Modular arithmetic (模運算)

- Reading assignments: Ch4: 4.1, 4.3, 4.4, 4.6

- Exercise:
  - 4.1: 17, 42, 43, 51, 52.
  - 4.3: 32, 34, 36, 37, 38, 39.
  - 4.4: 11, 13, 21, 34.
  - 4.6: 28.
  - p. 326: 28.

Definition. Given two integers a and b, and a positive integer m, we say that a is congruent to b modulo m if $m \mid (a-b)$.

Notation: $a \equiv b \pmod{m}$. ($\rightarrow$ a 同餘 b 模 m)

Proposition. Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$. The following two congruences hold.

- $a \equiv b \pmod{m}, c \equiv d \pmod{m} \implies (a+c) \equiv (b+d) \pmod{m}$.
- $a \equiv b \pmod{m}, c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$.

Proof: [$a \equiv b \pmod{m}, c \equiv d \pmod{m} \implies (a+c) \equiv (b+d) \pmod{m}$]

- By definition, $m \mid (a-b)$ and $m \mid (c-d)$, which means that

$$(a-b) = k_1 m \text{ and } (c-d) = k_2 m$$

  for some integers k_1 and k_2.

- We have that

$$(a+c)-(b+d) = (a-b)+(c-d) = (k_1+k_2)m,$$

  which means that $m \mid ((a+c)-(b+d))$. ∎

Proof: [$a \equiv b \pmod{m}, c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$]

- By definition, $m \mid (a-b)$ and $m \mid (c-d)$, which means that

$$(a-b) = k_1 m \text{ and } (c-d) = k_2 m$$

  for some integers k_1 and k_2.

- We have that $a = b + k_1 m$ and $c = d + k_2 m$, and thus

$$ac = bd + m \cdot (k_1 c + k_2 b + k_1 k_2 m),$$

  which means that $m \mid (ac - bd)$. ∎

RSA cryptography system

Ronald Rivest | Adi Shamir | Leonard Adleman (1976)

Alice wants to send a message to Bob via a communication channel (usually unsafe). Can Alice "properly manipulate" (encrypt) the massage, with Bob's help, so that "only" Bob can retrieve the "original message" from the encrypted one?

RSA cryptography system

Ronald Rivest | Adi Shamir | Leonard Adleman (1976)

Alice wants to send a message to Bob via a communication channel (usually unsafe). Can Alice "properly manipulate" (encrypt) the massage, with Bob's help, so that "only" Bob can retrieve the "original message" from the encrypted one?

Preprocessing (by Bob)

1. Choose two (big) prime numbers p & q. Let $n = p \cdot q$, $r = (p-1) \cdot (q-1)$.

2. Choose a pair of numbers e and d such that $d \cdot e \equiv 1 \pmod{r}$.

    - e: the encryption key

    - d: the decryption key

Then, Bob announces (n, e) in public, and keeps p, q, r, d private.

Alice encrypts her message m as c, and sends c via a public channel to Bob.

(Assume that $m < n$.)

$$\text{Alice} \quad \xrightarrow{c} \quad \text{Bob}$$

$$c \equiv m^e \pmod{n} \qquad\qquad c^d \equiv m \pmod{n}$$

Q0: How do we find large primes?

Q1: Given r, how do we find e and d such that $d \cdot e \equiv 1 \pmod{r}$?

→ We can choose e so that $\gcd(r, e) = 1$, then d is guaranteed to exist.

Q2: For any $m < n$, why $(m^e)^d \equiv m \pmod{n}$?

Q3: Is the decryption "easy"?

→ if we have d, then we know the secret. (we need d)

→ we can solve $d \cdot e \equiv 1 \pmod{r}$ for d. (we need r)

→ if we know p and q, then we have r. (we need to factorize n)

Theorem (Bézout's identity). For $a, b \in \mathbb{N}$, if $\gcd(a, b) = d$, then $\exists x, y \in \mathbb{Z}$ such that $ax + by = d$.

Proof:

(Well-ordering axiom: every nonempty subset of $\mathbb{N}$ has a smallest element.)

- Let $S = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}$.
- S is nonempty (why?) so there exists a smallest element $d^* = ax^* + by^*$.
- claim: $d^* = d$, namely
  - d^* is a common divisor of a and b.

    $\rightarrow d^* \mid a$, $d^* \mid b$.
  - Every common divisor c of a and b divides d^*.

    $\rightarrow \forall c\ (c \mid a) \wedge (c \mid b) \implies c \mid d^*$

- $d^* \mid a$, $d^* \mid b$ (direct proof)
  - Let $a = k \cdot d^* + r$, $0 \le r < d^*$. $\rightarrow r = a - kd^* = a \cdot (1 - kx^*) - b \cdot ky^*$
  - $r = 0$ since otherwise $r \in S$ and is smaller than d^*.
- $\forall c\ (c \mid a) \wedge (c \mid b) \implies c \mid d^*$ (direct proof)
  - Let $a = ck_1, b = ck_2$. We have $d^* = c(k_1x^* + k_2y^*)$, which implies $c \mid d^*$. ∎

Q. We know that there "exist" x and y such that $ax + by = d$, where

$d = \gcd(a, b)$, but how do we find x and y?

e.g., a = 18, b = 32, d = ?

Euclidean algorithm		backward substitution
32 = 1*18 + 14	→	14 = 32 - 1*18
18 = 1*14 + 4	→	4 = 18 - 1*14
14 = 3*4 + 2	→	2 = 14 - 3*4 = 14 - 3*(18 - 1*14)
		= -3*18 + 4*14 = -3*18 + 4 * (32 - 1*18)
		= 4*32 - 7*18
4 = 2*2 + 0		

Q2: For any $m < n$, why $(m^e)^d \equiv m \pmod{n}$?

Recall: $c \equiv m^e \pmod{n}, ed \equiv 1 \pmod{r}, r = (p-1)(q-1)$

$\rightarrow$ $c^d \equiv m^{ed} \equiv m^{1+kr} \equiv m \cdot m^{kr} \pmod{n}$ for some integer k

$\rightarrow$ claim: $m \cdot m^{kr} \equiv m \pmod{n}$ or (more strictly) $m^{kr} \equiv 1 \pmod{n}$

Theorem (Fermat's little theorem). Let p be a prime. Then

$$\forall a \in \mathbb{Z},\ \gcd(a, p) = 1 \implies a^{p-1} \equiv 1 \pmod{p}.$$

(Proposed by Fermat in 1636, formally proved by Euler in 1736)

Proof.

- Consider the numbers $1,2,3,\ldots,p-1$. We multiply each number by a.
- For $i,j \in [p-1], i \neq j \implies ai \not\equiv aj \pmod{p}$.
  - Otherwise, $p \mid a(i-j)$.
  - $\gcd(a,p)=1 \implies p \mid (i-j)$.
  - However, $i<p$ and $j<p \implies |i-j|<p \implies p \nmid |i-j|$. $(\Rightarrow\!\Leftarrow)$
- Thus, $1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}$.

  $\to p \mid 1 \cdot 2 \cdot \ldots \cdot (p-1) \cdot (a^{p-1}-1)$
- Since p is prime, $1 \cdot 2 \cdot \ldots \cdot (p-1)$ has no factor p.
- Thus, $p \mid a^{p-1}-1$, which implies $a^{p-1} \equiv 1 \pmod{p}$. $\blacksquare$

Q2: For any $m < n$, why $(m^e)^d \equiv m \pmod{n}$?

Recall: $c \equiv m^e \pmod{n}, ed \equiv 1 \pmod{r}, r = (p-1)(q-1)$

$\rightarrow c^d \equiv m^{ed} \equiv m^{1+kr} \equiv m \cdot m^{kr} \pmod{n}$ for some integer k

$\rightarrow$ claim: $m \cdot m^{kr} \equiv m \pmod{n}$ or (more strictly) $m^{kr} \equiv 1 \pmod{n}$

If $\gcd(m, p) = 1$ and $\gcd(m, q) = 1$, then ?

If $\gcd(m, p) \neq 1$ or $\gcd(m, q) \neq 1$, then ?

- If $\gcd(m, p) = 1$ and $\gcd(m, q) = 1$, then by Fermat's little theorem
  - $m^{p-1} \equiv 1 \pmod{p} \implies m^{kr} \equiv 1 \pmod{p}$
  - $m^{q-1} \equiv 1 \pmod{q} \implies m^{kr} \equiv 1 \pmod{q}$
- By the definition of congruence, $p \mid m^{kr} - 1$ and $q \mid m^{kr} - 1$.
- Along with the fact that p and q are distinct prime numbers, we have

  $pq \mid m^{kr} - 1 \quad \implies m^{kr} \equiv 1 \pmod{n} \implies m^{ed} \equiv m \pmod{n}.$

- If $\gcd(m,p) \neq 1$, then $p \mid m$. ($\rightarrow$ which implies that $\gcd(m,q) = 1$)
  - $m^{ed} \equiv m \pmod{p}$
  - $m^{ed} \equiv m^{1+k(p-1)(q-1)} \equiv m \cdot (m^{q-1})^{k(p-1)} \equiv m \pmod{q}$
- By the definition of congruence, $p \mid m^{ed} - m$ and $q \mid m^{ed} - m$.
- Along with the fact that p and q are distinct prime numbers, we have

  $pq \mid m^{ed} - m \implies m^{ed} \equiv m \pmod{n}$.
- A similar argument holds for $\gcd(m,q) \neq 1$. ∎

Remark.

[Euler's theorem] Let a and n be positive integers. If $\gcd(a, n) = 1$, then

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

where $\varphi(n)$ is the Euler's totient function, indicating the number of integers i, for $i \in \{1, 2, \ldots, n\}$, that are relatively prime to n.

- We can apply Euler's theorem to show that

  $$m^{k(p-1)(q-1)} \equiv 1 \pmod{pq}$$

  for $\gcd(m, pq) = 1$.

  (you have to know that $\varphi(pq) = (p-1)(q-1)$, for primes p and q.)

- We still have to argue why $m^{ed} \equiv m \pmod{pq}$ when $\gcd(m, pq) \neq 1$.

Discussion

- In the proof given above, we have to find a solution for either

$$\begin{cases} x \equiv 1 \pmod{p} \\ x \equiv 1 \pmod{q} \end{cases} \quad \text{or} \quad \begin{cases} x \equiv m \pmod{p} \\ x \equiv m \pmod{q} \end{cases}$$

- We look for "the" solution for a system of congruences.

- Can we solve a system of congruences in a more general form?

Solving congruence equations.

E.g.,
$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$
$$x = ?$$

Q1: Is there such a solution? (existence)

Q2: Is the solution unique if there exists one? (uniqueness)

Proposition [Uniqueness]. Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than 1, and $a_1, a_2, \ldots, a_n$ arbitrary integers. If x_1 and x_2 are two solutions of the system

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\vdots \\
x &\equiv a_n \pmod{m_n}
\end{aligned}
$$

then $m_1 \cdot m_2 \cdot \ldots \cdot m_n \mid (x_1 - x_2)$.

Proof:

- Let x_1 and x_2 be two solutions of the system.
- Then $x_1 \equiv a_k \pmod{m_k}$ and $x_2 \equiv a_k \pmod{m_k}$ for $k \in \{1, 2, \ldots, n\}$.
- Thus, $x_1 - x_2 \equiv 0 \pmod{m_k}$ for $k \in \{1, 2, \ldots, n\}$.

  $\rightarrow m_k \mid (x_1 - x_2)$ for $k \in \{1, 2, \ldots, n\}$.
- $\gcd(m_k, m_i) = 1$ for $i \neq k \Longrightarrow m_1 \cdot m_2 \cdot \ldots \cdot m_n \mid (x_1 - x_2)$.
  - Since otherwise, there exists i, with $1 \leq i < n$, such that

    $$\frac{x_1 - x_2}{m_1 \cdot \ldots \cdot m_i} \in \mathbb{Z} \quad \text{and} \quad m_{i+1} \nmid \frac{x_1 - x_2}{m_1 \cdot \ldots \cdot m_i}.$$
  - Then $\gcd(m_{i+1}, m_1 \cdot \ldots \cdot m_i) > 1$.
  - This implies that $\gcd(m_{i+1}, m_j) > 1$ for some $j < i + 1$. $(\Rightarrow\Leftarrow)$ ∎

Theorem. (Chinese remainder theorem) Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than 1, and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}.$$

has a unique solution modulo $m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

Proof:

- Let $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$, and let $M_k = m/m_k$ for $k \in \{1, 2, \ldots, n\}$.
- Since $\gcd(m_i, m_k) = 1$ for $i \neq k$, we have $\gcd(M_k, m_k) = 1$.
- By Bézout's identity there exists an integer y_k such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

- claim: $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n$ is a solution.
  - $M_j \equiv 0 \pmod{m_k}$ for $j \neq k$.
  - $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$ for $k \in \{1, 2, \ldots, n\}$.
- By the proposition of uniqueness, the theorem follows. ∎

[Interpretation: The algorithm provided by the proof]

$$
\begin{array}{cccc}
x \equiv a_1 \pmod{m_1} & x \equiv 0 \pmod{m_1} & \dots & x \equiv 0 \pmod{m_1} \\
x \equiv 0 \pmod{m_2} & x \equiv a_2 \pmod{m_2} & \dots & x \equiv 0 \pmod{m_2} \\
\vdots & \vdots & & \vdots \\
x \equiv 0 \pmod{m_n} & x \equiv 0 \pmod{m_n} & \dots & x \equiv a_n \pmod{m_n} \\
\downarrow & \downarrow & & \downarrow
\end{array}
$$

$$
x_1 = (m_2 \cdot m_3 \cdot \ldots \cdot m_n) \cdot y_1 \quad x_2 = (m_1 \cdot m_3 \cdot \ldots \cdot m_n) \cdot y_2 \quad x_n = (m_1 \cdot m_2 \cdot \ldots \cdot m_{n-1}) \cdot y_n
$$

$$
x_1 + k_1 m_1 = a_1 \qquad x_2 + k_2 m_2 = a_2 \qquad x_n + k_n m_n = a_n
$$

$\rightarrow x_1 + x_2 + \ldots + x_n$ is a solution to the original congruence system.

Exercise

- Solve

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

Consider the systems:

$$\boxed{\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 0 \pmod{5} \\ x &\equiv 0 \pmod{7} \end{aligned}} \qquad \boxed{\begin{aligned} x &\equiv 0 \pmod{3} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 0 \pmod{7} \end{aligned}} \qquad \boxed{\begin{aligned} x &\equiv 0 \pmod{3} \\ x &\equiv 0 \pmod{5} \\ x &\equiv 1 \pmod{7} \end{aligned}}$$

Then solve

$$35y_1 \equiv 1 \pmod{3} \qquad 21y_2 \equiv 1 \pmod{5} \qquad 15y_3 \equiv 1 \pmod{7}$$

for y_1, y_2, and y_3.

$\rightarrow$ $70y_1 + 63y_2 + 30y_3$ is a solution to the original system.