# 初等数论

1. 整除性质
    a) 若 a|b，a|c，则 a|(b ±c)。
    b) 若 a|b，则对任意 c，a|bc。
    c) 对任意非零整数 a，±1|a，±a|a。
    d) 若 a|b，b|a，则 |a|=|b|。
    e) 如果 a 能被 b 整除，c 是任意整数，那么积 ac 也能被 b 整除。
    f) 如果 a 同时被 b 与 c 整除，并且 b 与 c 互质，那么 a 一定能被积 bc 整除，反过来也成立。
    g) 如果 a|b 且 b|c，则 a|c。
    h) 如果 c|a 且 c|b，则 c|ua+vb，其中 u，v 是整数。
    i) 对任意整数 a，b，b>0，存在唯一的数对 q，r，使 a=bq+r，其中 0≤r<b，这个事实称为带余除法定理，是整除理论的基础。
    j) 若 c|a，c|b，则称 c 是 a，b 的公因数。若 d 是 a，b 的公因数，d≥0，且 d 可被 a，b 的任意公因数整除，则 d 是 a，b 的最大公因数。若 a，b 的最大公因数等于 1，则称 a，b 互素，也称互质。累次利用带余除法可以求出 a，b 的最大公因数，这种方法常称为辗转相除法。又称欧几里得算法。
2. 带余除法
    a) 对于 a，b 两个整数，其中 b≠0，则存在唯一 q，r 使得：

       a = bq+r，0 ≤r< |b|．r 称为 a 被 b 除得到的余数．显然当 r = 0 时，b|a.
3. 最大公约数

    设 a，b 是两个整数，如果整数 c|a 且 c|b，则 c 称为 a，b 的公因子．设 c>0 是两个不全为零的整数 a，b 的公因子，如果 a，b 的任何公因子都整除 c，则 c 称为 a，b 的最大公因子，记为 c=(a，b).
    a) (a,b)=(-a,b)=(a,-b)=(-a,-b)
    b) (0,a)=a
    c) 设 a，b 是两个不全为零的整数，则存在两个整数 u，v，使

       (a，b)= ua+vb .
4. 欧几里德除法（辗转相除法）：

    已知整数 a，b，记 $r_0$=a，$r_1$=b，

    $r_0=q_1r_1+r_2$，$0 \le r_2 < r_1=b$；

    $r_1=q_2r_2+r_3$，$0 \le r_3 < r_2$；

    …

    $r_{n-2}=q_{n-1}r_{n-1}+r_n$，$0 \le r_n < r_{n-1}$；

    $r_{n-1}=q_nr_n$

$r_n=(a, b)$

5. 互素

设 a，b 是两个不全为 0 的整数，如果 $(a, b)=1$，则称 a，b 互素．

推论：a，b 互素的充分必要条件是：存在 u，v，使 $ua+vb=1$．

a) 如果 $c \mid ab$ 且 $(c, a)=1$，则 $c \mid b$

b) 如果 $a \mid c$，$b \mid c$，且 $(a, b)=1$，则 $ab \mid c$

c) 如果 $(a, c)=1$，$(b, c)=1$，则 $(ab, c)=1$

6. 最小公倍数

设 a，b 是两个不等于零的整数．如果 $a \mid d$，$b \mid d$，则称 d 是 a 和 b 的公倍数． a 和 b 的正公倍数中最小的称为 a 和 b 的最小公倍数，记为 $[a, b]$．

a) $[a, b]=[-a, b]=[a, -b]=[-a, -b]$．

b) 设 d 是 a，b 的任意公倍数，则 $[a, b] \mid d$．

$[a, b]=\dfrac{|ab|}{(a, b)}$，特别地，如果 $(a, b)=1$，$[a, b]=|ab|$．

7. 素数

如果一个大于 1 的整数 p 除 $\pm1$ 和 $\pm p$ 外无其他因子，则 p 称为一个素数，否则称为合数．设 p 是一个素数，则

a) 对任意整数 a，如果 p 不整除 a，则 $(p, a)=1$．

b) 如果 $p \mid ab$，则 $p \mid a$，或 $p \mid b$．

c) 素数有无穷多个

8. 算术基本定理

每个大于 1 的整数 a 都可以分解为有限个素数的乘积：

$a=p_1p_2\cdots p_r$．

该分解除素数因子的排列外是唯一的．

a) 设 a 是任意大于 1 的整数，则 a 的除 1 外最小正因子 q 是一素数，并且当 a 是一合数时，$q \le \sqrt{a}$

9. 同余

给定一个称为模的正整数 m．如果 m 除整数 a，b 得相同的余数，即

$a=q_1m+r$，$b=q_2m+r$，$0\le r<m$，则称 a 和 b 关于模 m 同余，记为

$a\equiv b \pmod m$．

整数 a，b 对模 m 同余的充分必要条件是：$m \mid (a-b)$，即 $a=b+mt$，t 是整数

a) 反身性 $a\equiv a \pmod m$

b) 对称性若 $a\equiv b \pmod m$，则 $b\equiv a \pmod m$

c) 传递性若 $a\equiv b \pmod m$，$b\equiv c \pmod m$，则 $a\equiv c \pmod m$

d) 同余式相加若 $a\equiv b \pmod m$，$c\equiv d \pmod m$，则 $a+c\equiv b+d \pmod m$

e) 同余式相乘若 $a\equiv b \pmod m$，$c\equiv d \pmod m$，则 $ac\equiv bd \pmod m$

f) 除法若 $ac \equiv bc \pmod m$ $c \neq 0$ 则 $a \equiv b \pmod{m/\gcd(c,m)}$ 其中 gcd(c,m) 表示 c,m 的最大公约数，特殊地 ,gcd(c,m)=1 则 $a \equiv b \pmod m$

g) 幂运算如果 $a \equiv b \pmod m$，那么 $a^n \equiv b^n \pmod m$

h) 如果 $a \equiv b \pmod m$，且 $d \mid m$，d 是正整数，则 $a \equiv b \pmod d$

i) 若 $a \equiv b \pmod{m_i}$ (i=1,2...n) 则 $a \equiv b \pmod{[m_1,m_2,\dots,m_n]}$ 其中 $[m_1,m_2,\dots,m_n]$ 表示 $m_1,m_2,\dots,m_n$ 的最小公倍数

j) 推论 如果 $a_1 \equiv b_1 \pmod m$，$a_2 \equiv b_2 \pmod m$，则

$a_1x+a_2y \equiv b_1x+b_2y \pmod m$，其中 x，y 是任意整数.

$a_1^n \equiv b_1^n \pmod m$，其中 n 是正整数.

$f(a_1) \equiv f(b_1) \pmod m$，其中 f(x)是任一给定的整系数多项式：

$f(x)=c_0+c_1x+\cdots+c_kx_k$.

10. 威尔逊定理

若 p 为质数，则 p 可整除 (p-1)!+1 。

11. 欧拉定理

若 n,a 为正整数，且 n,a 互素，即 gcd(a,n) = 1 ，则 $a^{\varphi(n)} \equiv 1 \pmod n$

12. 孙子定理

中国剩余定理说明：假设整数 $m_1,m_2,\dots,m_n$ 两两互质，则对任意的整数：$a_1,a_2,\dots,a_n$，方程组 $(S)$ 有解，并且通解可以用如下方式构造得到：

设 $M = m_1 \times m_2 \times \cdots \times m_n = \prod_{i=1}^{n} m_i$ 是整数 $m_1,m_2,\dots,m_n$ 的乘积，并设

$M_i = M/m_i, \ \forall i \in \{1,2,\cdots,n\}$ 是除了 $m_i$ 以外的 n-1 个整数的乘积。

设 $t_i = M_i^{-1}$ 为 $M_i$ 模 $m_i$ 的数论倒数

$$t_iM_i \equiv 1 \pmod{m_i}, \ \forall i \in \{1,2,\cdots,n\}.$$ ：

方程组 $(S)$ 的通解形式为

$$x = a_1t_1M_1 + a_2t_2M_2 + \cdots + a_nt_nM_n + kM = kM + \sum_{i=1}^{n} a_it_iM_i, \quad k \in \mathbb{Z}.$$ ：

在模 $M$ 的意义下，方程组 $(S)$ 只有一个解：$x = \sum_{i=1}^{n} a_it_iM_i.$

13. 费马小定理

假如 p 是质数，若 p 不能整除 a，则 a^(p-1) ≡1(mod p)，若 p 能整除 a，则 a^(p-1) ≡0(mod p)。

若 p 是质数，且 a,p 互质，那么 a 的 (p-1) 次方除以 p 的余数恒等于 1。

14.