1、可除性：Divisibility: We say that a divides b if there is an integer c such that $b = ac$, or equivalently b/a is an integer.

- If a, b, c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|(mb + nc)$ whenever m and n are integers.

余数计算 **Corollary:** Let m be a positive integer and let a and b be integers. Then,

$$(a + b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$$

$$ab \textbf{ mod } m = ((a \textbf{ mod } m)(b \textbf{ mod } m)) \textbf{ mod } m$$

同余关系 Congruence Relation: If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$, denoted by $a \equiv b$ (**mod** m).

Theorem: Let m be a positive integer. If $a \equiv b$ (**mod** m) and $c \equiv d$ (**mod** m), then

$$a + c \equiv b + d \ (\textbf{mod } m)$$

$$ac \equiv bd \ (\textbf{mod } m)$$

The integers a and b are congruent modulo m if and only if there is an integer k such that

$$a = b + km.$$

2、若a为一整数，则称 a divides b，记作 $a|b$，若不可除，记作 $a \nmid b$

3、Euclidean Algorithm 欧几里德算法计算gcd：For two integers 287 and 91, we want to find $\gcd(287, 91)$.

Step 1: $287 = 91 \cdot 3 + 14$

Step 2: $91 = 14 \cdot 6 + 7$

Step 3: $14 = 7 \cdot 2 + 0$

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$$

4、若 $\gcd(a,b)=1$，则称a,b are relatively prime

5、**Bezout'S Theorem**: If a and b are positive integers, then there exist integers s and t such that

$$\gcd(a, b) = sa + tb.$$

Lemma: If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Lemma: If p is prime and $p|a_1a_2...a_n$, then $p|a_i$ for some i.

6、线性同余：A congruence of the form $ax \equiv b$ (**mod** m), where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

The solutions to a linear congruence $ax \equiv b$ $\boxed{(\textbf{mod } m) \text{ are all integers } x}$ $\to x \equiv \bar{a}b \,(\text{mod})\, m$ that satisfy the congruence.

7、模逆元：**Modular Inverse**: An integer $\bar{a}$ such that $\bar{a}a \equiv 1$ (**mod** m) is said to be an inverse of a modulo m.

Solve the congruence $ax \equiv b$ (**mod** m) by multiplying both sides by $\bar{a}$.

$$x \equiv \bar{a}b \ (\textbf{mod } m).$$

存在条件 When does inverse exist?

Theorem: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. The inverse is unique modulo m. That is,

例题：$\bar{a} \cdot 101 \equiv 1 \,(\text{mod } 4620)$，求 $\bar{a}$ ⇒解：①写 $\gcd(4620, 101) = 1$ 的过程

②逆推，数与数的相乘保持，如3×5不要写为15。

③得到 $1 = -35 \cdot 4620 + 1601 \cdot 101$，稍作变换，则 $\bar{a} = 1601$

8、求线性同余方程组：两种方法相互验证

① The Chinese Remainder Theorem: Example

$x \equiv 2$ (**mod** 3) $a_1 = 2$ $m_1 = 3$ $M_1 = \frac{m}{m_1} = 35$

$x \equiv 3$ (**mod** 5) $a_2 = 3$ $m_2 = 5$ $M_2 = \frac{m}{m_2} = 21$

$x \equiv 2$ (**mod** 7) $a_3 = 2$ $m_3 = 7$ $M_3 = \frac{m}{m_3} = 15$

$m = m_1 \cdot m_2 \cdot m_3$

1. Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, and $M_3 = m/7 = 15$.
2. Compute y_k, i.e., the inverse of M_k modulo m_k:
   - $35 \cdot 2 \equiv 1$ (**mod** 3) $y_1 = 2$
   - $21 \equiv 1$ (**mod** 5) $y_2 = 1$
   - $15 \equiv 1$ (**mod** 7) $y_3 = 1$

   $\Leftarrow \begin{cases} M_1 y_1 \equiv 1 \,(\text{mod } m_1) \\ M_2 y_2 \equiv 1 \,(\text{mod } m_2) \\ M_3 y_3 \equiv 1 \,(\text{mod } m_3) \end{cases}$
3. Compute a solution $x = a_1M_1y_1 + \ldots + a_nM_ny_n$:
   $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23$ (**mod** 105)
4. The solutions are all integers x that satisfy $x \equiv 23$ (**mod** 105).

② Back Substitution

We may also solve systems of linear congruences with pairwise relatively prime moduli $m_1, m_2, \ldots m_n$ by back substitution.

Example:

(1) $x \equiv 1$ (**mod** 5)

(2) $x \equiv 2$ (**mod** 6)

(3) $x \equiv 3$ (**mod** 7)

According to (1), $x = 5t + 1$, where t is an integer.

Substituting this expression into (2), we have $5t + 1 \equiv 2$ (**mod** 6), which means that $t \equiv 5$ (**mod** 6). Thus, $t = 6u + 5$, where u is an integer.

Substituting $x = 5t + 1$ and $t = 6u + 5$ into (3), we have $30u + 26 \equiv 3$ (**mod** 7), which implies that $u \equiv 6$ (**mod** 7). Thus, $u = 7v + 6$, where v is an integer.

Thus, we must have $x = 210v + 206$. Translating this back into a congruence,

$$x \equiv 206 \ (\textbf{mod } 210).$$

② 的答案过程：

$x = 5t + 1$

代(2) $5t + 1 - 2 = 6m \Rightarrow t = \frac{6m+1}{5} = m + \frac{m+1}{5}$

$m = 5n - 1 \Rightarrow t = 6n - 1$

$\Rightarrow x = 30n - 4$

代(3) $30n - 4 - 3 = 7p \Rightarrow n = \frac{7p+7}{30}$

$p = 30q - 1 \Rightarrow n = 7q$

$\therefore x = 30n - 4 = 210q - 4 = 206 + 210v$

9、Fermat's Little Theorem：若p为质数 $p \nmid a$，则 $a^{p-1} \equiv 1 \,(\text{mod } p)$。若p为质数，则 $a^p \equiv a \,(\text{mod } p)$

10、RAS Cryptosystem：

p,q应大于200位

p,q需密秘保存

Pick two large primes p and q. Let $n = pq$. **Encryption key** (n, e) and **decryption key** (n, d) are selected such that

(1) $\gcd(e, (p-1)(q-1)) = 1$ public key公钥：(n, e)

(2) $ed \equiv 1$ (**mod** $(p-1)(q-1)$) private key私钥：d

RSA encryption: $C = M^e$ **mod** n;

RSA decryption: $M = C^d$ **mod** n.

11、数学归纳强形式

Principle (Strong Principle of Mathematical Induction):

(a) Basic Step: the statement $P(b)$ is true

(b) Inductive Step: for all $n > b$, the statement

$$P(b) \wedge P(b+1) \wedge \ldots \wedge P(n-1) \to P(n) \text{ is true.}$$

Then, $P(n)$ is true for all integers $n \geq b$.

12、迭代函数：构造迭代函数：To specify a function on the basis of a recurrence:

- Basis step (initial condition): Specify the value of the function at zero.
- Recursive step: Give a rule for finding its value at an integer from its values at smaller integers.

Find a closed-form solution? "Top-down" and "bottom-up"

找迭代函数的closed form：

$$\begin{aligned} T(n) &= rT(n-1) + a \\ &= r(rT(n-2) + a) + a \\ &= r^2T(n-2) + ra + a \\ &= r^2(rT(n-3) + a) + ra + a \\ &= r^3T(n-3) + r^2a + ra + a \\ &= r^3(rT(n-4) + a) + r^2a + ra + a \\ &= r^4T(n-4) + r^3a + r^2a + ra + a. \end{aligned}$$

$T(0) = b$

$T(1) = rT(0) + a = rb + a$

$T(2) = rT(1) + a = r(rb + a) + a = r^2b + ra + a$

$T(3) = rT(2) + a = r^3b + r^2a + ra + a$

13、鸽巢定理：使用此定理时通常用反证法

The Pigeonhole Principle: If k is a positive integer and $k + 1$ or more objects are placed into k boxes, then there is at least one box containing two or more of the objects.

If N objects are placed into k bins, then there is at least one bin containing at least $\lceil N/k \rceil$ objects.

14、counting：

product rule：n步，相互依赖：$n = n_1 \times n_2 \times n_3 \times \ldots \times n_k$

sum rule：要么走 n_1 中的一步，要么走 n_2 中的一步，n_1, n_2 完全不同，$n = n_1 + n_2$

subtraction rule：与上相似，但 n_1, n_2 可能部分相似

$n = |A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

principle of inclusion-exclusion

15、排列 permutation: $A_n^r = P(n,r) = \frac{n!}{(n-r)!}$ 组合 combinations $C_n^r = C(n,r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}$, $C_n^r = C_n^{n-r}$

16. binomial coefficient: $\binom{n}{r}$ 即 $C_n^r = \frac{n!}{r!(n-r)!}$ trinomial coefficient: $\binom{n}{k_1\ k_2\ k_3} = \frac{n!}{k_1!k_2!k_3!}$, 相等于 $\binom{n}{k_1}\cdot\binom{n-k_1}{k_2}$

17. Pascal's Identity: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, 即 $C_n^k = C_{n-1}^{k-1} + C_{n-1}^{k}$ 组合求和: $C_n^0 + C_n^1 + C_n^2 + \dots + C_n^{n-1} + C_n^n = 2^n$

18. The Binomial Theorem: $(x+y)^n = \sum_{j=0}^{n}\binom{n}{j}x^{n-j}y^j = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$

19. A linear homogeneous relation of degree k with constant coefficients is a recurrence,

其形式为 $a_n = c_1a_{n-1} + c_2a_{n-2} + \dots + c_ka_{n-k}$, $c_1, c_2, \dots, c_k \in R$, $c_k \neq 0$

linear: 为前项线性组合, homogeneous: 齐次,所有项均为 a_n 前项的一次的倍数, degree k: 用前 k 项表示

20、解线性齐次:

The characteristic equation (CE) is:

$$r^k - \sum_{i=1}^{k} c_i r^{k-i} = 0.$$

对 $k=2$ 无重数

$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$

若 r 无重数

则 $a_n = \sum_{i=1}^{k} a_i r_i^n$

Theorem: Suppose that there are t roots $r_1, \dots, r_t$ with multiplicities $m_1, \dots, m_t$. Then,

$$\begin{aligned} a_n = \ & (\alpha_{1,0} + \alpha_{1,1}n + \cdots + \alpha_{1,m_1-1}n^{m_1-1})r_1^n \\ & + (\alpha_{2,0} + \alpha_{2,1}n + \cdots + \alpha_{2,m_2-1}n^{m_2-1})r_2^n \\ & + \cdots + (\alpha_{t,0} + \alpha_{t,1}n + \cdots + \alpha_{t,m_t-1}n^{m_t-1})r_t^n \end{aligned}$$

对 $k=2$, 有重数 $a_n = (\alpha_1 + \alpha_2 n)r_0^n$

- Solving the roots with CE
- Solving the α_i for all i using initial conditions

21、解线性非齐次:

Definition: A linear nonhomogeneous relation with constant coefficients may contain some terms $F(n)$ that depend only on n

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \dots + c_ka_{n-k} + F(n).$$

The recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2} + \dots + c_ka_{n-k}$ is called the associated homogeneous recurrence relation.

Theorem: If $\{a_n^{(p)}\}$ is any particular solution to the linear nonhomogeneous relation with constant coefficients,

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \dots + c_ka_{n-k} + F(n),$$

Then all its solutions are of the form

$$a_n = a_n^{(p)} + a_n^{(h)},$$

where $\{a_n^{(h)}\}$ is any solution to the associated homogeneous recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2} + \dots + c_ka_{n-k}$.

22、找21.中的特解:

若 $F(n) = (b_tn^t + b_{t-1}n^{t-1} + \cdots + b_1n + b_0)s^n$

若 s 为特征根且重数为 m

$a_n^{(p)} = n^m(p_tn^t + p_{t-1}n^{t-1} + \cdots + p_1n + p_0)s^n.$

若 s 不为特征根

$a_n^{(p)} = (p_tn^t + p_{t-1}n^{t-1} + \cdots + p_1n + p_0)s^n.$

例题: Find all solutions of the recurrence relation $a_n = 5a_{n-1} - 6a_{n-2} + 7^n$.

Solution:

- $a_n^{(h)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n$
- Let $a_n^{(p)} = C \cdot 7^n$:

$$C \cdot 7^n = 5C \cdot 7^{n-1} - 6C \cdot 7^{n-2} + 7^n.$$

Thus, $C = 49/20$, and $a_n^{(p)} = (49/20)7^n$.

- Solve α_i in $a_n = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n + (49/20)7^n$ using initial conditions.

23. The generating function for the sequence $a_0, a_1, \dots, a_k, \dots$ of real numbers is the infinite series

$$G(x) = a_0 + a_1x + \dots + a_kx^k + \dots = \sum_{k=0}^{\infty} a_kx^k.$$

若 $f(x) = \sum_{k=0}^{\infty} a_kx^k$, $g(x) = \sum_{k=0}^{\infty} b_kx^k$

则 $f(x) + g(x) = \sum_{k=0}^{\infty}(a_k + b_k)x^k$

$f(x)g(x) = \sum_{k=0}^{\infty}\left(\sum_{j=0}^{k} a_jb_{k-j}\right)x^k$

例题 **Example 2**: To obtain the corresponding sequence of $G(x) = 1/(1-ax)^2$ for $|ax| < 1$:

Consider $f(x) = 1/(1-ax)$ and $g(x) = 1/(1-ax)$. Since the sequence of $f(x)$ and $g(x)$ corresponds to $1, a, a^2, \dots$, we have

$$G(x) = f(x)g(x) = \sum_{k=0}^{\infty}(k+1)a^kx^k.$$

24. For $|x| < 1$, function $G(x) = 1/(1-x)$ is the generating function of the sequence $1, 1, 1, 1, \dots$,

$$1/(1-x) = 1 + x + x^2 + \dots$$

For $|ax| < 1$, function $G(x) = 1/(1-ax)$ is the generating function of the sequence $1, a, a^2, a^3, \dots$,

$$1/(1-ax) = 1 + ax + a^2x^2 + \dots$$

For $|x| < 1$, $G(x) = 1/(1-x)^2$ is the generating function of the sequence $1, 2, 3, 4, 5, \dots$

$$1/(1-x)^2 = 1 + 2x + 3x^2 + \dots$$

25. Reflexive Relation: A relation R on a set A is called reflexive if $(a,a) \in R$ for every element $a \in A$.

Irreflexive Relation: A relation R on a set A is called irreflexive if $(a,a) \notin R$ for every element $a \in A$.

Symmetric Relation: A relation R on a set A is called symmetric if $(b,a) \in R$ whenever $(a,b) \in R$ for all $a, b \in A$.

Antisymmetric Relation: A relation R on a set A is called antisymmetric if $(b,a) \in R$ and $(a,b) \in R$ implies $a = b$ for all $a, b \in A$.

Transitive Relation: A relation R on a set A is called transitive if $(a,b) \in R$ and $(b,c) \in R$ implies $(a,c) \in R$ for all $a, b, c \in A$.

Let $A = \{a_1, a_2, \dots, a_m\}$ and $B = \{b_1, b_2, \dots, b_n\}$, the Cartesian product $A \times B$ is the set of pairs $\{(a_1,b_1), (a_2,b_2), \dots, (a_1,b_n), \dots, (a_m,b_n)\}$.

Let A and B be two sets. A binary relation from A to B is a subset of a Cartesian product $A \times B$.

A relation on the set A is a relation from A to itself.

We use the notation aRb to denote $(a,b) \in R$, and $a\not{R}b$ to denote $(a,b) \notin R$.

Definition: Let R be a relation from a set A to a set B and S be a relation from B to C. The composite of R and S is the relation consisting of the ordered pairs (a,c) where $a \in A$ and $c \in C$ and for which there is a $b \in B$ such that $(a,b) \in R$ and $(b,c) \in S$.

Example: Let $A = \{1,2,3\}$, $B = \{0,1,2\}$, and $C = \{a,b\}$:

- $R = \{(1,0), (1,2), (3,1), (3,2)\}$
- $S = \{(0,b), (1,a), (2,b)\}$
- $S \circ R = \{(1,b), (3,a), (3,b)\}$