1 定义

1. 整除
   设 $a,b\in\mathbb{Z}$ 且 $b\neq 0$, 若 $\exists c\in\mathbb{Z}$, s.t.$a=bc$, 则称 a 能被 b 整除，记作 $b\mid a$; 否则，则称 a 不能被 b 整除，记作 $b\nmid a$.

2. 素数与合数
   若正数 a 除了 1 和自身以外，没有别的因子，则称 a 为素数；
   若正数 a 除了 1 和自身以外，还有别的因子，则称 a 为合数。

3. Gauss 函数

   - $[x]$
     $[x]$ 代表不大于 x 的最大整数。
   - $\{x\}$
     $\{x\}=x-[x]$

4. 同余
   对于 $m\in\mathbb{N}_+$, 若 $m\mid a-b$, 则称 a 与 b 关于模 m 同余。记作

   $$a\equiv b \pmod m$$

5. 剩余类
   对于正整数 m 和 r,$0\le r<m$, 集合

   $$K_r(m)=\{qm+r|q\in\mathbb{Z}\}$$

   称为模 m 的一个剩余类。

6. 完全剩余系
   从模 m 的 m 个剩余类中，每个剩余类里取一个数 x_i. 称集合 $\{x_0,x_1,\dots,x_{m-1}\}$ 是模 m 的一个完全剩余系。

7. 最小非负完全剩余系
   $\{0,1,\dots,m-1\}$ 为模 m 的最小非负完全剩余系。

8. 绝对最小完全剩余系
   当 m 为偶数时，$\{-\frac{m}{2},-\frac{m}{2}+1,\dots,\frac{m}{2}-1\}$ 称为模 m 的最小完全剩余系。
   当 m 为奇数时，$\{-\frac{m-1}{2},-\frac{m-3}{2},\dots,\frac{m-1}{2}\}$ 称为模 m 的最小完全剩余系。

9. 简化剩余类
   对于正整数 m 和 r,$0\le r<m,(r,m)=1$, 集合

   $$K_r(m)=\{qm+r|q\in\mathbb{Z}\}$$

   称为模 m 的一个简化剩余类。

10. 简化剩余系
    从模 m 的 $\varphi(m)$ 个简化剩余类中,每个简化剩余类里取一个数 x_i. 称集合 $\{x_0,x_1,\dots,x_{\varphi(m)-1}\}$ 是模 m 的一个简化剩余系。

11. 二次剩余 设 $(n, m) = 1$. 对于同余方程

$$x^2 \equiv n \pmod m$$

若其有解，则称 n 是模 m 的二次剩余。
若其无解，则称 n 是模 m 的二次非剩余。

12. Legendre 符号

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & p \mid n \\ 1 & n\text{是模}p\text{的二次剩余} \\ -1 & n\text{是模}p\text{的二次非剩余} \end{cases}$$

2 定理

1. 整除的简单性质
   - $a \mid b \Leftrightarrow a \mid \pm b$
   - $a \mid b, b \mid c \Leftrightarrow a \mid c$
   - $\forall 1 \le i \le k, b \mid a_i \Rightarrow \forall x_i \in \mathbb{Z}, b \mid a_1x_1 + a_2x_2 + \cdots + a_kx_k$
   - $b \mid a \Rightarrow \forall c \in \mathbb{Z}, bc \mid ac$
   - $b \mid a, a \neq 0 \Rightarrow |a| \le |b|$
   - $b \mid a, a \neq 0 \Rightarrow \dfrac{a}{b} \mid a$
2. 带余除法
   设 $a, b \in \mathbb{Z}, b \neq 0$. 则 $\exists! q, r \in \mathbb{Z}$, s.t.$a = bq + r, 0 \le r < |b|$
3. 辗转相除法
   设 u_0, u_1 是给定的两个整数，$u_1 \neq 0, u_1 \nmid u_0$. 则一定可以在有限步内完成下面操作：
   - $u_0 = q_0u_1 + u_1, 0 < u_2 < |u_1|$
   - $u_1 = q_1u_2 + u_3, 0 < u_3 < |u_2|$
   - $\cdots$
   - $u_k = q_ku_{k+1}$

   且 $u_{k+1} = (u_0, u_1)$.
4. 设 $a_1, a_2, \ldots, a_k \in \mathbb{Z}$, 记 $A = (y \mid y = a_1x_1 + a_2x_2 + \cdots + a_kx_k, x_i \in \mathbb{Z})$,$y_0$ 是 A 中最小正数，则 $y_0 = (a_1, a_2, \ldots, a_k)$.
   Remark
   推论为：
   - 设 d 是 $a_1, a_2, \ldots, a_k$ 的公约数，则 $d \mid (a_1, a_2, \ldots, a_k)$.
   - $(ma_1, ma_2, \ldots, ma_k) = |m| (a_1, a_2, \ldots, a_k)$
   - 若 $\delta = (a_1, a_2, \ldots, a_k)$, 则
     $$\left(\frac{a_1}{\delta}, \frac{a_2}{\delta}, \ldots, \frac{a_k}{\delta}\right) = 1$$
     特别地，$\left(\dfrac{a_1}{(a_1, a_2)}, \dfrac{a_2}{(a_1, a_2)}\right) = 1$

5. Bezout 定理

$$
\begin{gathered}
(a_1, a_2, \ldots, a_k) = 1 \\
\Leftrightarrow \exists x_1, x_2, \ldots, x_k \in \mathbb{Z}, \text{s.t.} a_1x_1 + a_2x_2 + \cdots + a_kx_k = 1
\end{gathered}
$$

6. 整除与最大公因数的关系
   $\forall a, b, c \in \mathbb{Z}$

   - 若 $b \mid ac$ 且 $(a,b)=1$，则 $b \mid c$
   - 若 $b \mid c, a \mid c$ 且 $(a,b)=1$，则 $ab \mid c$
     Remark
     推论：
     - 若 $(a,b)=1$，则 $\forall c \in \mathbb{Z}, (a, bc) = (a, c)$
     - 若 $\forall 1 \leq i \leq n, (a, b_i) = 1,$ 则 $(a, b_1, b_2, \ldots, b_n) = 1$

7. Gauss 函数的性质

   - $$x = [x] + (x)$$
   - $$x - 1 < [x] \leq x < [x] + 1$$
   - $$\forall n \in \mathbb{Z}, [x+n] = [x] + n$$
   - $$
\begin{gathered}
[x] + [y] \leq [x+y] \\
(x) + (y) \geq (x+y)
\end{gathered}
$$
   - $$[-x] = \begin{cases} -[x] - 1 & x \notin \mathbb{Z} \\ -[x] & x \in \mathbb{Z} \end{cases}$$
   - $$a = b\left[\frac{a}{b}\right] + b\left(\frac{a}{b}\right)$$
   - $\forall a, b \in \mathbb{N}_+,$ 不大于 a 的 b 的倍数有 $\left[\frac{a}{b}\right]$ 个

8. Legendre 定理
   若素数 $p \mid n!,$ 且 p 在 $n!$ 中的最高指数为 $\alpha,$ 则

$$\alpha = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$$

9. 同余的性质

   - 下面三个命题等价

    - $a \equiv b \pmod m$
    - $\exists q \in \mathbb{Z}, \text{s.t.} a = b + qm$
    - $\exists q_1, q_2 \in \mathbb{Z}, \text{s.t.} a = q_1 m + r, b = q_2 m + r, 0 \le r < m$
- $a \equiv a \pmod m$
- 若 $a \equiv b \pmod m$，则 $b \equiv a \pmod m$
- 若 $a \equiv b \pmod m, b \equiv c \pmod m$, 则 $a \equiv c \pmod m$
- 已知 $a, b, c, d \in \mathbb{Z}$, 且 $a \equiv b \pmod m, c \equiv d \pmod m$, 则
    - $$a + c \equiv b + d \pmod m$$
    - $$ac \equiv bd \pmod m$$
    - $$a^n \equiv b^n \pmod m$$
    - 对于任意多项式 f
    $$f(a) \equiv f(b) \pmod m$$
- 若 $a \equiv b \pmod m$, 且 $d \mid m$, 则 $a \equiv b \pmod d$
- 若 $a \equiv b \pmod m$, 且 $k \in \mathbb{N}_+$, 则 $ak \equiv bk \pmod{mk}$
- 若 $\forall 1 \le i \le k, a \equiv b \pmod{m_i}$, 则 $a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$
- 若 $a \equiv b \pmod m$, 则 $(a, m) = (b, m)$
- 若 $ac \equiv bc \pmod m$, 且 $(c, m) = 1$, 则 $a \equiv b \pmod m$

10. 完全剩余系的判别法
对于正整数 m，集合 A 是模 m 的完全剩余系的充要条件为：
    (a) $|A| = m$
    (b) $\forall a, b \in A$, 若 $a \ne b$, 则 $a \not\equiv b \pmod m$.

11. 完全剩余系的性质
    - 设 m 是正整数，$(a, m) = 1$,b 是任意整数，若 X 是模 m 的一个完全剩余系，则 $aX + b$ 也是模 m 的一个完全剩余系。
    - 设 $(m_1, m_2) = 1$,X_1 和 X_2 分别是模 m_1 和 m_2 的完全剩余系，则 $m_2 X_1 + m_1 X_2$ 为模 $m_1 m_2$ 的完全剩余系。

12. 简化剩余系的判别法
对于正整数 m，集合 A 是模 m 的简化剩余系的充要条件为：
    (a) $|A| = \varphi(m)$
    (b) $\forall a, b \in A$, 若 $a \ne b$, 则 $a \not\equiv b \pmod m$.
    (c) $\forall a \in A, (a, m) = 1$.

13. 简化剩余系的性质
    设 m 是正整数，$(a,m)=1$，若 X 是模 m 的一个简化剩余系，则 aX 也是模 m 的一个简化剩余系。

14. Euler 函数的性质
    - 设 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},\alpha_i>0,$ 则
    $$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$
    - 若 $(m,n)=1,$ 则 $\varphi(mn)=\varphi(m)\varphi(n)$

15. Euler 定理
    设 m 是大于 1 的整数，$(a,m)=1,$ 则
    $$a^{\varphi(m)}\equiv 1 \pmod m$$

16. Fermat 小定理
    设 p 是素数，$(a,p)=1,$ 则
    $$a^{p-1}\equiv 1 \pmod p$$

17. 二次剩余与二次非剩余的判断方法：
    若
    $$n^{\frac{p-1}{2}}\equiv 1 \pmod p$$
    则 n 是模 p 的二次剩余；
    若
    $$n^{\frac{p-1}{2}}\equiv -1 \pmod p$$
    则 n 是模 p 的二次非剩余。

18. Legendre 符号的性质
    设 p 是奇素数，$n\in\mathbb{Z},$ 则
    - $$\left(\frac{n}{p}\right)\equiv n^{\frac{p-1}{2}} \pmod p$$
    - 若 $n\equiv n_1 \pmod p,$ 则 $\left(\frac{n}{p}\right)=\left(\frac{n_1}{p}\right)$
    - $$\left(\frac{1}{p}\right)=1$$
    - $$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1 & p\equiv 1 \pmod 4\\ -1 & p\equiv 3 \pmod 4\end{cases}$$
    - $$\left(\frac{a_1a_2}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)$$

- $$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1 & p\equiv\pm 1 \pmod 8\\ -1 & p\equiv\pm 3 \pmod 8\end{cases}$$

19. 二次互反律
    p,q 为奇数，且 $(p,q)=1$, 则
    $$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

3 小结论

1. 若 P 为连续 n 个整数之积，则 $n\mid P$.
   Remark
   常见推论：
   $$\forall n\in\mathbb{Z}, 2|n(n+1)$$
2. 对于质数 p 和整数 a, 若 $p\mid a^2$, 则 $p\mid a$ 且 $p^2\mid a^2$
3. 求 a^k 模 m 的余数时，首先找出满足 $a^d\equiv 1 \pmod m$ 的数，再求 k 模 d 的余数。
4. 对于正整数 n, 设 $X=\{a_1,a_2,\dots,a_{\varphi(n)}\}$ 为所有小于它且与它互质的数组成的集合, 则 $\{n-a_1,n-a_2,\dots,n-a_{\varphi(n)}\}=X$
5. 对于正整数 n, 设 $X=\{a_1,a_2,\dots,a_k\}$ 为其所有因子组成的集合, 则 $\left\{\frac{n}{a_1},\frac{n}{a_2},\dots,\frac{n}{a_k}\right\}=X$
6. 求形如 b^n-1 的素因子分解式的方法：
   若素数 $p\mid b^n-1$, 且 $d\mid n$, 则要么 $p\mid b^d-1$, 要么 $p\equiv 1 \pmod n$