一、整除

1. 带余除法　$a = dq + r \quad (0 \le r < b)$　唯一表示
   商　余数
2. 整除定义　$r = 0 \Rightarrow b \mid a$
3. 整除性质

$$a \mid b,\ a \mid c \Rightarrow a \mid mb + nc$$
$$a \mid b \Rightarrow a \mid bc$$
$$a \mid b,\ b \mid c \Rightarrow a \mid c$$

二、同余

1. 定义　$r \equiv a \pmod{d}$
2. 性质

$$a \equiv b \pmod{m} \Leftrightarrow m \mid a - b$$
$$a \equiv b \pmod{m} \text{ 且 } c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$$
$$ac \equiv bd \pmod{m}$$

3. 模 m 算术

$\mathbb{Z}_m$ 上的运算满足：

封闭性
结合律
交换律
单位元：加法 0，乘法 1
加法逆元：$a +_m m - a = 0$

三、素数

1. 定义：　$a \mid p \Leftrightarrow a = 1$ 或 p

2. 性质：

(1) 算术基本定理：存在唯一质因数分解

(2) 存在无限多个素数

(3) 素数定理：$x \to \infty \Rightarrow \pi(x) \to \frac{x}{\ln x}$

(4) 威尔逊定理：$(p-1)! \equiv -1 \pmod p$

四、最大公约数(gcd)与最小公倍数[lcm]

1. 定义：

$(a,b) = \max\{c \mid c|a \wedge c|b\}$

$[a,b] = \min\{c \mid a|c \wedge b|c\}$

2. 性质：

(1) $(a,b)[a,b] = a \cdot b$

(2) 欧几里得算法：$(a,b) = (a, b-a)$

(3) 裴蜀定理：$(a,b) = sa + tb$

$(a,b) = 1 \Leftrightarrow sa+tb = 1$

(4) $a|bc$ 且 $(a,b)=1 \Rightarrow a|c$

(5) $p|ab \Rightarrow p|a$ 或 $p|b$

(6) $ac \equiv bc \pmod m \Rightarrow a \equiv b \pmod{\frac{m}{(m,c)}}$

五、求解同余方程

1. 线性同余方程 $ax \equiv b \pmod m$

2. 性质：

(1) $(a,m)=1$ 且 $m>1 \Rightarrow \exists \bar{a},\ a \cdot \bar{a} \equiv 1 \pmod m$

(2) 中国剩余定理：

模互质序列的线性同余方程组有唯一的模互质序列积的解.

(3) 费马小定理：$a^p \equiv a \pmod p$

若 $(a,p)=1$，则 $a^{p-1}\equiv 1 \pmod p$

(4) 欧拉定理：$a^{\varphi(m)}\equiv 1 \pmod m$

其中，$(a,m)=1$，$\varphi(m)$ 为欧拉函数

$\varphi(m)=m\prod_{p\mid m}(1-\frac{1}{p})$（$p$ 为 m 的质因数）