离散数学及其应用 第4章 数论与密码学

4. Number Theory and Crytography

Number theory is the part of mathematics devoted to the study of the integers and their properties.

💡 这些都是初中奥数的知识了，看看英文怎么表达基本上就能搞定。

4.1 Divisibility and Modular Arithmetic

4.1.1 Division

If a and b are integers with $a \neq 0$, then a `divides` b if there exists an integer c such that $b = ac$, or equivalently $\frac{b}{a} \in \mathbb{Z}$, denoted by $a|b$. When a divides b, we say that a is a `factor` or `divisor` of b and that b is a `multiple` of a. If a does not divide b, we write $a \nmid b$.

📋 Properties of Divisibility

Let a , b , and c be integers, where $a \neq 0$.

- If $a|b$ and $a|c$, then $a|(mb+nc)$ whenever $m, n \in \mathbb{Z}$;
- If $a|b$, then $a|bc$ for all integers c ;
- If $a|b$ and $b|c$, then $a|c$.

📋 Division Algorithm

If a is an integer and d a positive integer, then there are unique integers q and r , with $0 \leq r < d$, such that $a = dq + r$. Here d is called the **`divisor`** , a is called the **`dividend`** , q is called the **`quotient`** , r is called the **`remainder`** . The notation is $q = a \,\mathbf{div}\, d$ and $r = a \bmod d$.

⚠️ Note that the remainder cannot be negative. $-4 = -11 \,\mathbf{div}\, 3$, $1 = -11 \bmod 3$.+

4.1.2 Congruence

`Congruence Relation` If a and b are integers and m is a positive integer, then a is congruent to b modulo m if $m|(a-b)$, denoted by $a \equiv b \pmod{m}$. We say that $a \equiv b \pmod{m}$ is a **`congruence`** and that m is its **`modulus`** . If a is not congruent to b modulo m , we write $a \not\equiv b \pmod{m}$.

📋 Two integers are congruent mod m if and only if they have the same remainder when divided by m , or equivalently there is an integer k such that $a = b + km$.

📋 Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m} \leftrightarrow a \bmod m = b \bmod m$.

⚠️ The use of "mod" in $a \equiv b \pmod{m}$ and $a \bmod m = b \bmod m$ are different. $a \equiv b \pmod{m}$ is a relation on the set of integers, while in $a \bmod m = b \bmod m$, the notation $\mathbf{mod}$ denotes a function.

📋 Congruences of Sums and Products

Let m be a positive integer.

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$,

then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Corollary: Let m be a positive integer and let a and b be integers, then

$$(a+b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m$$

$$ab \bmod m = [(a \bmod m)(b \bmod m)] \bmod m$$

📋 Algebraic Manipulation of Congruences

- Multiplying both sides of a valid congruence by an integer preserves validity.
  - If $a \equiv b (\bmod m)$ holds, then $c \cdot a \equiv c \cdot b (\bmod m)$, where c is any integer, holds by the theorem of congruences of products with $d = c$.
- Adding an integer to both sides of a valid congruence preserves validity.
  - If $a \equiv b (\bmod m)$ holds then $c + a \equiv c + b (\bmod m)$, where c is any integer, holds by the theorem of congruences of sums with $d = c$.

4.1.3 Arithmetic Modulo

The operation $+_m$ is defined as $a +_m b = (a + b) \mathbf{mod}\, m$. This is `addition modulo m` .

The operation $\cdot_m$ is defined as $a \cdot_m b = (a \cdot b) \mathbf{mod}\, m$. This is `multiplication modulo m` .

Using these operations is said to be doing `arithmetic modulo m` .

Let $\mathbb{Z}_m$ be the set of nonnegative integers less than m . That is $\mathbb{Z}_m = \{0, 1, ..., m - 1\}$.

🌰 e.g.

7 $+_{11}$ 9 = (7 + 9) mod 11 = 5

9 $\cdot_{11}$ 7 = (9 · 7) mod 11 = 8

📋 The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication.

- Closure: $a, b \in \mathbb{Z}_m \to (a +_m b), (a \cdot_m b) \in \mathbb{Z}_m$
- Associativity: $a, b, c \in \mathbb{Z}_m \to [(a +_m b) +_m c = a +_m (b +_m c)] \wedge [(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)]$
- Commutativity: $a, b \in \mathbb{Z}_m \to (a +_m b = b +_m a) \wedge (a \cdot_m b = b \cdot_m a)$
- Identity elements: The elements 0 and 1 are identity elements for addition and multiplication modulo m , respectively. If a belongs to $\mathbb{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.
- Additive inverses: If $a \neq 0$ belongs to $\mathbb{Z}_m$, then $m - a$ (⚠️ not $-a$ because it is not in $\mathbb{Z}_m$) is the additive inverse of a modulo m and 0 is its own additive inverse.

$a +_m (m - a) = 0$ and $0 +_m 0 = 0$.

- Distributivity: If $a, b, c \in \mathbb{Z}_m$, then $[a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)]$ and $[(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)]$

⚠️ Multiplicatative inverses have not been included since they do not always exist. For example, there is no multiplicative inverse of 2 modulo 6.

> 4.2 节没什么知识，跳过了。

4.3 Primes and GCDs

4.3.1 Primes

A positive integer p greater than 1 is called `prime` if the only positive factors of p are 1 and p . A positive integer that is greater than 1 and is not prime is called `composite` .

📋 The Foundamental Theorm of Arithmetic

Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

📋 Trial division

Trial division, a very inefficient method of determining if a number *n* is prime, is to try every integer $i \leq \sqrt{n}$ and see if n is divisible by i . This is because if an integer n is a composite integer, then it has a prime divisor less than or equal to $\sqrt{n}$. To see this, note that if $n = a$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

📋 Infinitude of Primes (proof by Eucluid)

There are infinitely many primes.

Proof:

> Assume finitely many primes: $p_1, p_2, ..., p_n$.
>
> Let $q = p_1 p_2 ... p_n + 1$, then q is a prime not in the list of all the primes.
>
> So there are infinitely many primes.

4.3.2 GCD and LCM

Let a and b be integers, not both zero. The largest integer d such that $d|a$ and also $d|b$ is called the `greatest common divisor (GCD)` of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

The `least common multiple (LCM)` of the positive integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by $\operatorname{lcm}(a, b)$.

The integers a and b are `relatively prime` if their greatest common divisor is 1. The integers $a_1, a_2, \ldots, a_n$ are `pairwise relatively prime` if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

📋 Finding GCDs and LCMs Using Prime Factorizations

Suppose the prime factorizations of a and b are:

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n},$$

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \ldots p_n^{\min(a_n,bn)}$$

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,bn)}$$

📋 Let a and b be positive integers. Then $ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$.

📋 Euclidean Algorithm（辗转相除法）

The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that $\gcd(a, b)$ is equal to $\gcd(b, r)$ when $a > b$ and r is the remainder when a is divided by b.

The Euclidean algorithm expressed in pseudocode is:

```
procedure gcd(a, b: positive integers)
x := a
y := b
while  y ≠ 0
      r := x mod y
      x := y
      y := r
return x {gcd(a,b) is x}
```

📋 Bézout's Theorem（裴蜀定理）

If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$. Integers s and t such that $\gcd(a, b) = sa + tb$ are called `Bé`

zout coefficients of a and b. The equation $\gcd(a,b)=sa+tb$ is called **Bézout's identity** （裴蜀恒等式）. To find Bézout coefficients, first use the Euclidian algorithm to find the gcd, and then works backwards to express the gcd as a linear combination of the original two integers.

0089-过不了520，来解一位民科大哥出的题 | 裴蜀定理与扩欧算法_哔哩哔哩_bilibili

e.g.

Express $\gcd(252,198)=18$ as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show $\boldsymbol{gcd}(252,198) = 18$

i. $252 = 1\cdot 198 + 54.$ ii. $198 = 3\cdot 54 + 36$

iii. $54 = 1\cdot 36 + 18$ iv. $36 = 2\cdot 18$

- Now working backwards, from (iii) and (ii) above
  - $18 = 54 - 1\cdot 36$
  - $36 = 198 - 3\cdot 54$
- Substituting the 2nd equation into the 1st yields:
  - $18 = 54 - 1\cdot(198 - 3\cdot 54) = 4\cdot 54 - 1\cdot 198$
- Substituting $54 = 252 - 1\cdot 198$ (from i)) yields:
  - $18 = 4\cdot(252 - 1\cdot 198) - 1\cdot 198 = 4\cdot 252 - 5\cdot 198$

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

Proof:

Since $\gcd(a,b)=1$, by Bézout's Theorem there are integers s and t such that $sa+tb=1$. Multiplying both sides of the equation by c, yields $sac+tbc=c$.

Since $a|sac$ and $a|tbc$, we can conclude that $a|sac+tbc$.

If p is prime and $p\,/\,a_1a_2...a_n$, then $p\,/\,a_i$ for some i.

(Proof uses mathematical induction. It is crucial in the proof of the uniqueness of prime factorizations.)

A prime factorization of a positive integer where the primes are in nondecreasing order is unique.

Proof: (by contradiction) Suppose that the positive integer n can be written as a product of primes in two distinct ways:

$$n = p_1 p_2 \cdots p_s \text{ and } n = q_1 q_2 \cdots p_t.$$

- Remove all common primes from the factorizations to get $p_{i1}p_{i2} \cdots p_{iu} = q_{j1}q_{j2} \cdots q_{jv}$
- By Lemma 3, it follows that p_{i1} divides q_{jk} for some k, contradicting the assumption that and are distinct primes.
- Hence, there can be at most one factorization of n into primes in nondecreasing order.

📋Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Proof: Since $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$ and the fact that $gcd(c, m) = 1$, it follows that $m \mid a - b$. Hence, $a \equiv b \pmod{m}$.

4.4 Solving Congruences

4.4.1 Linear Congruences

A congruence of the form $ax \equiv b \pmod{m}$, 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 $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an `inverse` of a modulo m.

The Euclidean algorithm and Bézout coefficients gives us a systematic approaches to finding inverses.

📋If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (This means that there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.)

Proof:

Since $gcd(a, m) = 1$, there exist integers s and t such that $sa + tm = 1$. Hence, $sa + tm \equiv 1 \pmod{m}$. Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$. Consequently, s is an inverse of a modulo m.

📋Finding Inverses

The Euclidean algorithm and Bézout coefficients gives us a systematic approaches to finding inverses.

🌰e.g.

Find an inverse of 3 modulo 7.

Solution:

3 and 7 are relatively prime, so there exist an inverse of 3 modulo 7. Using the Euclidian algorithm: $7 = 2 \times 3 + 1$, so -2 and 7 are Bézout coefficients of 3 and 7.

$-2 \times 3 + 1 \times 7 = 1$, and $-2 \times 3 + 1 \times 7 \equiv -2 \times 3 \pmod 7$, so -2 is an inverse of 3 modulo 7. And every integer congruent to -2 modulo 7 is an inverse of 3 modulo 7.

📋Solving Congruences Using Inverses

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

🌰e.g.

What are the solutions of the congruence $3x \equiv 4 (mod\ 7)$?

Solution:

-2 is an inverse of 3 modulo 7, so multiply both sides of the congruence by -2 giving $-2 \times 3x \equiv -2 \times 4 (mod\ 7)$. Because $-6 \equiv 1 \ (mod\ 7)$ and $-8 \equiv 6 \ (mod\ 7)$, it follows that if x is a solution, then $x \equiv -8 \equiv 6 \ (mod\ 7)$.

We need to determine if every x with $x \equiv 6 \ (mod\ 7)$ is a solution. Multiply both sides by 3 and get $3x \equiv 18 \equiv 4 (mod\ 7)$, which shows that all such x satisfy the congruence.

📋Solving Systems of Linear Congruences Using Back Substitution

Substitute the value for the variable into another congruence, and continuing the process until we have worked through all the congruences.

🌰e.g.

Use the method of back substitution to find all integers x such that $x \equiv 1 \ (mod\ 5)$, $x \equiv 2 \ (mod\ 6)$, and $x \equiv 3 \ (mod\ 7)$.

Solution:

The first congruence can be rewritten as $x = 5t + 1$, $t \in \mathbb{Z}$.

Substituting into the second congruence yields $5t + 1 \equiv 2 \ (mod\ 6)$. Solving this tells us that $t \equiv 5 \ (mod\ 6)$. So $t = 6u + 5$, $u \in \mathbb{Z}$. Substituting this back into $x = 5t + 1$, gives $x =$

$5(6u + 5) +1 = 30u + 26$.

Inserting this into the third equation gives $30u + 26 \equiv 3 \ (mod\ 7)$. Solving this congruence tells us that $u \equiv 6 \ (mod\ 7)$. So $u = 7v + 6, v \in \mathbb{Z}$. Substituting this expression for u into $x = 30u + 26$, tells us that $x = 30(7v + 6) + 26 = 210u + 206$.

Translating this back into a congruence we find the solution $x \equiv 206 \ (mod\ 210)$.

4.4.2 The Chinese Remainder Theorem

It is a different method to solve a system of linear congruences.

📋The 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:

$$\begin{aligned} x &\equiv a_1 \,(\,mod\ m_1) \\ x &\equiv a_2 \,(\,mod\ m_2) \\ &\ldots \\ x &\equiv an \,(\,mod\ m_n) \end{aligned}$$

has a unique solution modulo $m = m_1 \times m_2 \times \ldots \times m_n$. (That is, there is a solution x with $0 \leqslant x < m$ and all other solutions are congruent modulo m to this solution.)

Proof:

It is a constructive proof.

First let $M_k = m/m_k$ for $k = 1, 2, \ldots, n$. Since $gcd(m_k, M_k) = 1$, there is an integer y_k, an inverse of M_k modulo m_k, such that $M_k y_k \equiv 1 \ (mod\ m_k)$. Form the sum $x = a_1M_1y_1 + a_2M_2y_2 + \ldots + a_nM_ny_n$. Note that because $M_j \equiv 0 \ (mod\ m_k)$ whenever $j \neq k$, all terms except the k-th term in this sum are congruent to 0 modulo m_k. Because $M_ky_k \equiv 1(mod\ m_k)$, we see that $x \equiv a_kM_ky_k \equiv a_k(mod\ m_k)$, for $k = 1, 2, \ldots, n$. Hence, x is a simultaneous solution to the n congruences.

0084–无解？小学看《射雕》时傻算了好久 | 中国剩余定理 【修正版】_哔哩哔哩_bilibili

🌰e.g.

有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何？（《孙子算经》）

Solution:

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

$m = 3 \times 5 \times 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, $M_3 = m/7 = 15$.

2 is an inverse of M_1 modulo 3, 1 is an inverse of M_2 modulo 5, 1 is an inverse of M_3 modulo 7.

Hence, $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 = 2\times35\times2 + 3\times21\times1 + 2\times15\times1 = 233 \equiv 23 \pmod{105}$. So 23 is the smallest positive integer that is a simultaneous solution.

⚙️It is important to solve systems of linear congruences. Computers sometime store big integers in the form of theirs remainders and moduli.

4.4.3 Fermat's Little Theorem

📋Fermat's Little Theorem

If *p* is prime and *a* is an integer not divisible by *p*, then $a^{p-1} \equiv 1 \pmod p$. Furthermore, for every integer *a*, no matter if it is divisible by *p*, we have $a^p \equiv a \pmod p$.

Proof:

0082-两种证明费马小定理的美妙方法 | 如何用这个定理秒解一道IMO题? _哔哩哔哩_bilibili

⚙️Fermat's little theorem is useful in computing the remainders modulo p of large powers of integers.

🌰e.g.

Find 7^{222} mod 11.

Solution:

By Fermat's little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, and so $(7^{10})^k \equiv 1 \pmod{11}$, for every positive integer k. Therefore, $7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} \times 7^2 \equiv (1)^{22} \times 49 \equiv 5 \pmod{11}$. Hence, 7^{222} mod 11 = 5.

A number *p* not satisfying Fermat's Little Theorem must be a composite, but not every *p* satisfying Fermat's Little Theorem is a prime. Let *b* be a positive integer. If *n* is a composite integer, and $b^{n-1} \equiv 1 \pmod n$, then *n* is called a `pseudoprime` to the `base` *b*. Among the positive integers not exceeding a positive real number *x*, compared to primes, there are relatively few pseudoprimes to the base *b*.

🌰e.g.

Show that 341 is a pseudoprime to the base 2.

Proof:

$341 = 11 \cdot 31$, so 341 is a composite. $2^{340} \equiv 1 \pmod{341}$, so it is a pseudoprime.

We can replace 2 by any integer $b \geqslant 2$ as well.

There are composite integers n that pass all tests with bases b such that $gcd(b, n) = 1$. A composite integer n that satisfies the congruence $b^{n-1} \equiv 1 \pmod{n}$ for all positive integers b with $gcd(b, n) = 1$ is called a `Carmichael number`.

e.g.

Show that 561 is a Carmichael number.

Proof:

561 is composite, since $561 = 3 \cdot 11 \cdot 13$.

If $gcd(b, 561) = 1$, then $gcd(b, 3) = gcd(b, 11) = gcd(b, 17) = 1$.

Using Fermat's Little Theorem: $b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$, $b^{16} \equiv 1 \pmod{17}$.

Then

$$
\begin{aligned}
b^{560} &= (b^2)^{280} \equiv 1 \pmod{3},\\
b^{560} &= (b^{10})^{56} \equiv 1 \pmod{11},\\
b^{560} &= (b^{16})^{35} \equiv 1 \pmod{17}.
\end{aligned}
$$

It follows that $b^{560} \equiv 1 \pmod{561}$ for all positive integers b with $gcd(b,561) = 1$. Hence, 561 is a Carmichael number.