{b_2} \cdot (x^2)^{b_1}\right) & x^4
\end{tikzcd}$$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod{m}$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

✧ Method 1:

$$\begin{tikzcd} x^{b_2} \arrow[r, Rightarrow] \arrow[r, bend right, "\text{square}"'] & (x^{b_2}) \cdot (x^2)^{b_1} \arrow[r, Rightarrow] \arrow[r, bend right, "\text{square}"'] & \left(x^{b_2} \cdot (x^2)^{b_1}\right) \cdot (x^4)^{b_0} \end{tikzcd}$$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod{m}$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

✧ Method 1:

$$\begin{tikzcd}
x^{b_2} \arrow[r, Rightarrow] \arrow[r, bend right, "\text{square}"'] & (x^{b_2}) \cdot (x^2)^{b_1} \arrow[r, Rightarrow] \arrow[r, bend right, "\text{square}"'] & \left(x^{b_2} \cdot (x^2)^{b_1}\right) \cdot (x^4)^{b_0}
\end{tikzcd}$$

✧ Method 2:

$$x$$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod{m}$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

- Method 1:

$$\begin{tikzcd} x^{b_2} \arrow[r] \arrow[r, bend right, "\text{square}"'] & (x^{b_2}) \cdot (x^2)^{b_1} \arrow[r] \arrow[r, bend right, "\text{square}"'] & \left(x^{b_2} \cdot (x^2)^{b_1}\right) \cdot (x^4)^{b_0} \end{tikzcd}$$

- Method 2:

$$x^{b_0}$$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod{m}$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

- ✧ Method 1:

$$\begin{tikzcd}
x^{b_2} \arrow[r, Rightarrow] \arrow[r, bend right, "\text{square}"'] & (x^{b_2}) \cdot (x^2)^{b_1} \arrow[r, Rightarrow] \arrow[r, bend right, "\text{square}"'] & \left(x^{b_2} \cdot (x^2)^{b_1}\right) \cdot (x^4)^{b_0}
\end{tikzcd}$$

- ✧ Method 2:

$$\begin{tikzcd}
x^{b_0} \arrow[r, bend right, "\text{square}"'] & (x^{b_0})^2
\end{tikzcd}$$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod m$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

✧ Method 1:

$$\begin{tikzcd} x^{b_2} \arrow[r, Rightarrow] \arrow[r, bend right, "\text{square}"'] & (x^{b_2})\cdot(x^2)^{b_1} \arrow[r, Rightarrow] \arrow[r, bend right, "\text{square}"'] & \left(x^{b_2}\cdot(x^2)^{b_1}\right)\cdot(x^4)^{b_0} \end{tikzcd}$$

✧ Method 2:

$$\begin{tikzcd} x^{b_0} \arrow[r, Rightarrow] \arrow[r, bend right, "\text{square}"'] & (x^{b_0})^2 \cdot x^{b_1} \end{tikzcd}$$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod{m}$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

✧ Method 1:

$$\begin{tikzcd}
x^{b_2} \arrow[r, Rightarrow] \arrow[rr, bend right, "\text{square}"'] & (x^{b_2}) \cdot & (x^2)^{b_1} \arrow[r, Rightarrow] \arrow[rr, bend right, "\text{square}"'] & \left(x^{b_2} \cdot (x^2)^{b_1}\right) \cdot & (x^4)^{b_0}
\end{tikzcd}$$

✧ Method 2:

$$\begin{tikzcd}
x^{b_0} \arrow[r, Rightarrow] \arrow[r, bend right, "\text{square}"'] & (x^{b_0})^2 \cdot x^{b_1} \arrow[r, bend right, "\text{square}"'] & (x^{2 \cdot b_0 + b_1})^2
\end{tikzcd}$$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod{m}$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

- Method 1:

$$\begin{tikzcd}
x^{b_2} \arrow[r, Rightarrow] \arrow[r, bend right=40, "\text{square}"'] & (x^{b_2}) \cdot (x^2)^{b_1} \arrow[r, Rightarrow] \arrow[r, bend right=40, "\text{square}"'] & \left(x^{b_2} \cdot (x^2)^{b_1}\right) \cdot (x^4)^{b_0}
\end{tikzcd}$$

- Method 2:

$$\begin{tikzcd}
x^{b_0} \arrow[r, Rightarrow] \arrow[r, bend right=40, "\text{square}"'] & (x^{b_0})^2 \cdot x^{b_1} \arrow[r, Rightarrow] \arrow[r, bend right=40, "\text{square}"'] & (x^{2 \cdot b_0 + b_1})^2 \cdot x^{b_2}
\end{tikzcd}$$

Exponentiation in Z_m (cont'd)

calculate $x^y \pmod m$ where $y = b_0 \cdot 2^2 + b_1 \cdot 2 + b_2$

✧ Method 1:

$$x^{b_2} \Longrightarrow (x^{b_2})\,\underline{\cdot}\,(\underline{x^2})^{b_1} \Longrightarrow \left(x^{b_2}\cdot(x^2)^{b_1}\right)\underline{\cdot}\,(\underline{x^4})^{b_0}$$

square square

✧ Method 2:

$$x^{b_0} \Longrightarrow \underline{(x^{b_0})^2}\;\underline{\cdot}\, x^{b_1} \Longrightarrow \underline{(x^{2\cdot b_0+b_1})^2}\;\underline{\cdot}\, x^{b_2}$$

square square

square and **multiply** $\lfloor \log y \rfloor$ times

Exponentiation in Z_m (cont'd)

Method 1:

$$1234 = 1024 + 128 + 64 + 16 + 2 \qquad (10011010010)_2$$

$$3^{1234} \equiv 3^{0+2(1+2(0+2(0+2(1+2(0+2(1+2(1+2(0+2(0+2(1))))))))))}$$

$$\equiv 9 \cdot 9^{2(0+2(0+2(1+2(0+2(1+2(1+2(0+2(0+2(1)))))))))}$$

$$\equiv 9 \cdot 81^{2(0+2(1+2(0+2(1+2(1+2(0+2(0+2(1))))))))}$$

$$\equiv 9 \cdot 249^{2(1+2(0+2(1+2(1+2(0+2(0+2(1)))))))}$$

$$\equiv 9 \cdot 459 \cdot 459^{2(0+2(1+2(1+2(0+2(0+2(1))))))}$$

$$\equiv 9 \cdot 459 \cdot 18^{2(1+2(1+2(0+2(0+2(1)))))}$$

$$\equiv 9 \cdot 459 \cdot 324 \cdot 324^{2(1+2(0+2(0+2(1))))}$$

$$\equiv 9 \cdot 459 \cdot 324 \cdot 39 \cdot 39^{2(0+2(0+2(1)))}$$

$$\equiv 9 \cdot 459 \cdot 324 \cdot 39 \cdot 732^{2(0+2(1))}$$

$$\equiv 9 \cdot 459 \cdot 324 \cdot 39 \cdot 93^{2(1)}$$

$$\equiv 9 \cdot 459 \cdot 324 \cdot 39 \cdot 759 \bmod 789$$

Exponentiation in Z_m (cont’d)

Method 2: $1234 = 1024 + 128 + 64 + 16 + 2 \qquad (10011010010)_2$

$$3^{1234} \equiv 3^{0+2(1+2(0+2(0+2(1+2(0+2(1+2(1+2(0+2(0+2(1))))))))))}$$

$$\equiv (3\bullet\ 3^{2(0+2(1+2(0+2(1+2(1+2(0+2(0+2(1))))))))})^2$$

$$\equiv (3\bullet(3^{2(1+2(\ 0+2(1+2(1+2(0+2(0+2(1)))))))})^2)^2$$

$$\equiv (3\bullet((3\bullet 3^{2(\ 0+2(1+2(1+2(0+2(0+2(1))))))})^2)^2)^2$$

$$\equiv (3\bullet((3\bullet(3^{2(1+2(1+2(0+2(0+2(1)))))})^2)^2\ )^2)^2$$

$$\equiv (3\bullet((3\bullet((3\bullet 3^{2(1+2(0+2(0+2(1))))})^2)^2\ )^2)^2)^2$$

$$\equiv (3\bullet((3\bullet((3\bullet(3\bullet 3^{2(0+2(0+2(1)))})^2\ )^2)^2\ )^2)^2)^2$$

$$\equiv (3\bullet((3\bullet((3\bullet(3\bullet(3^{2(0+2(1))})^2\ )^2)^2)^2\ )^2)^2)^2$$

$$\equiv (3\bullet((3\bullet((3\bullet(3\bullet((3^{2(1)})^2\ )^2)^2)^2\ )^2\ )^2)^2)^2$$

$$\equiv (3\bullet((3\bullet((3\bullet(3\bullet(((3^{1})^2\ )^2\ )^2)^2)^2\ )^2\ )^2)^2)^2$$

Chinese Remainder Theorem (CRT)

✧ $\forall\ i \neq j \in \{1,2,\ldots k\}$, $\gcd(r_i, r_j) = 1$, $0 \leq m_i < r_i$
Is there an m that satisfies simultaneously the following set of congruence equations?

$$
\begin{aligned}
m &\equiv m_1 \pmod{r_1}\\
&\equiv m_2 \pmod{r_2}\\
&\quad \bullet\bullet\bullet\\
&\equiv m_k \pmod{r_k}
\end{aligned}
$$

Chinese Remainder Theorem (CRT)

- $\forall\ i \neq j \in \{1,2,\ldots k\}$, $\gcd(r_i, r_j) = 1$, $0 \le m_i < r_i$
  Is there an m that satisfies simultaneously the following set of congruence equations?

$$
\begin{aligned}
m &\equiv m_1 \pmod{r_1} \\
&\equiv m_2 \pmod{r_2} \\
&\;\;\bullet \bullet \bullet \\
&\equiv m_k \pmod{r_k}
\end{aligned}
$$

ex: $m \equiv 1 \pmod 3$
$\equiv 2 \pmod 5$
$\equiv 3 \pmod 7$

Note: $\gcd(3,5) = 1$
$\gcd(3,7) = 1$
$\gcd(5,7) = 1$

Chinese Remainder Theorem (CRT)

- $\forall\ i \neq j \in \{1,2,\ldots k\},\ \gcd(r_i, r_j) = 1,\ 0 \leq m_i < r_i$

  Is there an m that satisfies simultaneously the following set of congruence equations?

$$
\begin{aligned}
m &\equiv m_1 \pmod{r_1} \\
&\equiv m_2 \pmod{r_2} \\
&\bullet\bullet\bullet \\
&\equiv m_k \pmod{r_k}
\end{aligned}
$$

ex: $m \equiv 1 \pmod 3$

$\equiv 2 \pmod 5$

$\equiv 3 \pmod 7$

Note: $\gcd(3,5) = 1$

$\gcd(3,7) = 1$

$\gcd(5,7) = 1$

- 韓信點兵: 三個一數餘一, 五個一數餘二, 七個一數餘三, 請問隊伍中至少有幾名士兵?

Chinese Remainder Theorem (CRT)

✧ first solution:

Chinese Remainder Theorem (CRT)

- first solution:

$$n = r_1\, r_2 \cdots r_k$$

Chinese Remainder Theorem (CRT)

- ✧ first solution:

$$n = r_1\, r_2 \cdot \cdot \cdot r_k$$

$$z_i = n \,/\, r_i$$

Chinese Remainder Theorem (CRT)

- first solution:

$$n = r_1\, r_2 \cdot \cdot \cdot r_k$$

$$z_i = n \,/\, r_i$$

$$\exists!\ s_i \in Z^*_{ri} \ \text{ s.t. } \ s_i \cdot z_i \equiv 1 \ (\text{mod } r_i) \ (\text{since } \gcd(z_i, r_i) = 1)$$

Chinese Remainder Theorem (CRT)

✧ first solution:

$$n = r_1\, r_2 \cdot \cdot \cdot r_k$$

$$z_i = n \,/\, r_i$$

$$\exists!\ s_i \in Z^*_{ri} \text{ s.t. } s_i \cdot z_i \equiv 1 \pmod{r_i} \text{ (since } \gcd(z_i, r_i) = 1)$$

$$m \equiv \sum_{i=1}^{k} z_i \cdot s_i \cdot m_i \pmod{n}$$

Chinese Remainder Theorem (CRT)

- first solution:

$$n = r_1 r_2 \cdot \cdot \cdot r_k$$

$$z_i = n / r_i$$

$$\exists!\ s_i \in Z^*_{ri} \ \text{ s.t. } \ s_i \cdot z_i \equiv 1 \pmod{r_i} \text{ (since } \gcd(z_i, r_i) = 1)$$

$$m \equiv \sum_{i=1}^{k} z_i \cdot s_i \cdot m_i \pmod{n}$$

- ex: $m_1=1,\ m_2=2, m_3=3$

$r_1=3, \quad r_2=5, \quad r_3=7 \qquad\qquad n = 3 \cdot 5 \cdot 7$

Chinese Remainder Theorem (CRT)

✧ first solution:

$$n = r_1 \, r_2 \cdot \cdot \cdot r_k$$

$$z_i = n \,/\, r_i$$

$$\exists!\; s_i \in Z^*_{ri} \;\text{ s.t. }\; s_i \cdot z_i \equiv 1 \pmod{r_i} \text{ (since } \gcd(z_i, r_i) = 1)$$

$$m \equiv \sum_{i=1}^{k} z_i \cdot s_i \cdot m_i \pmod{n}$$

✧ ex: $m_1=1$, $m_2=2$, $m_3=3$

$r_1=3$, $r_2=5$, $r_3=7$ $n = 3 \cdot 5 \cdot 7$

$z_1=35$, $z_2=21$, $z_3=15$

Chinese Remainder Theorem (CRT)

✧ first solution:

$$n = r_1 \, r_2 \cdot \cdot \cdot r_k$$

$$z_i = n / r_i$$

$$\exists! \; s_i \in Z^*_{ri} \;\; \text{s.t.} \;\; s_i \cdot z_i \equiv 1 \pmod{r_i} \; (\text{since } \gcd(z_i, r_i) = 1)$$

$$m \equiv \sum_{i=1}^{k} z_i \cdot s_i \cdot m_i \pmod{n}$$

✧ ex: $m_1=1$, $m_2=2$, $m_3=3$

$r_1=3$, $r_2=5$, $r_3=7$ $\qquad n = 3 \cdot 5 \cdot 7$

$z_1=35$, $z_2=21$, $z_3=15$

$s_1=2$, $s_2=1$, $s_3=1$ $\qquad 35 \cdot 2 + 3\,(-23) = 1$

Chinese Remainder Theorem (CRT)

✧ first solution:

$$n = r_1\, r_2 \cdot \cdot \cdot r_k$$

$$z_i = n / r_i$$

$$\exists!\ s_i \in Z^*_{ri} \ \text{ s.t. } \ s_i \cdot z_i \equiv 1 \ (\text{mod } r_i)\ (\text{since gcd}(z_i, r_i) = 1)$$

$$m \equiv \sum_{i=1}^{k} z_i \cdot s_i \cdot m_i \ \ (\text{mod } n)$$

✧ ex: $m_1=1,\ m_2=2,\ m_3=3$

$r_1=3,\quad r_2=5,\quad r_3=7$ $\qquad\qquad n = 3 \cdot 5 \cdot 7$

$z_1=35,\ z_2=21,\ z_3=15$

$s_1=2,\quad s_2=1,\quad s_3=1$

$$m \equiv 35{\cdot}2{\cdot}1 + 21{\cdot}1{\cdot}2 + 15{\cdot}1{\cdot}3 \equiv 157 \equiv 52\ (\text{mod } 105)$$

Chinese Remainder Theorem (CRT)

✧ first solution:

$$n = r_1\, r_2 \cdot \cdot \cdot r_k$$

$$z_i = n / r_i$$

$$\exists!\ s_i \in Z^*_{ri}\ \text{ s.t. }\ s_i \cdot z_i \equiv 1 \pmod{r_i}\ (\text{since } \gcd(z_i, r_i) = 1)$$

$$m \equiv \sum_{i=1}^{k} z_i \cdot s_i \cdot m_i \pmod{n}$$

Unique solution in Z_n?

✧ ex: $m_1=1,\ m_2=2, m_3=3$

$r_1=3,\quad r_2=5,\quad r_3=7$ $\qquad n = 3 \cdot 5 \cdot 7$

$z_1=35, z_2=21, z_3=15$

$s_1=2,\quad s_2=1,\quad s_3=1$

$$m \equiv 35\cdot 2\cdot 1 + 21\cdot 1\cdot 2 + 15\cdot 1\cdot 3 \equiv 157 \equiv 52 \pmod{105}$$

Chinese Remainder Theorem (CRT)

✧ Uniqueness:

1. If there exists $m' \in Z_n$ $(\neq m)$ also satisfies the previous k congruence relations, then

$$\forall i,\ m'-m \equiv 0 \pmod{r_i}.$$

2. This is equivalent to $\forall i,\ r_i \mid m' - m$
3. $\forall i,j,\ \gcd(r_i, r_j) = 1 \ \Rightarrow\ r_1\, r_2 \ldots r_k \mid m' - m$

➡ $m' = m + k \cdot r_1, r_2 \ldots r_k = m + k \cdot n$

➡ $m' \notin Z_n$ for all $k \neq 0$

contradiction!

Chinese Remainder Theorem (CRT)

✧ second solution:

$$R_i = r_1\, r_2 \cdot \cdot \cdot\, r_{i-1}$$

$$\exists!\ t_i \in Z^*_{r_i} \ \text{ s.t. } t_i \cdot R_i \equiv 1 \ (\text{mod } r_i)\ (\text{since gcd}(R_i, r_i) = 1)$$

satisfies the first i-1 congruence relations

$$\begin{cases} \hat{m}_1 = m_1 \\ \hat{m}_i = \hat{m}_{i-1} + R_i \cdot (m_i - \hat{m}_{i-1}) \cdot t_i \ (\text{mod } R_{i+1}) \qquad i \geq 2 \\ m = \hat{m}_k \end{cases}$$

Note that $\hat{m}_i \equiv m_1 \ (\text{mod } r_1)$

$\equiv m_2 \ (\text{mod } r_2)$

• • •

$\equiv m_i \ (\text{mod } r_i)$

$m_1=1,\ \ m_2=2,\ m_3=3$

$r_1=3,\ \ \ r_2=5,\ \ \ r_3=7$

$R_2=3,\ R_3=15,\ R_4=105$

$t_2=2,\ \ \ t_3=1$

ex: $\hat{m}_1 \equiv 1$

$\hat{m}_2 \equiv 1+3\cdot(2\text{-}1)\cdot 2=7$

$\hat{m} \equiv m_3 \equiv 7+15\cdot(3\text{-}7)\cdot 1$

$\equiv \text{-}53 \equiv 52\ (\text{mod } 105)$

Incremental Manual Calculation

$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \\ &\equiv 3 \pmod{7} \end{aligned}$$

Incremental Manual Calculation

$$\begin{aligned} m &\equiv 1 \pmod 3) \\ &\equiv 2 \pmod 5) \\ &\equiv 3 \pmod 7) \end{aligned}$$

① $\hat{m}_1 \equiv 1 \pmod 3$ … satisfying the 1st eq.

Incremental Manual Calculation

$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \\ &\equiv 3 \pmod{7} \end{aligned}$$

$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \end{aligned}$$

① $\hat{m}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

Incremental Manual Calculation

$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \\ &\equiv 3 \pmod{7} \end{aligned} \qquad\qquad \begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \end{aligned}$$

① $\hat{m}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

Incremental Manual Calculation

$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \\ &\equiv 3 \pmod{7} \end{aligned}$$

$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \end{aligned}$$

① $\hat{m}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

inverse of 3 (mod 5)

② $3 \cdot (-3) + 5 \cdot 2 = 1$

Incremental Manual Calculation

$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \\ &\equiv 3 \pmod{7} \end{aligned} \qquad\qquad \begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \end{aligned}$$

① $\hat{m}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

inverse of 3 (mod 5)

② $3 \cdot (-3) + 5 \cdot 2 = 1$

inverse of 5 (mod 3)

Incremental Manual Calculation

$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \\ &\equiv 3 \pmod{7} \end{aligned} \qquad \begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \end{aligned}$$

① $\hat{m}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

inverse of 3 (mod 5)

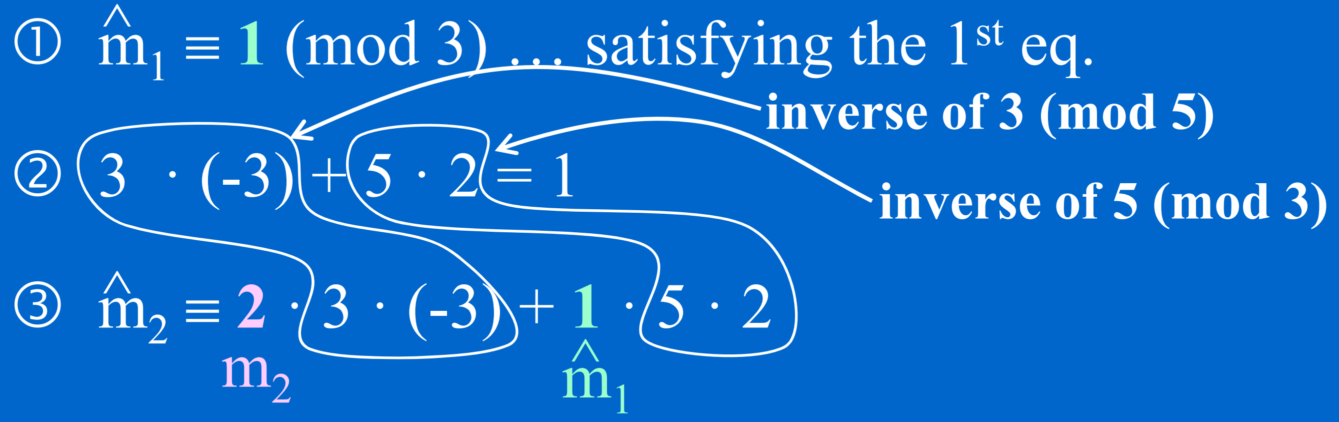
② $3 \cdot (-3) + 5 \cdot 2 = 1$

inverse of 5 (mod 3)

③ $\hat{m}_2 \equiv 2 \cdot 3 \cdot (-3) + \underset{\hat{m}_1}{1} \cdot 5 \cdot 2$

Incremental Manual Calculation

$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \\ &\equiv 3 \pmod{7} \end{aligned} \qquad\qquad \begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \end{aligned}$$



① $\hat{m}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{m}_2 \equiv \underset{m_2}{2} \cdot 3 \cdot (-3) + \underset{\hat{m}_1}{1} \cdot 5 \cdot 2$

inverse of 3 (mod 5)

inverse of 5 (mod 3)

Incremental Manual Calculation

$$\begin{aligned} m &\equiv 1 \pmod 3 \\ &\equiv 2 \pmod 5 \\ &\equiv 3 \pmod 7 \end{aligned} \qquad\qquad \begin{aligned} m &\equiv 1 \pmod 3 \\ &\equiv 2 \pmod 5 \end{aligned}$$

① $\hat{m}_1 \equiv 1 \pmod 3$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{m}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

Incremental Manual Calculation

$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \\ &\equiv 3 \pmod{7} \end{aligned}$$

$$\begin{aligned} m &\equiv 7 \pmod{15} \\ &\equiv 3 \pmod{7} \end{aligned}$$

① $\hat{m}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{m}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

Incremental Manual Calculation

$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \\ &\equiv 3 \pmod{7} \end{aligned}$$

$$\begin{aligned} m &\equiv 7 \pmod{15} \\ &\equiv 3 \pmod{7} \end{aligned}$$

① $\hat{m}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{m}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

④ $15 \cdot 1 + 7 \cdot (-2) = 1$

Incremental Manual Calculation

$m \equiv 1 \pmod{3}$
$\quad \equiv 2 \pmod{5}$
$\quad \equiv 3 \pmod{7}$

$m \equiv 7 \pmod{15}$
$\quad \equiv 3 \pmod{7}$

① $\hat{m}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{m}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

inverse of 15 (mod 7)

④ $15 \cdot 1 + 7 \cdot (-2) = 1$

inverse of 7 (mod 15)

Incremental Manual Calculation

$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \\ &\equiv 3 \pmod{7} \end{aligned}$$

$$\begin{aligned} m &\equiv 7 \pmod{15} \\ &\equiv 3 \pmod{7} \end{aligned}$$

① $\hat{m}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{m}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

inverse of 15 (mod 7)

④ $15 \cdot 1 + 7 \cdot (-2) = 1$

inverse of 7 (mod 15)

⑤ $\hat{m}_3 \equiv 3 \cdot 15 \cdot 1 + \underset{\hat{m}_2}{7} \cdot 7 \cdot (-2)$

Incremental Manual Calculation

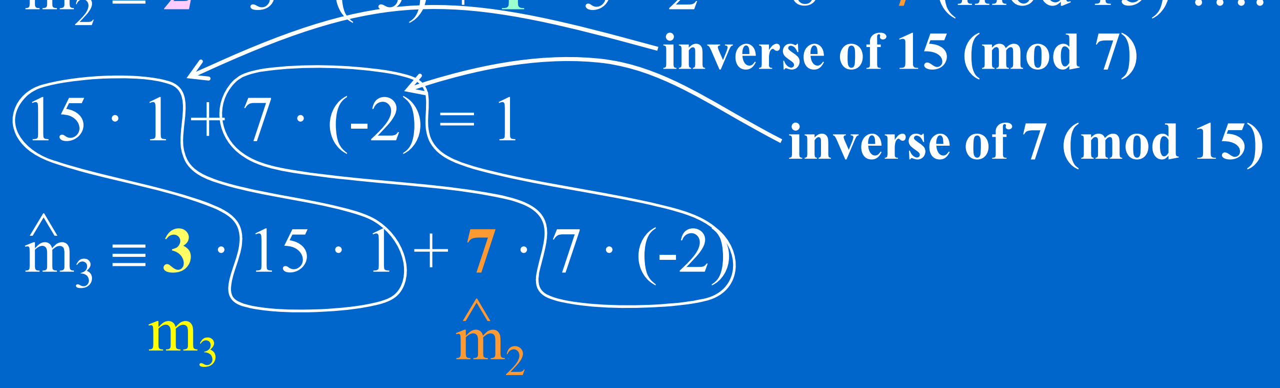
$$\begin{aligned} m &\equiv 1 \pmod{3} \\ &\equiv 2 \pmod{5} \\ &\equiv 3 \pmod{7} \end{aligned}$$

$$\begin{aligned} m &\equiv 7 \pmod{15} \\ &\equiv 3 \pmod{7} \end{aligned}$$

① $\hat{m}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{m}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.



④ $15 \cdot 1 + 7 \cdot (-2) = 1$

inverse of 15 (mod 7)

inverse of 7 (mod 15)

⑤ $\hat{m}_3 \equiv \underbrace{3}_{m_3} \cdot 15 \cdot 1 + \underbrace{7}_{\hat{m}_2} \cdot 7 \cdot (-2)$

Incremental Manual Calculation

$$
\begin{aligned}
m &\equiv 1 \pmod{3} \\
&\equiv 2 \pmod{5} \\
&\equiv 3 \pmod{7}
\end{aligned}
$$

① $\hat{m}_1 \equiv 1 \pmod{3}$ … satisfying the 1st eq.

② $3 \cdot (-3) + 5 \cdot 2 = 1$

③ $\hat{m}_2 \equiv 2 \cdot 3 \cdot (-3) + 1 \cdot 5 \cdot 2 \equiv -8 \equiv 7 \pmod{15}$ …. satisfying first 2 eqs.

④ $15 \cdot 1 + 7 \cdot (-2) = 1$

⑤ $\hat{m}_3 \equiv 3 \cdot 15 \cdot 1 + 7 \cdot 7 \cdot (-2) \equiv -53 \equiv \mathbf{52} \pmod{105}$ … satisfying all 3 eqs.

Chinese Remainder Theorem (CRT)

✧ special case:

$$x \equiv m \pmod{r_1} \equiv m \pmod{r_2} \cdots \equiv m \pmod{r_n} \Rightarrow x \equiv m \pmod{r_1 r_2 \cdots r_n}$$

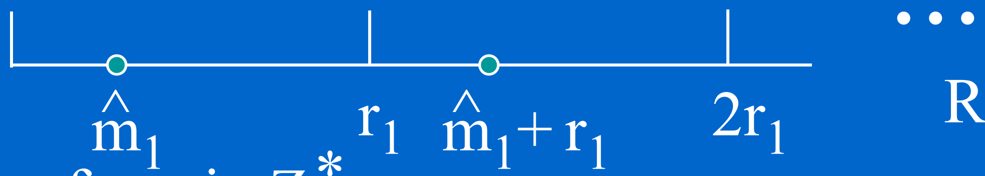
✧ insight of the second solution:

every step satisfies one more equation

step 1

$x \equiv m_1 \pmod{r_1}$

let $\hat{m}_1 = m_1$



$R_2 = r_1$

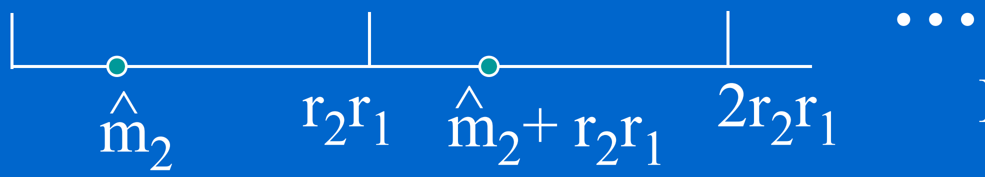
m_1 is the only solution for x in $Z^*_{R_2}$

general solution of x must be $\hat{m}_1 + k\, R_2$ for some k

step 2

$x \equiv m_1 \pmod{r_1}$

$\equiv m_2 \pmod{r_2}$



$R_3 = r_2 r_1$

let $\hat{m}_2 \equiv \hat{m}_1 + k^*\, R_2 \pmod{R_3}$ where $k^* = t_2(m_2 - \hat{m}_1)$ and $t_2\, R_2 \equiv 1 \pmod{r_2}$

m_2 is the only solution for x in $Z^*_{R_3}$

general solution of x must be $\hat{m}_2 + k\, R_3$ for some k

Chinese Remainder Theorem (CRT)

- Applications: solve $x^2 \equiv 1 \pmod{35}$
  - $35 = 5 \cdot 7$
  - x^* satisfies $f(x^*) \equiv 0 \pmod{35}$ $\Leftrightarrow$
    x^* satisfies both $f(x^*) \equiv 0 \pmod 5$ and $f(x^*) \equiv 0 \pmod 7$

  Proof:

  $(\Leftarrow)$

  $p \mid f(x^*)$, $q \mid f(x^*)$, and $\gcd(p,q)=1$ imply that
  $p \cdot q \mid f(x^*)$ i.e. $f(x^*) \equiv 0 \pmod{p \cdot q}$

  $(\Rightarrow)$

  $f(x^*) = k \cdot p \cdot q$ implies that
  $f(x^*) = (k \cdot p) \cdot q = (k \cdot q) \cdot p$ i.e. $f(x^*) \equiv 0 \pmod p$
  $\equiv 0 \pmod q$

Chinese Remainder Theorem (CRT)

- since 5 and 7 are prime, we can solve

  $x^2 \equiv 1 \pmod 5$ and $x^2 \equiv 1 \pmod 7$

  far more easily than $x^2 \equiv 1 \pmod{35}$

Why?

Chinese Remainder Theorem (CRT)

- since 5 and 7 are prime, we can solve

  $x^2 \equiv 1 \pmod{5}$ and $x^2 \equiv 1 \pmod{7}$

  far more easily than $x^2 \equiv 1 \pmod{35}$

  - $x^2 \equiv 1 \pmod{5}$ has exactly two solutions: $x \equiv \pm 1 \pmod{5}$

Why?

Chinese Remainder Theorem (CRT)

- since 5 and 7 are prime, we can solve

  $x^2 \equiv 1 \pmod 5$ and $x^2 \equiv 1 \pmod 7$

  far more easily than $x^2 \equiv 1 \pmod{35}$

  Why?

  - $x^2 \equiv 1 \pmod 5$ has exactly two solutions: $x \equiv \pm 1 \pmod 5$
  - $x^2 \equiv 1 \pmod 7$ has exactly two solutions: $x \equiv \pm 1 \pmod 7$

Chinese Remainder Theorem (CRT)

- since 5 and 7 are prime, we can solve

  $$x^2 \equiv 1 \pmod{5} \text{ and } x^2 \equiv 1 \pmod{7}$$

  far more easily than $x^2 \equiv 1 \pmod{35}$

  Why?

  - $x^2 \equiv 1 \pmod{5}$ has exactly two solutions: $x \equiv \pm 1 \pmod{5}$
  - $x^2 \equiv 1 \pmod{7}$ has exactly two solutions: $x \equiv \pm 1 \pmod{7}$

- put them together and use CRT, there are four solutions

Chinese Remainder Theorem (CRT)

- since 5 and 7 are prime, we can solve

  $x^2 \equiv 1 \pmod 5$ and $x^2 \equiv 1 \pmod 7$

  far more easily than $x^2 \equiv 1 \pmod{35}$

  Why?

  - $x^2 \equiv 1 \pmod 5$ has exactly two solutions: $x \equiv \pm 1 \pmod 5$
  - $x^2 \equiv 1 \pmod 7$ has exactly two solutions: $x \equiv \pm 1 \pmod 7$

- put them together and use CRT, there are four solutions
  - $x \equiv 1 \pmod 5 \equiv 1 \pmod 7 \Rightarrow x \equiv 1 \pmod{35}$

Chinese Remainder Theorem (CRT)

- since 5 and 7 are prime, we can solve

  $x^2 \equiv 1 \pmod 5$ and $x^2 \equiv 1 \pmod 7$

  far more easily than $x^2 \equiv 1 \pmod{35}$

  Why?

  - $x^2 \equiv 1 \pmod 5$ has exactly two solutions: $x \equiv \pm 1 \pmod 5$
  - $x^2 \equiv 1 \pmod 7$ has exactly two solutions: $x \equiv \pm 1 \pmod 7$

- put them together and use CRT, there are four solutions
  - $x \equiv 1 \pmod 5 \equiv 1 \pmod 7 \Rightarrow x \equiv 1 \pmod{35}$
  - $x \equiv 1 \pmod 5 \equiv 6 \pmod 7 \Rightarrow x \equiv 6 \pmod{35}$

Chinese Remainder Theorem (CRT)

- since 5 and 7 are prime, we can solve

  $x^2 \equiv 1 \pmod{5}$ and $x^2 \equiv 1 \pmod{7}$

  far more easily than $x^2 \equiv 1 \pmod{35}$

  Why?

  - $x^2 \equiv 1 \pmod{5}$ has exactly two solutions: $x \equiv \pm 1 \pmod{5}$
  - $x^2 \equiv 1 \pmod{7}$ has exactly two solutions: $x \equiv \pm 1 \pmod{7}$
- put them together and use CRT, there are four solutions
  - $x \equiv 1 \pmod{5} \equiv 1 \pmod{7} \Rightarrow x \equiv 1 \pmod{35}$
  - $x \equiv 1 \pmod{5} \equiv 6 \pmod{7} \Rightarrow x \equiv 6 \pmod{35}$
  - $x \equiv 4 \pmod{5} \equiv 1 \pmod{7} \Rightarrow x \equiv 29 \pmod{35}$

Chinese Remainder Theorem (CRT)

- since 5 and 7 are prime, we can solve

  $x^2 \equiv 1 \pmod 5$ and $x^2 \equiv 1 \pmod 7$

  far more easily than $x^2 \equiv 1 \pmod{35}$

  Why?

  - $x^2 \equiv 1 \pmod 5$ has exactly two solutions: $x \equiv \pm 1 \pmod 5$
  - $x^2 \equiv 1 \pmod 7$ has exactly two solutions: $x \equiv \pm 1 \pmod 7$

- put them together and use CRT, there are four solutions
  - $x \equiv 1 \pmod 5 \equiv 1 \pmod 7 \Rightarrow x \equiv 1 \pmod{35}$
  - $x \equiv 1 \pmod 5 \equiv 6 \pmod 7 \Rightarrow x \equiv 6 \pmod{35}$
  - $x \equiv 4 \pmod 5 \equiv 1 \pmod 7 \Rightarrow x \equiv 29 \pmod{35}$
  - $x \equiv 4 \pmod 5 \equiv 6 \pmod 7 \Rightarrow x \equiv 34 \pmod{35}$

Matlab tools

	format rat format long
matrix inverse	inv(A)
matrix determinant	det(A)
$p = q\ d + r$	r = mod(p, d) or r = rem(p, d)
	q = floor(p / d)
	g = gcd(a, b)
$g = a\ s + b\ t$	[g, s, t] = gcd(a, b)
factoring	factor(N)
prime numbers < N	primes(N)
test prime	isprime(p)
mod exponentiation *	powermod(a,b,n)
find primitive root *	primitiveroot(p)
crt *	crt([a_1 a_2 a_3...], [m_1 m_2 m_3...])
$\phi(N)$ *	eulerphi(N)

Field

- Field: a set that has the operation of addition, multiplication, subtraction, and division by nonzero elements. Also, the associative, commutative, and distributive laws hold.

Field

- Field: a set that has the operation of addition, multiplication, subtraction, and division by nonzero elements. Also, the associative, commutative, and distributive laws hold.
- Ex. Real numbers, complex numbers, rational numbers, integers mod a prime are fields

Field

- Field: a set that has the operation of addition, multiplication, subtraction, and division by nonzero elements. Also, the associative, commutative, and distributive laws hold.
- Ex. Real numbers, complex numbers,
  rational numbers, integers mod a prime are fields
- Ex. Integers, 2×2 matrices with real entries are not fields

Field

- Field: a set that has the operation of addition, multiplication, subtraction, and division by nonzero elements. Also, the associative, commutative, and distributive laws hold.
- Ex. Real numbers, complex numbers, rational numbers, integers mod a prime are fields
- Ex. Integers, 2×2 matrices with real entries are not fields
- Ex. GF(4) = $\{0, 1, \omega, \omega^2\}$
  - $0 + x = x$
  - $x + x = 0$
  - $1 \cdot x = x$
  - $\omega + 1 = \omega^2$

Field

- Field: a set that has the operation of addition, multiplication, subtraction, and division by nonzero elements. Also, the associative, commutative, and distributive laws hold.
- Ex. Real numbers, complex numbers,
  rational numbers, integers mod a prime are fields
- Ex. Integers, 2×2 matrices with real entries are not fields
- Ex. GF(4) = $\{0, 1, \omega, \omega^2\}$
  - $0 + x = x$
  - $x + x = 0$
  - $1 \cdot x = x$
  - $\omega + 1 = \omega^2$

- Addition and multiplication are commutative and associative, and the distributive law $x(y+z)=xy+xz$ holds for all x, y, z

Field

- Field: a set that has the operation of addition, multiplication, subtraction, and division by nonzero elements. Also, the associative, commutative, and distributive laws hold.
- Ex. Real numbers, complex numbers, rational numbers, integers mod a prime are fields
- Ex. Integers, 2×2 matrices with real entries are not fields
- Ex. GF(4) = $\{0, 1, \omega, \omega^2\}$
  - $0 + x = x$
  - $x + x = 0$
  - $1 \cdot x = x$
  - $\omega + 1 = \omega^2$

- Addition and multiplication are commutative and associative, and the distributive law $x(y+z)=xy+xz$ holds for all x, y, z
  $x^3 = 1$ for all nonzero elements

Galois Field

- Galois Field: A field with finite element, finite field

Galois Field

- Galois Field: A field with finite element, finite field
- For every power p^n of a prime, there is exactly one finite field with p^n elements, GF(p^n), and these are the only finite fields.

Galois Field

- ✧ Galois Field: A field with finite element, finite field
- ✧ For every power p^n of a prime, there is exactly one finite field with p^n elements, $GF(p^n)$, and these are the only finite fields.
- ✧ For $n > 1$, {integers (mod p^n)} do not form a field.
  - ✶ Ex. $p \cdot x \equiv 1 \pmod{p^n}$ does not have a solution

    (i.e. p does not have multiplicative inverse)

How to construct a GF(p^n)?

✧ Def: $Z_2[X]$: the set of polynomials whose coefficients are integers mod 2

How to construct a GF(p^n)?

- Def: $Z_2[X]$: the set of polynomials whose coefficients are integers mod 2
  - ex. 0, 1, $1+X^3+X^6$…

How to construct a GF(p^n)?

- Def: $Z_2[X]$: the set of polynomials whose coefficients are integers mod 2
  - ex. 0, 1, $1+X^3+X^6$…
  - add/subtract/multiply/divide/Euclidean Algorithm: process all coefficients mod 2

How to construct a GF(p^n)?

- Def: $Z_2[X]$: the set of polynomials whose coefficients are integers mod 2
  - ex. 0, 1, $1+X^3+X^6$…
  - add/subtract/multiply/divide/Euclidean Algorithm: process all coefficients mod 2
    - $(1+X^2+X^4) + (X+X^2) = 1+X+X^4$ bitwise XOR

How to construct a $GF(p^n)$?

- Def: $Z_2[X]$: the set of polynomials whose coefficients are integers mod 2
  - ex. 0, 1, $1+X^3+X^6$…
  - add/subtract/multiply/divide/Euclidean Algorithm: process all coefficients mod 2
    - $(1+X^2+X^4) + (X+X^2) = 1+X+X^4$ bitwise XOR
    - $(1+X+X^3)(1+X) = 1+X^2+X^3+X^4$

How to construct a GF(p^n)?

- Def: $Z_2[X]$: the set of polynomials whose coefficients are integers mod 2
  - ex. 0, 1, $1+X^3+X^6$…
  - add/subtract/multiply/divide/Euclidean Algorithm: process all coefficients mod 2
    - $(1+X^2+X^4) + (X+X^2) = 1+X+X^4$ bitwise XOR
    - $(1+X+X^3)(1+X) = 1+X^2+X^3+X^4$
    - $X^4+X^3+1 = (X^2+1)(X^2+X+1) + X$ long division

      can be written as

      $X^4+X^3+1 \equiv X \pmod{X^2+X+1}$

How to construct GF(2^n)?

- Define $Z_2[X]$ (mod X^2+X+1) to be {0, 1, X, X+1}

How to construct GF(2^n)?

- Define $Z_2[X]$ (mod X^2+X+1) to be {0, 1, X, X+1}
  - addition, subtraction, multiplication are done mod X^2+X+1

How to construct GF(2^n)?

- Define $Z_2[X]$ (mod X^2+X+1) to be {0, 1, X, X+1}
  - addition, subtraction, multiplication are done mod X^2+X+1
  - $f(X) \equiv g(X)$ (mod X^2+X+1)

How to construct GF(2^n)?

- Define $Z_2[X]$ (mod X^2+X+1) to be {0, 1, X, X+1}
  - addition, subtraction, multiplication are done mod X^2+X+1
  - $f(X) \equiv g(X)$ (mod X^2+X+1)
    - if f(X) and g(X) have the same remainder when divided by X^2+X+1

How to construct GF(2^n)?

- Define $Z_2[X]$ (mod X^2+X+1) to be {0, 1, X, X+1}
  - addition, subtraction, multiplication are done mod X^2+X+1
  - $f(X) \equiv g(X)$ (mod X^2+X+1)
    - if f(X) and g(X) have the same remainder when divided by X^2+X+1
    - or equivalently $\exists$ h(X) such that $f(X) - g(X) = (X^2+X+1)\, h(X)$

How to construct GF(2^n)?

- Define $Z_2[X]$ (mod X^2+X+1) to be $\{0, 1, X, X+1\}$
  - addition, subtraction, multiplication are done mod X^2+X+1
  - $f(X) \equiv g(X)$ (mod X^2+X+1)
    - if $f(X)$ and $g(X)$ have the same remainder when divided by X^2+X+1
    - or equivalently $\exists$ $h(X)$ such that $f(X) - g(X) = (X^2+X+1)\ h(X)$
    - ex. $X \cdot X = X^2 \equiv X+1$ (mod X^2+X+1)

How to construct GF(2^n)?

- Define $Z_2[X]$ (mod X^2+X+1) to be {0, 1, X, X+1}
  - addition, subtraction, multiplication are done mod X^2+X+1
  - $f(X) \equiv g(X) \pmod{X^2+X+1}$
    - if f(X) and g(X) have the same remainder when divided by X^2+X+1
    - or equivalently ∃ h(X) such that $f(X) - g(X) = (X^2+X+1)\, h(X)$
    - ex. $X \cdot X = X^2 \equiv X+1 \pmod{X^2+X+1}$
  - if we replace X by ω, we can get the same GF(4) as before

How to construct GF(2^n)?

- Define $Z_2[X]$ (mod X^2+X+1) to be {0, 1, X, X+1}
  - addition, subtraction, multiplication are done mod X^2+X+1
  - $f(X) \equiv g(X)$ (mod X^2+X+1)
    - if f(X) and g(X) have the same remainder when divided by X^2+X+1
    - or equivalently ∃ h(X) such that $f(X) - g(X) = (X^2+X+1)\ h(X)$
    - ex. $X \cdot X = X^2 \equiv X+1$ (mod X^2+X+1)
  - if we replace X by ω, we can get the same GF(4) as before
  - the modulus polynomial X^2+X+1 should be irreducible

How to construct GF(2^n)?

- Define $Z_2[X]$ (mod X^2+X+1) to be {0, 1, X, X+1}
  - addition, subtraction, multiplication are done mod X^2+X+1
  - $f(X) \equiv g(X)$ (mod X^2+X+1)
    - if f(X) and g(X) have the same remainder when divided by X^2+X+1
    - or equivalently ∃ h(X) such that $f(X) - g(X) = (X^2+X+1)\,h(X)$
    - ex. $X \cdot X = X^2 \equiv X+1$ (mod X^2+X+1)
  - if we replace X by ω, we can get the same GF(4) as before
  - the modulus polynomial X^2+X+1 should be irreducible

Irreducible: polynomial does not factor into polynomials of lower degree with mod 2 arithmetic

ex. X^2+1 is not irreducible since $X^2+1 = (X+1)(X+1)$

How to construct GF(p^n)?

- $Z_p[X]$ is the set of polynomials with coefficients mod p

How to construct GF(p^n)?

- $Z_p[X]$ is the set of polynomials with coefficients mod p
- Choose P(X) to be any one irreducible polynomial mod p of degree n (other irreducible P(X)'s would result to isomorphisms)

How to construct GF(p^n)?

- $Z_p[X]$ is the set of polynomials with coefficients mod p
- Choose P(X) to be any one irreducible polynomial mod p of degree n (other irreducible P(X)'s would result to isomorphisms)
- Let GF(p^n) be $Z_p[X]$ mod P(X)

How to construct GF(p^n)?

- $Z_p[X]$ is the set of polynomials with coefficients mod p
- Choose $P(X)$ to be any one irreducible polynomial mod p of degree n (other irreducible $P(X)$’s would result to isomorphisms)
- Let GF(p^n) be $Z_p[X]$ mod $P(X)$

- An element in $Z_p[X]$ mod $P(X)$ must be of the form

$$a_0 + a_1 X + \ldots + a_{n-1} X^{n-1}$$

each a_i are integers mod p, and have p choices, hence there are p^n possible elements in GF(p^n)

How to construct GF(p^n)?

- $Z_p[X]$ is the set of polynomials with coefficients mod p
- Choose P(X) to be any one irreducible polynomial mod p of degree n (other irreducible P(X)'s would result to isomorphisms)
- Let GF(p^n) be $Z_p[X]$ mod P(X)

- An element in $Z_p[X]$ mod P(X) must be of the form
$$a_0 + a_1 X + \ldots + a_{n-1} X^{n-1}$$
each a_i are integers mod p, and have p choices, hence there are p^n possible elements in GF(p^n)
- multiplicative inverse of any element in GF(p^n) can be found using extended Euclidean algorithm (over polynomial)

GF(2^8)

✧ AES (Rijndael) uses GF(2^8) with irreducible polynomial $X^8 + X^4 + X^3 + X + 1$

GF(2^8)

- AES (Rijndael) uses GF(2^8) with irreducible polynomial $X^8 + X^4 + X^3 + X + 1$
- each element is represented as
  $b_7 X^7 + b_6 X^6 + b_5 X^5 + b_4 X^4 + b_3 X^3 + b_2 X^2 + b_1 X + b_0$
  each b_i is either 0 or 1

GF(2^8)

- AES (Rijndael) uses GF(2^8) with irreducible polynomial $X^8 + X^4 + X^3 + X + 1$
- each element is represented as $b_7 X^7 + b_6 X^6 + b_5 X^5 + b_4 X^4 + b_3 X^3 + b_2 X^2 + b_1 X + b_0$ each b_i is either 0 or 1
- elements of GF(2^8) can be represented as 8-bit bytes $b_7b_6b_5b_4b_3b_2b_1b_0$

GF(2^8)

- AES (Rijndael) uses GF(2^8) with irreducible polynomial $X^8 + X^4 + X^3 + X + 1$
- each element is represented as
  $b_7 X^7 + b_6 X^6 + b_5 X^5 + b_4 X^4 + b_3 X^3 + b_2 X^2 + b_1 X + b_0$
  each b_i is either 0 or 1
- elements of GF(2^8) can be represented as 8-bit bytes
  $b_7b_6b_5b_4b_3b_2b_1b_0$
- mod 2 operations can be implemented by XOR in H/W

-
-

GF(p^n)

GF(p^n)

- ✧ Definition of generating polynomial g(X) is parallel to the generator in Z_p:
  - ✶ every element in GF(p^n) (except 0) can be expressed as a power of g(X)

GF(p^n)

- Definition of generating polynomial g(X) is parallel to the generator in Z_p:
  - every element in GF(p^n) (except 0) can be expressed as a power of g(X)
  - the smallest exponent k such that $g(X)^k \equiv 1$ is p^n -1

GF(p^n)

- Definition of generating polynomial g(X) is parallel to the generator in Z_p:
  - every element in GF(p^n) (except 0) can be expressed as a power of g(X)
  - the smallest exponent k such that $g(X)^k \equiv 1$ is p^n -1
- Discrete log problem in GF(p^n):
  - given h(X), find an integer k such that

$$h(X) \equiv g(X)^k \pmod{P(X)}$$

GF(p^n)

- Definition of generating polynomial g(X) is parallel to the generator in Z_p:
  - every element in GF(p^n) (except 0) can be expressed as a power of g(X)
  - the smallest exponent k such that $g(X)^k \equiv 1$ is p^n -1
- Discrete log problem in GF(p^n):
  - given h(X), find an integer k such that

    $$h(X) \equiv g(X)^k \ (\text{mod } P(X))$$
  - believed to be very hard in most situations

Recursive GCD

```
int gcd(int p, int q) // assume p >= q
{
    int ans;

    if (p % q == 0)
        ans = q;
    else
        ans = gcd(q, p % q);

    return ans;
}
```

Recursive GCD

```
int gcd(int p, int q) // assume p >= q
{
    int ans;

    if (p % q == 0)
        ans = q;
    else
        ans = gcd(q, p % q);

    return ans;
}
```

```
int gcd(int p, int q)
{
    int r = p%q;
    if (r == 0)
        return q;
    return gcd(q, r);
}
```

Recursive Extended GCD

- Given $a>b\geq 0$, find $g=GCD(a,b)$ and x, y s.t. $a\,x + b\,y = g$ where $|x|\leq b+1$ and $|y|\leq a+1$

Recursive Extended GCD

- Given a>b≥0, find g=GCD(a,b) and x, y s.t. a x + b y = g where |x|≤b+1 and |y|≤a+1, if g = 1, then x is a's inverse mod b

Recursive Extended GCD

- Given $a>b\geq 0$, find $g=GCD(a,b)$ and x, y s.t. $a\,x + b\,y = g$ where $|x|\leq b+1$ and $|y|\leq a+1$, if $g = 1$, then x is a's inverse mod b
- Let $a = q\,b + r$, $b>r\geq 0 \Rightarrow (q\,b + r)\,x + b\,y = g$

$$\Rightarrow b\,(q\,x + y) + r\,x = g$$

$$\Rightarrow b\,y' + r\,x = g, \text{ where } y' = q\,x + y$$

Recursive Extended GCD

- Given $a>b\geq 0$, find $g=GCD(a,b)$ and x, y s.t. $a\,x + b\,y = g$ where $|x|\leq b+1$ and $|y|\leq a+1$, if $g = 1$, then x is a's inverse mod b
- Let $a = q\,b + r$, $b>r\geq 0 \Rightarrow (q\,b + r)\,x + b\,y = g$
  $\Rightarrow b\,(q\,x + y) + r\,x = g$
  $\Rightarrow b\,y' + r\,x = g$, where $y' = q\,x + y$
- This means that if we can find y' and x satisfying $b\,y' + (a\%b)\,x = g$ then x and $\mathbf{y} = y' - q\,x = \mathbf{y' - (a/b)\,x}$ satisfies $a\,x + b\,y = g$
  Note that in this way r will eventually be 0

Recursive Extended GCD

- Given $a>b\geq 0$, find g=GCD(a,b) and x, y s.t. $a\,x + b\,y = g$ where $|x|\leq b+1$ and $|y|\leq a+1$, if $g = 1$, then x is a's inverse mod b
- Let $a = q\,b + r$, $b>r\geq 0 \Rightarrow (q\,b + r)\,x + b\,y = g$
  $\Rightarrow b\,(q\,x + y) + r\,x = g$
  $\Rightarrow b\,y' + r\,x = g$, where $y' = q\,x + y$
- This means that if we can find y' and x satisfying $b\,y' + (a\%b)\,x = g$ then x and **y = $y' - q\,x$ = $y' -$ (a/b) x** satisfies $a\,x + b\,y = g$
  Note that in this way r will eventually be 0

```
void extgcd(int a, int b, int *g, int *x, int *y) { // a > b >=0
    if (b == 0)
        *g = a, *x = 1, *y = 0;
    else {
        extgcd(b, a%b, g, y, x);
        *y = *y - (a/b)*(*x);
    }
}
```

$x^{|G|} = 1$

✧ If G is a finite group, $\forall x \in G$, $\mathbf{x^{|G|} = 1}$

$x^{|G|} = 1$

✧ If G is a finite group, $\forall x \in G$, $\mathbf{x^{|G|} = 1}$

1. Lagrange Thm: if H is a subgroup of G then $|G| = k\,|H|$

$x^{|G|} = 1$

- If G is a finite group, $\forall x \in G$, $\mathbf{x^{|G|} = 1}$

1. Lagrange Thm: if H is a subgroup of G then $|G| = k\,|H|$
2. $\forall x \in G$, x generates a cyclic subgroup $H = \{x, x^2, \ldots, x^{ord(x)}\}$, $|H|=ord(x)$, where $x^{ord(x)} = 1$ is the identity

$x^{|G|} = 1$

✧ If G is a finite group, $\forall x \in G$, **$x^{|G|} = 1$**

1. Lagrange Thm: if H is a subgroup of G then $|G| = k\,|H|$
2. $\forall x \in G$, x generates a cyclic subgroup $H = \{x, x^2, \ldots, x^{ord(x)}\}$, $|H| = ord(x)$, where $x^{ord(x)} = 1$ is the identity

1 and 2 imply that $\forall x \in G$, $x^{|G|} = x^{k|H|} = (x^{ord(x)})^k = 1$

$x^{|G|} = 1$

✧ If G is a finite group, $\forall x \in G$, $x^{|G|} = 1$

1. Lagrange Thm: if H is a subgroup of G then $|G| = k\,|H|$
2. $\forall x \in G$, x generates a cyclic subgroup $H = \{x, x^2, \ldots, x^{ord(x)}\}$, $|H|=ord(x)$, where $x^{ord(x)} = 1$ is the identity

1 and 2 imply that $\forall x \in G$, $x^{|G|} = x^{k|H|} = (x^{ord(x)})^k = 1$

Note: $\forall x \in G$, $\exists!\ ord(x) \in [1,|G|]$ such that $x^{ord(x)} = 1$

$$\forall x \in G,\ \exists!\ \mathrm{ord}(x) \in [1,|G|] \text{ such that } x^{\mathrm{ord}(x)} = 1$$

Assume that there does not exist such an integer **ord(x)** in $[1,|G|]$, i.e. $1 \notin S=\{x, x^2, x^3, \ldots, x^{|G|}\}$

-
-

$\forall x \in G$, $\exists!$ ord(x)$\in[1,|G|]$ such that $x^{\mathrm{ord}(x)} = 1$

Assume that there does not exist such an integer **ord(x)** in $[1,|G|]$, i.e. $1 \notin S=\{x, x^2, x^3, \ldots, x^{|G|}\}$

Consider the following 2 cases:

-
-

$\forall x \in G, \exists!\ \mathrm{ord}(x) \in [1,|G|]$ such that $x^{\mathrm{ord}(x)} = 1$

Assume that there does not exist such an integer **ord(x)** in $[1,|G|]$, i.e. $1 \notin S=\{x, x^2, x^3, \ldots, x^{|G|}\}$

Consider the following 2 cases:

1. if any two elements in S are equal, i.e. there exist distinct i, j, such that $x^i = x^j$, then $\mathbf{x^{j-i} = 1}$ and $1 \leq j-i \leq |G|$

-
-

$\forall x \in G$, $\exists!$ ord(x)$\in[1,|G|]$ such that $x^{\mathrm{ord}(x)} = 1$

Assume that there does not exist such an integer **ord(x)** in $[1,|G|]$, i.e. $1 \notin S=\{x, x^2, x^3, \ldots, x^{|G|}\}$

Consider the following 2 cases:

1. if any two elements in S are equal, i.e. there exist distinct i, j, such that $x^i = x^j$, then $\mathbf{x^{j-i} = 1}$ and $1\leq j-i\leq|G|$

2. if all elements are distinct, consider $x^{|G|+1} \in G$ (closeness), Pidgin hole principle $\Rightarrow$ $\exists$ i, $1\leq i\leq|G|$, s.t. $x^i = x^{|G|+1}$, then $\mathbf{x^{|G|+1-i} = 1}$ and $1\leq|G|+1-i\leq|G|$

$\forall x \in G, \exists!\ ord(x) \in [1,|G|]$ such that $x^{ord(x)} = 1$

Assume that there does not exist such an integer **ord(x)** in $[1,|G|]$, i.e. $1 \notin S=\{x, x^2, x^3, \ldots, x^{|G|}\}$

Consider the following 2 cases:

1. if any two elements in S are equal, i.e. there exist distinct i, j, such that $x^i = x^j$, then $\mathbf{x^{j-i} = 1}$ and $1 \le j-i \le |G|$
2. if all elements are distinct, consider $x^{|G|+1} \in G$ (closeness), Pidgin hole principle $\Rightarrow$ $\exists$ i, $1 \le i \le |G|$, s.t. $x^i = x^{|G|+1}$, then $\mathbf{x^{|G|+1-i} = 1}$ and $1 \le |G|+1-i \le |G|$

Both imply the result that $1 \le ord(x) \le |G|$

Lagrange Theorem

if H is a subgroup of a finite group G then **|H| divides |G|**

Lagrange Theorem

if H is a subgroup of a finite group G then **|H| divides |G|**

useful definition and lemmas:

➊ let g ∈ G, define the *left coset* **gH** of the subgroup H as:

Lagrange Theorem

if H is a subgroup of a finite group G then **|H| divides |G|**

useful definition and lemmas:

❶ let g ∈ G, define the *left coset* **gH** of the subgroup H as:

$$\mathbf{gH} = \{ g\,x \mid x \in H \}$$

Lagrange Theorem

if H is a subgroup of a finite group G then **|H| divides |G|**

useful definition and lemmas:

➊ let $g \in G$, define the *left coset* **gH** of the subgroup H as:

$$gH = \{ g\,x \mid x \in H \}$$

➋ $\forall\ g \in G,\ |\, gH \,| = |\, H \,|$

Lagrange Theorem

if H is a subgroup of a finite group G then **|H| divides |G|**

useful definition and lemmas:

➊ let $g \in G$, define the *left coset* **gH** of the subgroup H as:

$$gH = \{ g\,x \mid x \in H \}$$

➋ $\forall\, g \in G,\ |\, gH \,| = |\, H \,|$

➌ $\forall\, g_1, g_2 \in G,\ g_1 \neq g_2$, either $g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

Lagrange Theorem

if H is a subgroup of a finite group G then **|H| divides |G|**

useful definition and lemmas:

➊ let $g \in G$, define the *left coset* **gH** of the subgroup H as:

$$\mathbf{gH} = \{ g\,x \mid x \in H \}$$

➋ $\forall\ g \in G, \mid gH \mid = \mid H \mid$

➌ $\forall\ g_1, g_2 \in G, g_1 \neq g_2$, either $g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

➍ $G = \bigcup_{g \in G} gH$

Lagrange Theorem

if H is a subgroup of a finite group G then **|H| divides |G|**

useful definition and lemmas:

❶ let $g \in G$, define the *left coset* **gH** of the subgroup H as:

$$gH = \{ g\,x \mid x \in H \}$$

❷ $\forall\, g \in G, \mid gH \mid = \mid H \mid$

❸ $\forall\, g_1, g_2 \in G, g_1 \neq g_2$, either $g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

❹ $G = \bigcup_{g \in G} gH \qquad \because\ 1 \in H \Rightarrow g \in gH$

Lagrange Theorem

if H is a subgroup of a finite group G then **|H| divides |G|**

useful definition and lemmas:

➊ let g ∈ G, define the *left coset* **gH** of the subgroup H as:

$$gH = \{ g\,x \mid x \in H \}$$

➋ $\forall\, g \in G, \ | gH | = | H |$

➌ $\forall\, g_1, g_2 \in G, g_1 \neq g_2$, either $g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

➍ $G = \bigcup_{g\in G} gH \qquad \because\ 1 \in H \Rightarrow g \in gH$

pf:

Lagrange Theorem

if H is a subgroup of a finite group G then **|H| divides |G|**

useful definition and lemmas:

❶ let $g \in G$, define the *left coset* **gH** of the subgroup H as:

$$gH = \{ g x \mid x \in H \}$$

❷ $\forall\ g \in G, |gH| = |H|$

❸ $\forall\ g_1, g_2 \in G, g_1 \neq g_2$, either $g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

❹ $G = \bigcup_{g \in G} gH \quad \because\ 1 \in H \Rightarrow g \in gH$

pf: $G \underset{❹}{=} \bigcup_{g \in G} gH = H \cup g_1H \cup g_2H \cup \ldots \cup g_{k-1}H$

Lagrange Theorem

if H is a subgroup of a finite group G then **|H| divides |G|**

useful definition and lemmas:

❶ let $g \in G$, define the *left coset* **gH** of the subgroup H as:

$$\mathbf{gH} = \{\, g\,x \mid x \in H \,\}$$

❷ $\forall\, g \in G,\ |\, gH \,| = |\, H \,|$

❸ $\forall\, g_1, g_2 \in G,\ g_1 \neq g_2$, either $g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

❹ $G = \bigcup_{g \in G} gH \qquad \because\ 1 \in H \Rightarrow g \in gH$

pf: $G \underset{\text{❹}}{=} \bigcup_{g \in G} gH \underset{\text{❸}}{=} H \cup g_1H \cup g_2H \cup \ldots \cup g_{k-1}H$

Lagrange Theorem

if H is a subgroup of a finite group G then **|H| divides |G|**

useful definition and lemmas:

❶ let $g \in G$, define the *left coset* **gH** of the subgroup H as:

$$\mathbf{gH} = \{\, g\,x \mid x \in H \,\}$$

❷ $\forall\, g \in G,\ |\, gH \,| = |\, H \,|$

❸ $\forall\, g_1, g_2 \in G,\ g_1 \neq g_2$, either $g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

❹ $G = \bigcup_{g \in G} gH \qquad \because\ 1 \in H \Rightarrow g \in gH$

pf: $G \underset{\text{④}}{=} \bigcup_{g \in G} gH \underset{\text{③}}{=} H \cup g_1H \cup g_2H \cup \ldots \cup g_{k-1}H$

$$\underset{\text{②}}{\Rightarrow}\ \mathbf{|\, G \,| = k \,|\, H \,|}$$

•

•

$\forall\, g \in G,\ |\, gH \,| = |\, H \,|$

✧ define the mapping function f: $H \rightarrow gH$ as $f(x) = g\, x$

$\forall\, g \in G,\ |\, gH \,| = |\, H \,|$

- ✧ define the mapping function f: H → gH as f(x) = g x
- ✧ prove that f() is a bijection

$\forall\, g \in G,\ |\, gH \,| = |\, H \,|$

- ✧ define the mapping function f: H → gH as $f(x) = g\,x$
- ✧ prove that f() is a bijection

1. f() is 1-1

$\forall\, g \in G, \mid gH \mid = \mid H \mid$

✧ define the mapping function f: $H \rightarrow gH$ as $f(x) = g\,x$

✧ prove that f() is a bijection

1. f() is 1-1

   i.e. if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

$\forall\ g \in G,\ |\ gH\ | = |\ H\ |$

- define the mapping function f: $H \to gH$ as $f(x) = g\,x$
- prove that f() is a bijection

1. f() is 1-1

   i.e. if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

   contrapositive statement:

$\forall\, g \in G,\ |\, gH \,| = |\, H \,|$

- ✧ define the mapping function f: H → gH as $f(x) = g\,x$
- ✧ prove that f() is a bijection

1. f() is 1-1

   i.e. if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

   contrapositive statement: if $f(x_1) = f(x_2)$ then $x_1 = x_2$

$\forall\, g \in G, |\, gH \,| = |\, H \,|$

- ✧ define the mapping function f: $H \to gH$ as $f(x) = g\,x$
- ✧ prove that f() is a bijection

1. f() is 1-1

i.e. if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

contrapositive statement: if $f(x_1) = f(x_2)$ then $x_1 = x_2$

$f(x_1) = f(x_2)$

$\forall\ g \in G, |\, gH \,| = |\, H \,|$

- ✧ define the mapping function $f: H \rightarrow gH$ as $f(x) = g\,x$
- ✧ prove that f() is a bijection

1. f() is 1-1

   i.e. if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

   contrapositive statement: if $f(x_1) = f(x_2)$ then $x_1 = x_2$

   $f(x_1) = f(x_2) \;\; \Rightarrow \;\; g\,x_1 = g\,x_2$

$\forall\, g \in G,\ |\, gH \,| = |\, H \,|$

- define the mapping function f: H $\rightarrow$ gH as $f(x) = g\,x$
- prove that f() is a bijection

1. f() is 1-1

i.e. if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

contrapositive statement: if $f(x_1) = f(x_2)$ then $x_1 = x_2$

$$f(x_1) = f(x_2) \;\Rightarrow\; g\,x_1 = g\,x_2 \;\Rightarrow\; g^{-1}\,g\,x_1 = g^{-1}\,g\,x_2$$

$\forall\, g \in G,\ |\, gH \,| = |\, H \,|$

- ✧ define the mapping function $f: H \rightarrow gH$ as $f(x) = g\,x$
- ✧ prove that $f()$ is a bijection

1. $f()$ is 1-1

i.e. if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

contrapositive statement: if $f(x_1) = f(x_2)$ then $x_1 = x_2$

$$f(x_1) = f(x_2) \;\Rightarrow\; g\,x_1 = g\,x_2 \;\Rightarrow\; g^{-1}\,g\,x_1 = g^{-1}\,g\,x_2 \;\Rightarrow\; x_1 = x_2$$

$\forall\, g \in G, |\, gH \,| = |\, H \,|$

- ✧ define the mapping function f: H → gH as $f(x) = g\,x$
- ✧ prove that f() is a bijection

1. f() is 1-1

   i.e. if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

   contrapositive statement: if $f(x_1) = f(x_2)$ then $x_1 = x_2$

   $$f(x_1) = f(x_2) \;\Rightarrow\; g\,x_1 = g\,x_2 \;\Rightarrow\; g^{-1}\,g\,x_1 = g^{-1}\,g\,x_2 \;\Rightarrow\; x_1 = x_2$$

2. f() is onto

$\forall\ g \in G, |\ gH\ | = |\ H\ |$

- ✧ define the mapping function f: H → gH as $f(x) = g\ x$
- ✧ prove that f() is a bijection

1. f() is 1-1

   i.e. if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

   contrapositive statement: if $f(x_1) = f(x_2)$ then $x_1 = x_2$

   $f(x_1) = f(x_2) \Rightarrow g\ x_1 = g\ x_2 \Rightarrow g^{-1}\ g\ x_1 = g^{-1}\ g\ x_2 \Rightarrow x_1 = x_2$

2. f() is onto

   $\forall\ y \in gH,$

$\forall\, g \in G, \mid gH \mid = \mid H \mid$

- define the mapping function $f: H \rightarrow gH$ as $f(x) = g\,x$
- prove that f() is a bijection

1. f() is 1-1

i.e. if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

contrapositive statement: if $f(x_1) = f(x_2)$ then $x_1 = x_2$

$$f(x_1) = f(x_2) \;\Rightarrow\; g\,x_1 = g\,x_2 \;\Rightarrow\; g^{-1}\,g\,x_1 = g^{-1}\,g\,x_2 \;\Rightarrow\; x_1 = x_2$$

2. f() is onto

$\forall\, y \in gH, \exists\, h \in H, y = gh$

:

$\forall\ g \in G, |\ gH\ | = |\ H\ |$

- ✧ define the mapping function f: $H \rightarrow gH$ as $f(x) = g\ x$
- ✧ prove that f() is a bijection

1. f() is 1-1

   i.e. if $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$

   contrapositive statement: if $f(x_1) = f(x_2)$ then $x_1 = x_2$

   $f(x_1) = f(x_2) \quad \Rightarrow \quad g\ x_1 = g\ x_2 \quad \Rightarrow \quad g^{-1}\ g\ x_1 = g^{-1}\ g\ x_2 \quad \Rightarrow \quad x_1 = x_2$

2. f() is onto

   $\forall\ y \in gH, \exists\ h \in H, y = gh \quad \Rightarrow \quad h = g^{-1}\ y$

-
-

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

Lemma: $\forall\, g_1, g_2 \in G, g_1 \neq g_2 , g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$

-
-

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

<u>Lemma:</u> $\forall\, g_1, g_2 \in G,\ g_1 \neq g_2\ ,\ g_1H = g_2H \iff g_1^{-1}g_2 \in H$

$(\Rightarrow)$ $\quad 1 \in H \Rightarrow g_2 \in g_2H$

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

Lemma: $\forall\ g_1, g_2 \in G,\ g_1 \neq g_2\ ,\ g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$

$(\Rightarrow)\quad 1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$

•

•

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

Lemma: $\forall\ g_1, g_2 \in G, g_1 \neq g_2 , g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$

$(\Rightarrow)$ $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists\ h \in H, g_2 = g_1h$

-
-

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

$\boxed{\underline{\text{Lemma:}}\ \forall\, g_1, g_2 \in G,\ g_1 \neq g_2\,,\ g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H}$

$(\Rightarrow)$ $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists\, h \in H,\ g_2 = g_1h$

$\Rightarrow g_1^{-1}g_2 = h \in H$

-
-

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

Lemma: $\forall\, g_1, g_2 \in G,\ g_1 \neq g_2,\ g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$

$(\Rightarrow)$ $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists\, h \in H,\ g_2 = g_1h$

$\Rightarrow g_1^{-1}g_2 = h \in H$

$(\Leftarrow)$ let $h = g_1^{-1}g_2 \in H$

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

<u>Lemma</u>: $\forall\ g_1, g_2 \in G, g_1 \neq g_2\ , g_1H = g_2H \iff g_1^{-1}g_2 \in H$

$(\Rightarrow)$ $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists\ h \in H, g_2 = g_1h$

$\Rightarrow g_1^{-1}g_2 = h \in H$

$(\Leftarrow)$ let $h = g_1^{-1}g_2 \in H$

$\forall x \in g_1H, \exists h_1 \in H, x = g_1h_1$

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

$\boxed{\underline{\text{Lemma}}\text{: } \forall\, g_1, g_2 \in G,\ g_1 \neq g_2,\ g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H}$

$(\Rightarrow)$ $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists\, h \in H,\ g_2 = g_1h$

$\Rightarrow g_1^{-1}g_2 = h \in H$

$(\Leftarrow)$ let $h = g_1^{-1}g_2 \in H$

$\forall x \in g_1H, \exists h_1 \in H, x = g_1h_1 = (g_2h^{-1})\, h_1 = g_2(h^{-1}h_1) \in g_2H$

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

Lemma: $\forall\, g_1, g_2 \in G, g_1 \neq g_2, g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$

$(\Rightarrow)$ $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists\, h \in H, g_2 = g_1h$

$\Rightarrow g_1^{-1}g_2 = h \in H$

$(\Leftarrow)$ let $h = g_1^{-1}g_2 \in H$

$\forall x \in g_1H, \exists h_1 \in H, x = g_1h_1 = (g_2h^{-1})\, h_1 = g_2(h^{-1}h_1) \in g_2H$

$\forall x \in g_2H, \exists h_2 \in H, x = g_2h_2$

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

$\boxed{\underline{\text{Lemma}}\text{:}\ \forall\, g_1, g_2 \in G,\ g_1 \neq g_2,\ g_1H = g_2H \iff g_1^{-1}g_2 \in H}$

(⇒) $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists\, h \in H,\ g_2 = g_1h$

$\Rightarrow g_1^{-1}g_2 = h \in H$

(⇐) let $h = g_1^{-1}g_2 \in H$

$\forall x \in g_1H,\ \exists h_1 \in H,\ x = g_1h_1 = (g_2h^{-1})\, h_1 = g_2(h^{-1}h_1) \in g_2H$

$\forall x \in g_2H,\ \exists h_2 \in H,\ x = g_2h_2 = (g_1h)\, h_2 = g_1(hh_2) \in g_1H$

-
-

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

Lemma: $\forall\, g_1, g_2 \in G, g_1 \neq g_2 , g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$

$(\Rightarrow)$ $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists\, h \in H, g_2 = g_1h$

$\Rightarrow g_1^{-1}g_2 = h \in H$

$(\Leftarrow)$ let $h = g_1^{-1}g_2 \in H$

$\forall x \in g_1H, \exists h_1 \in H, x = g_1h_1 = (g_2h^{-1})\, h_1 = g_2(h^{-1}h_1) \in g_2H$

$\forall x \in g_2H, \exists h_2 \in H, x = g_2h_2 = (g_1h)\, h_2 = g_1(hh_2) \in g_1H$

pf: let $c \in g_1H \cap g_2H \neq \phi$

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

<u>Lemma</u>: $\forall\ g_1, g_2 \in G, g_1 \neq g_2\ , g_1H = g_2H \iff g_1^{-1}g_2 \in H$

$(\Rightarrow)$ $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists\ h \in H, g_2 = g_1h$

$\Rightarrow g_1^{-1}g_2 = h \in H$

$(\Leftarrow)$ let $h = g_1^{-1}g_2 \in H$

$\forall x \in g_1H, \exists h_1 \in H, x = g_1h_1 = (g_2h^{-1})\ h_1 = g_2(h^{-1}h_1) \in g_2H$

$\forall x \in g_2H, \exists h_2 \in H, x = g_2h_2 = (g_1h)\ h_2 = g_1(hh_2) \in g_1H$

<u>pf:</u> let $c \in g_1H \cap g_2H \neq \phi$

$\exists h_1 \in H, c = g_1h_1$

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

<u>Lemma</u>: $\forall\ g_1, g_2 \in G, g_1 \neq g_2 , g_1H = g_2H \iff g_1^{-1}g_2 \in H$

(⇒) $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists\ h \in H, g_2 = g_1h$

$\Rightarrow g_1^{-1}g_2 = h \in H$

(⇐) let $h = g_1^{-1}g_2 \in H$

$\forall x \in g_1H, \exists h_1 \in H, x = g_1h_1 = (g_2h^{-1})\ h_1 = g_2(h^{-1}h_1) \in g_2H$

$\forall x \in g_2H, \exists h_2 \in H, x = g_2h_2 = (g_1h)\ h_2 = g_1(hh_2) \in g_1H$

<u>pf:</u> let $c \in g_1H \cap g_2H \neq \phi$

$\exists h_1 \in H, c = g_1h_1$ $\exists h_2 \in H, c = g_2h_2$

-
-

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

Lemma: $\forall\ g_1, g_2 \in G, g_1 \neq g_2\ , g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$

(⇒) $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists\ h \in H, g_2 = g_1h$

$\Rightarrow g_1^{-1}g_2 = h \in H$

(⇐) let $h = g_1^{-1}g_2 \in H$

$\forall x \in g_1H, \exists h_1 \in H, x = g_1h_1 = (g_2h^{-1})\ h_1 = g_2(h^{-1}h_1) \in g_2H$

$\forall x \in g_2H, \exists h_2 \in H, x = g_2h_2 = (g_1h)\ h_2 = g_1(hh_2) \in g_1H$

pf: let $c \in g_1H \cap g_2H \neq \phi$

$\exists h_1 \in H, c = g_1h_1$ $\exists h_2 \in H, c = g_2h_2$

$\Rightarrow c = g_1h_1 = g_2h_2$

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

Lemma: $\forall\ g_1, g_2 \in G,\ g_1 \neq g_2,\ g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$

(⇒) $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists\ h \in H,\ g_2 = g_1h$

$\Rightarrow g_1^{-1}g_2 = h \in H$

(⇐) let $h = g_1^{-1}g_2 \in H$

$\forall x \in g_1H,\ \exists h_1 \in H,\ x = g_1h_1 = (g_2h^{-1})\,h_1 = g_2(h^{-1}h_1) \in g_2H$

$\forall x \in g_2H,\ \exists h_2 \in H,\ x = g_2h_2 = (g_1h)\,h_2 = g_1(hh_2) \in g_1H$

pf: let $c \in g_1H \cap g_2H \neq \phi$

$\exists h_1 \in H,\ c = g_1h_1$ $\exists h_2 \in H,\ c = g_2h_2$

$\Rightarrow c = g_1h_1 = g_2h_2 \Rightarrow h_1h_2^{-1} = g_1^{-1}g_2 \in H$

$g_1H = g_2H$ or $g_1H \cap g_2H = \phi$

Lemma: $\forall g_1, g_2 \in G, g_1 \neq g_2, g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$

($\Rightarrow$) $1 \in H \Rightarrow g_2 \in g_2H \Rightarrow g_2 \in g_1H$ i.e. $\exists h \in H, g_2 = g_1h$

$\Rightarrow g_1^{-1}g_2 = h \in H$

($\Leftarrow$) let $h = g_1^{-1}g_2 \in H$

$\forall x \in g_1H, \exists h_1 \in H, x = g_1h_1 = (g_2h^{-1})\, h_1 = g_2(h^{-1}h_1) \in g_2H$

$\forall x \in g_2H, \exists h_2 \in H, x = g_2h_2 = (g_1h)\, h_2 = g_1(hh_2) \in g_1H$

pf: let $c \in g_1H \cap g_2H \neq \phi$

$\exists h_1 \in H, c = g_1h_1$ $\exists h_2 \in H, c = g_2h_2$

$\Rightarrow c = g_1h_1 = g_2h_2 \Rightarrow h_1h_2^{-1} = g_1^{-1}g_2 \in H \Rightarrow g_1H = g_2H$