初等数论

一、整数（略）

二、整除

重点题型：

1. 已知$a,b\in Z$，求最大公约数$d=(a,b)$，并找出整数x,y，使得$ax+by=d$

（1）若$a=b=0$，则$(a,b)=0$，x,y取任意整数均可

（2）若$a=0$，$b\neq 0$，则$(a,b)=|b|$，x任取，y取 $1(b>0)$或$-1(b<0)$

（3）若a,b均不为 0：

若其中有负数，先由$(a,b)=(b,a)=(\pm a,\pm b)$，化为正数，再用 Euclid 算法

【例 1】求$(-1128,9917)$

求最大公约数：

$$
\begin{aligned}
(-1128,9917)&=(9917,1128)=((9917-8\times 1128),1128)=(1128,893)\\
&=((1128-1\times 893),893)=(893,235)=((893-3\times 235),235)\\
&=(235,188)=((235-1\times 188),188)=(188,47)\\
&=((188-4\times 47),47)=(0,47)=47
\end{aligned}
$$

通过上述过程可反推出系数x,y：

$$
\begin{aligned}
47=235-188&=235-(893-3\times 235)\\
&=(1128-893)-(893-3\times(1128-893))\\
&=(1128-(9917-8\times 1128))-(9917-8\times 1128-3\times(1128\\
&-(9917-8\times 1128)))=44\times 1128-5\times 9917\\
&=(-44)\times(-1128)-5\times 9917
\end{aligned}
$$

故$x=-44,y=-5$

（称$ax+by=(a,b)$为 Bezout 公式）

2. 素幂分解法求最大公因式（算术基本定理）

$\forall n \in N^*$，n可分解为有限个素数的乘积（约定 1 为 0 个素数的乘积），即

$$n = {p_1}^{q_1}{p_2}^{q_2}\ldots{p_s}^{q_s}(p_i\text{为素数，}q_i \in N, i = 1,\ldots,s)$$

若已知a, b的素幂分解式

$$a = {p_1}^{q_1}{p_2}^{q_2}\ldots{p_s}^{q_s}, b = {p_1}^{r_1}{p_2}^{r_2}\ldots{p_s}^{r_s}$$

则$(a, b) = {p_1}^{min\{q_1,r_1\}}\ldots{p_s}^{min\{q_s,r_s\}}$（每一个素数幂次对应取最小，允许取 0）

3. 整除基本性质

（1）若$a|b, b|c$，则$a|c$；若$c|a, c|b$，则$c|(ma + nb)$；

（2）带余除法定理：$\forall a, b \in Z, b \neq 0$，$\exists$唯一$q, r \in Z$使$a = bq + r$且 $0 \leq r < |b|$

（3）若p为素数，且p可整除几个整数之积，则p至少可整除其中一个整数

4. 有理数判别法

x为有理数$\Leftrightarrow$存在唯一的$m, n \in Z$，且满足$n > 0, (m, n) = 1$，使得$x = \frac{m}{n}$

$\Leftrightarrow x$可被表为无限循环小数（有限小数视为以 0 为循环节）

注：非零有理数$x = \frac{m}{n}$ 可被分解成素数幂次的乘积（允许幂次为负），对某个素数p和x，引入记号$v_p(x)$，表示x的素幂分解中p的幂次，例如$-\frac{18}{49} = -\frac{2^1 \times 3^2}{7^2}$，则$v_2(-\frac{18}{49}) = 1, v_3(-\frac{18}{49}) = 2, v_5(-\frac{18}{49}) = 0, v_7(-\frac{18}{49}) = -2$

三、同余

基础概念、定理：

（1）同余：若两个整数a,b之间相差m的整数倍，即$a-b=km(k\in Z)$，则称a与b模m同余，记为$a\equiv b \bmod m$（要求模m为正整数）

（2）模m下的剩余类：模m同余的所有整数构成的集合，例如$\{1+3k|k\in Z\}$为模 3 下的一个剩余类，可记作 $1 \bmod 3$（或者 $4 \bmod 3$ 等等）；由定义可知，模m下共有m个不同的剩余类

（3）逆元：若要求$(a,m)=1$，且有$ab\equiv 1 \bmod m$，则称b所在的剩余类$b \bmod m$为a所在的剩余类$a \bmod m$的逆元，记为$a^{-1} \bmod m = b \bmod m$

（注意此处a^{-1}仅仅是一个记号，不表示$\frac{1}{a}$）

（4）同余的基本性质：

满足自反性、对称性、传递性；

可同时进行加减与相乘：

$a\equiv b \bmod m, c\equiv d \bmod m \Leftrightarrow a\pm c\equiv b\pm d \bmod m$和$ac\equiv bd \bmod m$；

消去律：$ab\equiv ac \bmod m \ \Leftrightarrow \ b\equiv c \bmod \frac{m}{(a,m)}$

重点题型：

1. 解一元线性同余方程$ax\equiv b \bmod m$：

Step 1：先使得$(a,m)=1$：

$ax\equiv b \bmod m$

$\frac{a}{(a,m)}x\equiv \frac{b}{(a,m)} \bmod \frac{m}{(a,m)}$ （利用消去律，以及$((a,m),m)=(a,m)$）

$a'x\equiv b' \bmod m'$ （令$a'=\frac{a}{(a,m)}, b'=\frac{b}{(a,m)}, m'=\frac{m}{(a,m)}$，此时必有$(a',m')=1$）

Step 2：求$a' \bmod m$的逆元$a'^{-1} \bmod m$：

因为$(a',m')=1$，先由 Bezout 公式，求出$u,v\in Z$使得$ua'+vm'=1$（写出求

(a', m')的 Euclid 算法过程，之后逆推系数，如例 1 所示），从而$ua' = 1 - vm'$，即$ua' \equiv 1 \bmod m'$，故所求逆元$a'^{-1} \bmod m = u \bmod m$

Step 3：求出x所在的剩余类：

$$x \equiv a'^{-1} b' \bmod m'$$

故原方程的解为$a'^{-1} b' \bmod m'$，再转化为原方程的模m下即可

（即模m'下的剩余类$\{a'^{-1} b' + km' | k \in Z\}$中的任一元素均满足原方程）

【例 2】解同余方程 $14x \equiv 4 \bmod 62$

Step 1：由于 14 与 62 不互素，且$(14,62) = 2$，由消去律，原方程与方程 $7x \equiv 2 \bmod 31$ 同解

Step 2：求 $7 \bmod 31$ 的逆元：

写出求(31,7)的 Euclid 算法过程：

$$(31,7) = ((31 - 4 \times 7), 7) = (7,3) = ((7 - 2 \times 3), 3) = (3,1) = 1$$

故 $1 = 7 - 2 \times 3 = 7 - 2 \times (31 - 4 \times 7) = 9 \times 7 - 2 \times 31$

所求逆元$7^{-1} \bmod 31 \equiv 9 \bmod 31$

Step 3：求出x所在的剩余类：

$x \equiv 9 \times 2 \bmod 31 \equiv 18 \bmod 31$，在模 62 下有两组解 $18 \bmod 62$ 和 $49 \bmod 62$

2. 解一元线性同余方程组（运用中国剩余定理）

设方程组为$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_k \bmod m_k \end{cases}$，要求$(m_1, m_2, \ldots, m_k) = 1$（否则解不唯一），

Step 1：求M和$M_i (i = 1, \ldots, k)$

$M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$（所有模的乘积，即最小公倍数）；

$M_i = \frac{M}{m_i} = m_1 \cdot \ldots \cdot m_{i-1} \cdot m_{i+1} \cdot \ldots \cdot m_k (i = 1, \ldots, k)$（除了第$i$个以外的模乘积）

Step 2：求出M_i在模m_i下的逆元$t_i \bmod m_i$ $(i = 1, \ldots, k)$

（因为M_i是从M中去除m_i后得到的，且所有m_i之间互素，故M_i和m_i一定互素）

Step 3：表示出方程组的解集

$$x \equiv (a_1M_1t_1 + a_2M_2t_2 + \ldots + a_kM_kt_k) \bmod M$$

【例 3】解同余方程组$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \end{cases}$

Step 1：求M和$M_i(i = 1,2)$

$$M = 15, M_1 = 5, M_2 = 3$$

Step 2：求出M_1在模m_1下的逆元和M_2在模m_2下的逆元

①求 5 mod 3 的逆元：

列出求(5,3)的 Euclid 算法过程并逆推出 Bezout 公式：

$$(5,3) = ((5-3),3) = (3,2) = ((3-2),2) = (2,1)$$

$$1 = 3 - 2 = 3 - (5-3) = 2 \times 3 + (-1) \times 5$$

故 5 mod 3 的逆元为$-1 \bmod 3$

②同理求得 3 mod 5 的逆元为 2 mod 5

Step 3：表示出方程组的解集

$$x \equiv (2 \times 5 \times (-1) + 3 \times 3 \times 2) \bmod 15 \equiv 8 \bmod 15$$

（即$x = 8 + 15k(k \in Z)$时，方程组均成立）

四、乘性函数

基础概念、定理：

（1）乘性与完全乘性：

f为乘性函数：$\forall a,b$满足$(a,b)=1$，都有$f(ab)=f(a)f(b)$

f为完全乘性函数：$\forall a,b\in Z$，都有$f(ab)=f(a)f(b)$

（2）完全剩余系、既约剩余类、既约剩余系：

①**完全剩余系：**由剩余类的定义可知，模m下共有m个不同的剩余类，在这些剩余类中各取一个数作为代表元，则这些代表元构成的集合是完全剩余系

例：模 3 下共有 3 个不同的剩余类$\{1+3k|k\in Z\},\{2+3k|k\in Z\},\{3+3k|k\in Z\}$，令$k=0$，分别取 1,2,3 为代表元（也可令$k=1,2,3$，取 4,8,12，等等），则$\{1,2,3\}$是模 3 下的一个完全剩余系。

注：由定义可知，任取连续的m个整数，必构成一个模m下的完全剩余系。

②**既约剩余类：**若$(a,m)=1$，则称a所在的剩余类为模m下的既约剩余类

例：$(3,8)=1$，则 3 所在的剩余类$3 \bmod 8=\{3+8k|k\in Z\}$为模 8 下的一个既约剩余类；而$(4,8)=2$，则 4 所在的剩余类$4 \bmod 8=\{4+8k|k\in Z\}$不是模 8 下的一个既约剩余类。

由定义可知，素数模p下有$(p-1)$个不同的既约剩余类。

③**既约剩余系：**从模m下所有不同的既约剩余类中，各取一个元素作为“代表元”，组合在一起构成的集合（和完全剩余系类似）

例：模 18 下的一个既约剩余系为$\{1,5,7,11,13,17\}$

由定义可知，素数模p下的既约剩余系中有$(p-1)$个元素

（3）几种常见的乘性函数：

① Euler 函数$\varphi(n)$：模n下的既约剩余系中的元素个数

由定义可知，若p为素数，则$\varphi(p) = p - 1$，$\varphi(p^e) = p^e - \frac{p^e}{p}$

（任意连续p个整数中恰有一个能被p整除，且其余与p互素，取由p^e个连续整数构成的完全剩余系，则其中去除掉$\frac{p^e}{p}$个能被p整除的数之后，剩下的均与p互素，构成既约剩余系，因此既约剩余系的元素个数为$p^e - \frac{p^e}{p}$）

② 算术函数f的和函数$S_f(n)$：正整数n的所有正因子用f作用之后求和

$$S_f(n) = \sum_{d|n,d>0} f(d)$$

例：$S_\varphi(n) = \sum_{d|n,d>0} \varphi(d) = n$

证明：将 1~n按照“与n的最大公约数”分类，每个d对应一类，考察每一个“类别d”的元素个数，设$(a,n) = d$，则a必为d的正整数倍kd，因$(a,n) = (kd,n) = d$，由定理 2.10 知$(k,\frac{n}{d}) = 1$，从而可以取的k均与$\frac{n}{d}$互素且不超过$\frac{n}{d}$，因而由 Euler 函数定义，“类别d”中的元素共有$\varphi(\frac{n}{d})$个，即$n = \sum_{d|n,d>0} \varphi(\frac{n}{d})$，因为$d$遍历$n$的所有正因子时，$\frac{n}{d}$也遍历了$n$的所有正因子，故$n = \sum_{d|n,d>0} \varphi(\frac{n}{d}) = \sum_{d|n,d>0} \varphi(d) = S_\varphi(n)$

注：S_f是乘性的充要条件是f是乘性的，若已知n的素幂分解，则可先求素因子的函数值再相乘以简化运算

③ 除子函数$\sigma_s(n)$：正整数n的所有正因子的s次幂之和（$f(n) = n^s$的和函数）

$$\sigma_s(n) = \sum_{d|n,d>0} d^s$$

注：此处$f(n) = n^s$为乘性的，故$\sigma_s(n)$是乘性的，若已知n的素幂分解，则可先求素因子的函数值再相乘以简化运算

④ Möbius 函数$\mu(n)$：

$$\mu(n) = \begin{cases} 1,\ n = 1 \\ 0,\ n\text{有平方因子（}n\text{的素幂分解中有幂次} \geq 2\text{ 的素数）} \\ -1,\ n\text{无平方因子，是奇数个不同素数的乘积} \\ 1,\ n\text{无平方因子，是偶数个不同素数的乘积} \end{cases}$$

注：$\mu(n)$是乘性的，因此和函数$S_\mu(n)$也是乘性的，且$S_\mu(n) = \begin{cases} 1, n = 1 \\ 0, n > 1 \end{cases}$

（4）Möbius 反演公式

函数f为算术函数，则$\forall n \in N^*$，有

$$f(n)=\sum_{d|n}\mu(d)S_f(\frac{n}{d})$$

【例 4】求 1~100 中，与 100 互素的数的个数

求$\varphi(100)$的值即可，取f为 Euler 函数，注意到$S_\varphi(n)=\sum_{d|n}\varphi(d)=n$

运用反演公式：$\varphi(100)=\sum_{d|100}\mu(d)S_\varphi(\frac{n}{d})=\sum_{d|100}\mu(d)\frac{n}{d}$

100 的因数有：1,2,4,5,10,20,25,50,100，$\mu(1)=1,\mu(2)=-1,\mu(4)=0,\mu(5)=-1,\mu(10)=1,\mu(20)=0,\mu(25)=0,\mu(50)=0,\mu(100)=0$，故

$$\varphi(100)=1\times100+(-1)\times50+(-1)\times20+1\times10=40$$

五、原根

引例：幂运算的余数循环现象

$$2^0 \equiv 1 \bmod 7, 2^1 \equiv 2 \bmod 7, 2^2 \equiv 4 \bmod 7$$
$$\cdots$$
$$2^{3k} \equiv 1 \bmod 7, 2^{3k+1} \equiv 2 \bmod 7, 2^{3k+2} \equiv 4 \bmod 7$$

2 的幂次的模 7 余数以 3 为周期变化，而 3 的幂次的模 7 余数以 6 为周期变化

$$3^0 \equiv 1 \bmod 7, 3^1 \equiv 3 \bmod 7, 3^2 \equiv 2 \bmod 7, 3^3 \equiv 6 \bmod 7, 3^4 \equiv 4 \bmod 7, 3^5 \equiv 5 \bmod 7$$
$$\cdots$$
$$3^{6k} \equiv 1 \bmod 7, 3^{6k+1} \equiv 3 \bmod 7, 3^{6k+2} \equiv 2 \bmod 7, 3^{6k+3} \equiv 6 \bmod 7, 3^{6k+4} \equiv 4 \bmod 7, 3^{6k+5} \equiv 5 \bmod 7$$

3 的幂次的模 7 余数 1,2,3,4,5,6 构成 7 的一个既约剩余系，是模 7 的一个原根

基础概念、定理：

（1）阶数$\mathrm{ord}_m(a)$的定义：

要求$(a, m) = 1$，定义使得$a^n \equiv 1 \bmod m$成立的最小的正整数n为$a \bmod m$的阶，

记为$\mathrm{ord}_m(a)$

注：因为n为零时该式恒成立，这个最小正整数就是a的幂次的余数的循环周期，

例如在引例中，2 的幂次的模 7 余数的变化周期是 3，$\mathrm{ord}_7(2) = 3$

（2）Euler 定理：

要求$(a, m) = 1 (m > 1)$，则必有$a^{\varphi(m)} \equiv 1 \bmod m$

注：但$\varphi(m)$只是使模m余 1 的一个正整数，未必是最小的正整数，例如引例中，

$2^{\varphi(7)} = 2^6 \equiv 1 \bmod 7$，但 3 才是使得$2^n \equiv 1 \bmod 7$ 的最小正整数，

即：$\varphi(m) \geq \mathrm{ord}_m(a)$

（3）原根的定义：

$(a, m) = 1$，若a的幂次的所有模m余数构成一个既约剩余系，称a为模m的原根。

注：$\varphi(m)$是m的一个既约剩余系包含元素的个数，由定义，原根a的幂次余数共

有$\varphi(m)$个，变化周期为$\varphi(m)$，也就是$\varphi(m) = \mathrm{ord}_m(a) \Leftrightarrow a$为模$m$的原根。

例如：3 为模 7 的一个原根，而 2 不是模 7 的一个原根

【说明】一般说“a为模m的原根”，是指a所在的剩余类中的每个元素都是模m的原根，也就是$a+km(k\in Z)$实际上都符合原根的定义，因此原根严格意义上是一个剩余类，而不是一个数，原根的个数，实际上是指剩余类的个数。

例如：模 7 有 3 和 5 两个原根，并不是指a只有取 3 和 5 时才是原根，而是指a为 3 和 5 所在的剩余类$\{3+7k|k\in Z\},\{5+7k|k\in Z\}$中的任一元素时都是原根，比如$a=10,a=12$ 等等，但是在剩余类意义下，a只有两种取值。

（4）原根的基本性质：

① $\mathrm{ord}_m(a)|\varphi(m)$

（因为$a^{\varphi(m)}$是模m余 1 的，且a^0也是模m余 1 的，所以 0 和$\varphi(m)$之间相隔了若干个幂次余数循环周期，即$\varphi(m)=k\cdot\mathrm{ord}_m(a)(k=1,2,\ldots)$）

② 若a为模m的原根，则a的 1~$\varphi(m)$次幂构成了模m的一个既约剩余系

$$\{a,a^2,\ldots,a^{\varphi(m)}\}$$

重点题型：

1. 给定一个正整数m，判断模m是否有原根，若有原根，求解出原根

Step 1 原根的存在性判别法：

m为大于 1 的正整数，则仅有以下形式的模数m才有原根

①$m=2,4$；②$m=p^k(k=1,2,\ldots)$；③$m=2\cdot p^k(k=1,2,\ldots)$

（其中p为**奇素数**）

Step 2 若原根存在，求$\varphi(m)$：

Case 1 $m=2,4$ 时，$\varphi(m)$分别为 1,2

Case 2 $m=p^k$（p为奇素数）时，$\varphi(p^k)=p^k-\frac{p^k}{p}$

Case 3 $m=2\cdot p^k$（p为奇素数）时，由于φ是乘性函数，且 2 和p^k互素，$\varphi(2\cdot p^k)=\varphi(2)\cdot\varphi(p^k)=\varphi(p^k)=p^k-\frac{p^k}{p}$

Step 3 对$\varphi(m)$进行素数分解

求得$\varphi(m)={p_1}^{q_1}{p_2}^{q_2}\ldots{p_s}^{q_s}$，列出其所有素因数$p_i(i=1,\ldots,s)$

Step 4 试验法试出一个原根g

先列出m的一个既约剩余系（即与m互素且不超过m的所有数），从小到大排列，再逐一判断，先判断a是否与模m互素，若不互素，则跳过；若互素，则只需对每个素因数p_i，验证$a^{\frac{\varphi(m)}{p_i}}\equiv 1 \bmod m$是否成立。

（如果担心遗漏，也可以对每一个小于$\varphi(m)$的正整数n验证$a^n\equiv 1 \bmod m$）

若有任意一个成立，则说明$\varphi(m)>\mathrm{ord}_m(a)$，$a$**不是原根，跳过。**

直到找到符合条件的一个原根为止。

Step 5 通过一个原根g找到剩余的原根

若已知g为原根，则模m的所有原根为

集合$\{g^r|1\le r\le\varphi(m),(r,\varphi(m))=1\} \pmod m$对应的剩余系

推论：在剩余类意义下，模m的原根个数要么为 0，要么为$\varphi(\varphi(m))$

【例 5】模 18 是否有原根？如果有，求出所有原根

Step 1 $m=18=2\times 3^2$，故存在原根

Step 2 $\varphi(2\times 3^2)=\varphi(3^2)=3^2-\frac{3^2}{3}=6$

Step 3 对 6 进行素因数分解，得 $6=2\times 3$，素因数为 2,3

Step 4 列出 18 的一个既约剩余系为$\{1,5,7,11,13,17\}$，进行试验：

对 1 进行试验：$1^{\frac{6}{2}}=1\equiv 1 \bmod 18$，不是原根；

对 5 进行试验：$5^{\frac{6}{2}}=125\equiv 17 \bmod 18$；$5^{\frac{6}{3}}=25\equiv 7 \bmod 18$，故 5 是原根

Step 5 $\varphi(18)=6$，满足$(r,\varphi(18))=1$ 且不超过$\varphi(m)$的正整数r有 1,5，故

$5^1\equiv 5 \bmod 18$ 和$5^5=3125\equiv 11 \bmod 18$ 为模 18 的所有原根，即

$a=5+18k(k\in Z)$或$a=11+18k(k\in Z)$时，a为 18 的原根

2. 给定m,n（m存在原根），求解同余方程$x^n\equiv 1 \bmod m$

Step 1 按照上述方法求出m的一个原根a

Step 2 令$(\varphi(m),n)=d$，则在剩余类意义下，方程的全部解为：

$$x\equiv a^{\frac{t\varphi(m)}{d}} \bmod m(t=0,1,\ldots,d-1)$$

简要证明：因为a为原根，故$\{a^k|k=1,\ldots,\varphi(m)\}$构成$m$的一个既约剩余系，即每一个$a^k$都和$m$互素，因为$x$必与$m$互素，从而$x$的解只可能包含在上述集合中；将$a^k$代入原方程得$a^{nk}\equiv 1 \bmod m$，由原根定义，$a$的阶为$\varphi(m)$，故$\varphi(m)|nk$，即$nk\equiv 0 \bmod \varphi(m)$，由消去律得$k\equiv 0 \bmod \frac{\varphi(m)}{d}$，也就是$k=t\frac{\varphi(m)}{d}$，从而代入$x\equiv a^k \bmod m$得全部解为$x\equiv a^{\frac{t\varphi(m)}{d}} \bmod m(t=0,1,\ldots,d-1)$，恰有$d$个解

【例 6】解同余方程$x^3\equiv 1 \bmod 18$

Step 1 求得 18 的一个原根为 5

Step 2 求得$\varphi(18)=\varphi(9)=3^2-3=6$，则$d=(\varphi(18),3)=3$，共有 3 个解

$$x\equiv 5^{2t} \bmod 18(t=0,1,2)$$

即$x\equiv 1 \bmod 18, x\equiv 25\equiv 7 \bmod 18, x\equiv 625\equiv 13 \bmod 18$

六、二次互反律

基础概念、定理：

（1）二次剩余与二次非剩余：

p为奇素数，且$(a,p)=1$，若二次同余方程$x^2\equiv a \bmod p$有解，称a为模p下的二次剩余，否则为二次非剩余；

（2）二次同余方程$x^2\equiv a \bmod p$的解的个数：若$(a,p)=1$，p为奇素数，则该同余方程要么无解，要么有两个解（在模p的剩余类意义下）

（3）Legendre 符号$(\frac{a}{p})$：注意其中的"$\frac{a}{p}$"不表示分数

$$(\frac{a}{p})=\begin{cases}0,(a,p)\neq 1\\ 1,a\text{为模}p\text{下的二次剩余}\\ -1,a\text{为模}p\text{下的二次非剩余}\end{cases}$$

由定义知，若$a\equiv b \bmod p$，则$(\frac{a}{p})=(\frac{b}{p})$

（4）$(\frac{a}{p})$在a为正整数时为完全乘性函数，因而若干个与p互素的正整数相乘时，若其中共有奇数个二次非剩余，则乘积为二次非剩余，否则乘积为二次剩余

（5）推广的 Legendre 符号$(\frac{a}{m})$：定义同上，**但只需要m为奇数即可**，可以证明推广的 Legendre 符号（称为 Jacobi 符号）仍然有和 Legendre 符号相同的性质（称为 Jacobi 二次互反律）

重点题型：

1. 判断方程$x^2\equiv a \bmod p$解的个数（计算推广的 Legendre 符号）

通过以下定理进行计算，若求得的结果为 1，说明方程有解

①Euler 准则：$(\frac{a}{p})\equiv a^{\frac{p-1}{2}} \bmod p$（当$p$较大时计算困难）

②同余变换：若$a\equiv b \bmod p$，则$(\frac{a}{p})=(\frac{b}{p})$，即$(\frac{a}{p})=(\frac{a+kp}{p})(k\in Z)$

③完全乘性：$(\frac{ab}{p})=(\frac{a}{p})\cdot(\frac{b}{p})$，若已知素幂分解$n=\pm p_1{}^{q_1}p_2{}^{q_2}\dots p_s{}^{q_s}$，则有：

$(\frac{n}{p})=(\frac{\pm1}{p})(\frac{p_1}{p})^{q_1}\dots(\frac{p_s}{p})^{q_s}$

④第一、第二附加律：

$(\frac{1}{p})=1$；$(\frac{-1}{p})=(-1)^{\frac{p-1}{2}}=\begin{cases}1, p\equiv 1 \bmod 4\\ -1, p\equiv 3 \bmod 4\end{cases}$；

$(\frac{2}{p})=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, p\equiv\pm 1 \bmod 8\\ -1, p\equiv\pm 3 \bmod 8\end{cases}$

⑤Gauss 二次互反律：$(\frac{q}{p})=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}(\frac{p}{q})$

【例 7】判断方程$x^2\equiv 713 \bmod 1009$ 的解的个数

将$(\frac{713}{1009})$视为 Jacobi 符号，由 Jacobi 互反律得：

$$(\frac{713}{1009})=(-1)^{\frac{1008}{2}\times\frac{712}{2}}(\frac{1009}{713})=(\frac{1009}{713})=(\frac{1009-713}{713})=(\frac{296}{713})$$

$$=(\frac{2^3}{713})(\frac{37}{713})=(\frac{2}{713})^3(\frac{37}{713})=1^3(\frac{37}{713})=(-1)^{\frac{36}{2}\times\frac{712}{2}}(\frac{713}{37})$$

$$=(\frac{713}{37})=(\frac{713-37\times 19}{37})=(\frac{10}{37})=(\frac{2}{37})(\frac{5}{37})=-(\frac{5}{37})$$

$$=-(-1)^{\frac{36}{2}\times\frac{4}{2}}(\frac{37}{5})=-(\frac{37}{5})=-(\frac{37-7\times 5}{5})=-(\frac{2}{5})$$

由 Euler 准则，$(\frac{2}{5})\equiv 2^{\frac{5-1}{2}}\equiv 4\equiv -1 \bmod 5$，$(\frac{2}{5})=-1$，故$(\frac{713}{1009})=-(\frac{2}{5})=1$，方程$x^2\equiv 713 \bmod 1009$ 有两个解。

七、p-adic 数

重点（定理内容要能够叙述）：强三角不等式、p-adic 幂级数展开、Hensel 引理（判断方程$x^2\equiv a \bmod p$在Z_p中是否有解）、定理 7.18

作业题参考答案（仅作参考）：

【1】练习 2.7

证明:

假设 $\sqrt{3}$ 为有理数，由练习2.6，$\exists$ 唯一的 $m,n\in\mathbb{Z}$，$(m,n)=1$ 且 $n>0$，使得 $\sqrt{3}=\frac{m}{n}$，故 $m^2=3n^2$，$3\mid m^2$，因为3为素数，由引理2.24，必有 $3\mid m$，$\exists c\in\mathbb{Z}$ 使 $m=3c$。

故 $3n^2=m^2=9c^2$，$n^2=3c^2$，$3\mid n^2$，同理可知 $3\mid n$。

从而 $3\mid m$ 且 $3\mid n$，3为 m,n 的公因数，这与 $(m,n)=1$ 矛盾。

【2】练习 3.12

证明:

对 $(x+y)^p$ 展开，有 $(x+y)^p=\sum_{k=0}^{p}C_p^k x^k y^{p-k}$

要证 $(x+y)^p\equiv x^p+y^p \bmod p$，只需证对应项系数同余。

即证 $\begin{cases} C_p^k\equiv 1 \bmod p & (k=0 \text{ 或 } k=p) \\ C_p^k\equiv 0 \bmod p，即\ p\mid C_p^k & (k=1,2,\cdots,p-1) \end{cases}$

$k=0$ 或 $k=p$ 时，$C_p^k=1$，显然有 $C_p^k\equiv 1 \bmod p$.

$k=1,2,\cdots,p-1$ 时，

$C_p^k=\frac{p!}{k!(p-k)!}$ $\cancel{\frac{(p-k+1)(p-k+2)\cdots(p-1)\cdot p}{1\times 2\times 3\times\cdots\times k}}$ $\Rightarrow p!=C_p^k\cdot k!\cdot(p-k)!$

故 $p\mid C_p^k\cdot k!\cdot(p-k)!$，由 $1\le k\le p-1$ 知，$p\nmid k!(p-k)!$，(p为素数) ~~故 $p\mid C_p^k$~~

故 $p\mid C_p^k$，从而命题证毕。

【3】练习 4.13

证明:

取2021个相异素数 $q_0,q_1,\cdots,q_{2020}$

则 $q_i^2\ (i=0,\cdots,2020)$ 两两互素，由中国剩余定理，同余方程组

$n\equiv -i \bmod q_i^2\ (i=0,1,\cdots,2020)$

在模 $M=\prod_{i=0}^{2020}q_i^2$ 下有唯一解，即 $\exists n_0\in\mathbb{Z}$ 且唯一，使 $0\le n_0<M$ 且 n_0 满足方程组，故 $\forall i=0,1,\cdots,2020$，$q_i^2\mid n_0+i$，

从而 n_0+i 有平方因子，$\mu(n_0+i)=0$，从而 $\sum_{i=0}^{2020}\mu(n_0+i)=0$ #

再取无穷多个 $n_k=n_0+kM$，$(k\in\mathbb{N}^+)$，

则 $\forall k\in\mathbb{N}^+$，n_k 满足同余方程组，故 $\sum_{i=0}^{2020}\mu(n_k+i)=0\ (\forall k\in\mathbb{N}^+)$

即存在无穷多个正整数 n_k，满足条件。

【4】练习 6.11

证明:

记集合 $R=\{a \mid a\in\{1,2,\cdots,p-1\}, a$ 为模 p 的二次剩余$\}$，则 R 中有 $\frac{p-1}{2}$ 个元素，由 $p\equiv 1 \mod 4$ 知 $\frac{p-1}{2}$ 为偶数，R 中元素个数为偶.

且由第一附加律，$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=1$，故 -1 为模 p 的二次剩余.

$\forall a\in R$，由于 -1 为二次剩余，$\exists y\in \mathbb{Z}$ s.t. $y^2\equiv -1 \mod p$，故

$-a\equiv y^2 a\equiv (ya)^2 \mod p$，$-a$ 也为二次剩余，$p-a$ 也为二次剩余.

即：$\forall a\in R$，$p-a\in R$，从而

$$\sum_{x\in R} x = \frac{1}{2}\sum_{a\in R}(a+(p-a)) = \frac{1}{2}p\cdot|R| = \frac{p}{2}\cdot\frac{p-1}{2} = \frac{p(p-1)}{4}$$

即：~~模p的~~ 在 $1,2,\cdots,p-1$ 中，模 p 的二次剩余之和为 $\frac{p(p-1)}{4}$.

【5】练习 7.11

1. 在 $\mathbb{Q}$ 上无解

方程的解为 $x=\pm\sqrt{2},\pm\sqrt{17},\pm\sqrt{34}$。由于 $\sqrt{2},\sqrt{17},\sqrt{34}$ 均为无理数（例如，由算术基本定理，这些数不能表示为有理数），因此这些解都不在 $\mathbb{Q}$ 中。故方程在 $\mathbb{Q}$ 上无解。

2. 在 $\mathbb{Q}_v$ 上均有解

需证明对于每个 $v=\infty$ 或 p（素数），方程在 $\mathbb{Q}_v$ 中至少有一个解。

(a) 当 $v=\infty$，即 $\mathbb{R}$

由于 $\sqrt{2},\sqrt{17},\sqrt{34}$ 都是实数，方程在 $\mathbb{R}$ 中有解。

(b) 当 $v=p$，即 $\mathbb{Q}_p$

需证明对每个素数 p，至少一个 of $\sqrt{2},\sqrt{17},\sqrt{34}$ 存在于 $\mathbb{Q}_p$ 中。这等价于证明至少一个 of $2,17,34$ 是 $\mathbb{Q}_p$ 中的平方数。

根据 p-进数的理论（见第7章），一个非零有理数 a 在 $\mathbb{Q}_p$ 中有平方根当且仅当在 p-进绝对值下，a 可写为 $a=p^{2k}u$，其中 u 是 p-进单位（即 $|u|_p=1$），且 u 是模 p 的二次剩余（对于奇素数 p）。对于 $p=2$，条件更严格：u 必须满足 $u\equiv 1 \pmod 8$。

考虑素数 p 的不同情况：

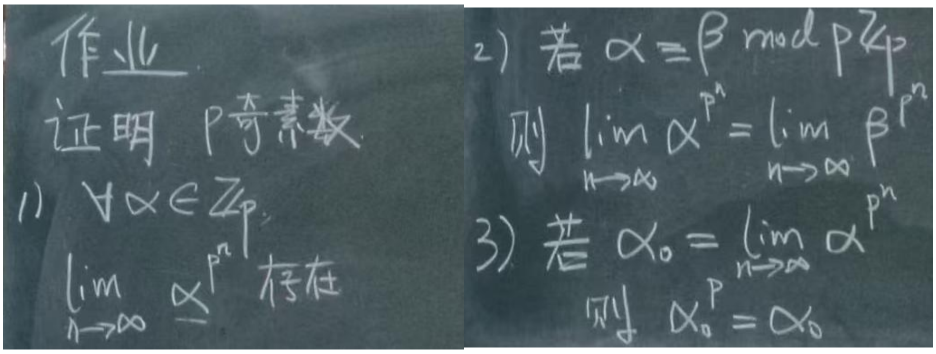
- **当 $p=2$:**
  - $2=2^1\cdot 1$，$v_2(2)=1$ 为奇数，故 2 不是 $\mathbb{Q}_2$ 中的平方数。
  - 17：$v_2(17)=0$，且 $17\equiv 1 \pmod 8$，故 17 是 $\mathbb{Q}_2$ 中的平方数（由 Hensel 引理，方程 $x^2=17$ 在 $\mathbb{Z}_2$ 中有解）。因此 $\sqrt{17}\in\mathbb{Q}_2$，方程有解。
- **当 $p=17$:**
  - $17=17^1\cdot 1$，$v_{17}(17)=1$ 为奇数，故 17 不是 $\mathbb{Q}_{17}$ 中的平方数。
  - 2：$v_{17}(2)=0$，且由二次互反律，2 是模 17 的二次剩余（因为 $17\equiv 1 \pmod 8$），故 2 是 $\mathbb{Q}_{17}$ 中的平方数。因此 $\sqrt{2}\in\mathbb{Q}_{17}$，方程有解。

- **当 p 为其他奇素数**:
  考虑 Legendre 符号 $\left(\frac{2}{p}\right)$ 和 $\left(\frac{17}{p}\right)$。
  - 如果 $\left(\frac{2}{p}\right) = 1$，则 2 是模 p 的二次剩余，故 $\sqrt{2} \in \mathbb{Q}_p$。
  - 如果 $\left(\frac{17}{p}\right) = 1$，则 $\sqrt{17} \in \mathbb{Q}_p$。
  - 如果 both $\left(\frac{2}{p}\right) = -1$ 和 $\left(\frac{17}{p}\right) = -1$，则

$$\left(\frac{34}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{17}{p}\right) = (-1)(-1) = 1,$$

    故 34 是模 p 的二次剩余，因此 $\sqrt{34} \in \mathbb{Q}_p$。
    综上，对任何奇素数 p，至少一个 of $2, 17, 34$ 是二次剩余模 p，由 Hensel 引理（定理 7.17），对应平方根存在于 $\mathbb{Q}_p$ 中，方程有解。

【6】



1) 对任意 $\alpha \in \mathbb{Z}_p$，极限 $\lim_{n\to\infty} \alpha^{p^n}$ 存在

考虑两种情况:

- **情况 1:** $\alpha \in p\mathbb{Z}_p$，即 $v_p(\alpha) \geq 1$。
  则 $v_p(\alpha^{p^n}) = p^n v_p(\alpha) \to \infty$ 当 $n \to \infty$，
  所以 $|\alpha^{p^n}|_p = p^{-v_p(\alpha^{p^n})} \to 0$，
  故 $\alpha^{p^n} \to 0$ 在 $\mathbb{Z}_p$ 中。
  因此极限存在且为 0。
- **情况 2:** $\alpha \in \mathbb{Z}_p^*$，即 α 是 p-adic 单位。
  由于 $\mathbb{Z}_p^* \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)$，其中 μ_{p-1} 是 $p-1$ 次单位根群，
  存在唯一的 $\omega \in \mu_{p-1}$ 和 $u \in 1 + p\mathbb{Z}_p$ 使得 $\alpha = \omega u$。
  那么 $\alpha^{p^n} = \omega^{p^n} u^{p^n}$。
  由于 $\omega^{p-1} = 1$，有 $\omega^p = \omega$，从而 $\omega^{p^n} = \omega$ 对所有 n。

现在考虑 u^{p^n}。
令 $u = 1 + pv$ 其中 $v \in \mathbb{Z}_p$。
我们claim $v_p(u^{p^n} - 1) \geq n + 1$。
证明由归纳法:

- $n = 0$: $v_p(u - 1) \geq 1$;
- 假设 $v_p(u^{p^n} - 1) \geq n + 1$，则 $u^{p^n} = 1 + p^{n+1}w$ 对于某个 $w \in \mathbb{Z}_p$。
  于是

$$u^{p^{n+1}} = (u^{p^n})^p = (1 + p^{n+1}w)^p = 1 + p \cdot p^{n+1}w + \binom{p}{2}p^{2(n+1)}w^2 + \cdots$$

由于 p 是奇素数，$v_p\left(\binom{p}{k}\right) \geq 1$ 对于 $1 \leq k \leq p-1$，
因此 $v_p(u^{p^{n+1}}-1) \geq n+2$。
所以 $u^{p^n} \to 1$ 当 $n \to \infty$。
从而 $\alpha^{p^n} = \omega u^{p^n} \to \omega \cdot 1 = \omega$。
因此极限存在且等于 ω，即 α 的 Teichmüller 代表元。

综上，极限 $\lim_{n\to\infty} \alpha^{p^n}$ 总是存在。

2) 若 $\alpha \equiv \beta \mod p\mathbb{Z}_p$，则 $\lim_{n\to\infty} \alpha^{p^n} = \lim_{n\to\infty} \beta^{p^n}$

由假设 $\alpha \equiv \beta \mod p\mathbb{Z}_p$，有两种情况：

- 如果 $\alpha, \beta \in p\mathbb{Z}_p$，则由部分 (1) 知 $\lim \alpha^{p^n} = 0$ 和 $\lim \beta^{p^n} = 0$，故相等。
- 如果 $\alpha, \beta \in \mathbb{Z}_p^*$，则 $\alpha \equiv \beta \mod p$ 意味着它们的 Teichmüller 代表元相同，即 $\omega(\alpha) = \omega(\beta)$。
  由部分 (1) 知 $\lim \alpha^{p^n} = \omega(\alpha)$ 和 $\lim \beta^{p^n} = \omega(\beta)$，故相等。

因此，在两种情况下，极限相等。

3) 若 $\alpha_0 = \lim_{n\to\infty} \alpha^{p^n}$，则 $\alpha_0^p = \alpha_0$

由部分 (1)，α_0 要么为 0，要么为 Teichmüller 代表元 ω。

- 如果 $\alpha_0 = 0$，则 $\alpha_0^p = 0^p = 0 = \alpha_0$。
- 如果 $\alpha_0 = \omega$，则由 Teichmüller 代表元的性质，$\omega^p = \omega$，所以 $\alpha_0^p = \alpha_0$.

因此，总有 $\alpha_0^p = \alpha_0$.

计算题自测

1. 求-522和1422的最大公约数d，并求一组整数x,y，使得

$$-522x+1422y=d$$

2. 解同余方程$6x\equiv 4 \bmod 10$

3. 解同余方程组$\begin{cases}x\equiv 2 \bmod 5\\ x\equiv 4 \bmod 8\end{cases}$

4. 计算以下函数值：

（1）$\varphi(24)$；（2）$S_{\varphi}(20)$；（3）$\sigma_2(18)$；

（4）$v_2(-48)$；（5）$\sum_{i=1}^{6}\mu(i)$；（6）$\mathrm{ord}_{25}(7)$

5. 求模 22 的所有原根：

6. 解方程$x^3\equiv 1 \bmod 7$

7. 判断方程$x^2\equiv 137 \bmod 421$的解的个数

参考答案：

1. $(-522, 1422) = 18$；$-522 \times (-30) + 1422 \times (-11) = 18$

2. $4, 9 \bmod 10$

3. $12 \bmod 40$

4.（1）8 （2）20 （3）455 （4）4 （5）-1 （6）4

5. $7, 13, 17, 19 \pmod{22}$

6. $1, 2, 4 \bmod 7$

7. 0（无解）