# 高一竞赛数论专题

## 11.模为素数的二次剩余

设素数 $p>2,d$ 是整数, $p\nmid d$. 如果同余方程 $x^2\equiv d(\mathrm{mod}\,p)$ 有解,则称 $d$ 是模 $p$ 的二次剩余,若无解,则称 $d$ 是模 $p$ 的二次非剩余.

注意到 $p\mid d$. 则同余方程 $x^2\equiv d\equiv 0(\mathrm{mod}\,p)$ ,则其有且只有一解 $x\equiv 0(\mathrm{mod}\,m)$.

若 $p=2,$ 且 $p\quad d$. 则同余方程 $x^2\equiv d(\mathrm{mod}\,2)$ 为 $x^2\equiv 1(\mathrm{mod}\,2)$ 有且只有一解 $x\equiv 1(\mathrm{mod}\,2)$.

1.设素数 $p>2$ ,证明在模 $p$ 的一个既约剩余系中,恰有 $\frac{p-1}{2}$ 个模 $p$ 的二次剩余, $\frac{p-1}{2}$ 个模 $p$ 的二次非剩余.此外,若 $d$ 是模 $p$ 的二次剩余,则同余方程 $x^2\equiv d(\mathrm{mod}\,p)$ 的解数为 2.

2.(Euler 判别法)设素数 $p>2,p\quad d$ ,那么, $d$ 是模 $p$ 的二次剩余的充要条件是 $d^{\frac{p-1}{2}}\equiv 1(\mathrm{mod}\,p)$; $d$ 是模 $p$ 的二次非剩余的充要条件是 $d^{\frac{p-1}{2}}\equiv -1(\mathrm{mod}\,p)$.

3. 若素数 $p>2,$ 证明： $-1$ 是模 $p$ 的二次剩余的充要条件是 $p\equiv 1(\mathrm{mod}\,4).$

当 $p\equiv 1(\mathrm{mod}\,4)$ 时, $\left(\pm\left(\frac{p-1}{2}\right)!\right)^2\equiv -1(\mathrm{mod}\,p).$

4.设 $p$ 是奇素数,证明： $1,2,\cdots,p-1$ 中全体模 $p$ 的二次剩余之和 $S=\dfrac{p(p^2-1)}{24}-p\sum\limits_{j=1}^{\frac{p-1}{2}}\left[\dfrac{j^2}{p}\right]$.

由此可以证明当 $p\equiv 1(\mathrm{mod}\,4)$ 时, $p\sum\limits_{j=1}^{\frac{p-1}{2}}\left[\dfrac{j^2}{p}\right]=\dfrac{p(p^2-1)}{24}-\dfrac{p(p-1)}{4}$.

# 高一竞赛数论专题

## 11.模为素数的二次剩余解答

设素数 $p>2,d$ 是整数, $p \quad d$. 如果同余方程 $x^2 \equiv d(\mathrm{mod}\, p)$ 有解,则称 $d$ 是模 $p$ 的二次剩余,若无解,则称 $d$ 是模 $p$ 的二次非剩余.

注意到 $p \mid d$. 则同余方程 $x^2 \equiv d \equiv 0(\mathrm{mod}\, p)$ ,则其有且只有一解 $x \equiv 0(\mathrm{mod}\, m)$.

若 $p=2$, 且 $p \quad d$. 则同余方程 $x^2 \equiv d(\mathrm{mod}\, 2)$ 为 $x^2 \equiv 1(\mathrm{mod}\, 2)$ 有且只有一解 $x \equiv 1(\mathrm{mod}\, 2)$.

1.设素数 $p>2$ ,证明在模 $p$ 的一个既约剩余系中,恰有 $\frac{p-1}{2}$ 个模 $p$ 的二次剩余, $\frac{p-1}{2}$ 个模 $p$ 的二次非剩余.此外,若 $d$ 是模 $p$ 的二次剩余,则同余方程 $x^2 \equiv d(\mathrm{mod}\, p)$ 的解数为 2.

证明：取模 $p$ 的绝对最小既约剩余系 $-\frac{p-1}{2},-\frac{p-1}{2}+1,\cdots,-1,1,\cdots,\frac{p-1}{2}-1,\frac{p-1}{2}$.

$d$ 是模 $p$ 的二次剩余当且仅当 $d \equiv (-\frac{p-1}{2})^2,(-\frac{p-1}{2}+1)^2,\cdots,(-1)^2,1^2,\cdots,(\frac{p-1}{2}-1)^2,(\frac{p-1}{2})^2$.

由于 $(-j)^2 \equiv j^2(\mathrm{mod}\, p)$, 所以 $d$ 是模 $p$ 的二次剩余当且仅当 $d \equiv 1^2,\cdots,(\frac{p-1}{2}-1)^2,(\frac{p-1}{2})^2$.

当 $1 \le i<j \le \frac{p-1}{2}$ 时, $2<i+j<p-1, 1-\frac{p-1}{2}<i-j<0$, $i^2-j^2=(i+j)(i-j) \not\equiv 0(\mathrm{mod}\, p)$.

所以 $d \equiv 1^2,\cdots,(\frac{p-1}{2}-1)^2,(\frac{p-1}{2})^2$ 给出了模 $p$ 的全部二次剩余,共有 $\frac{p-1}{2}$ 个.

由于模 $p$ 的既约剩余系(简系)有 $p-1$ 个数,所以另外的 $\frac{p-1}{2}$ 个必为模 $p$ 的二次非剩余.

当 $d$ 是模 $p$ 的二次剩余时,必存在唯一的 $i, 1 \le i \le \frac{p-1}{2}$, 使得 $x = i(\mathrm{mod}\ p)$ 是同余方程 $x^2 \equiv d(\mathrm{mod}\ p)$ 的解,于是在模 $p$ 的绝对最小既约剩余系 $-\frac{p-1}{2}, -\frac{p-1}{2}+1, \cdots, -1, 1, \cdots, \frac{p-1}{2}-1, \frac{p-1}{2}$. 中有且仅有 $x = \pm i(\mathrm{mod}\ p)$ 是同余方程 $x^2 \equiv d(\mathrm{mod}\ p)$ 的解,所以解数为 2.

2.(Euler 判别法)设素数 $p > 2, p \quad d$, 那么, $d$ 是模 $p$ 的二次剩余的充要条件是 $d^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$; $d$ 是模 $p$ 的二次非剩余的充要条件是 $d^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\ p)$.

证明：首先来证明对任一 $d, p \quad d, d^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p), d^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\ p)$ 有且仅有一个成立.

由 Euler 定理知道 $d^{p-1} \equiv 1(\mathrm{mod}\ p)$. 因此 $(d^{\frac{p-1}{2}}+1)(d^{\frac{p-1}{2}}-1) \equiv 0(\mathrm{mod}\ p)$.

由于素数 $p > 2$ 即 $(d^{\frac{p-1}{2}}+1)-(d^{\frac{p-1}{2}}-1) \equiv 2$.

所以对任一 $d, p \quad d, d^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p), d^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\ p)$ 有且仅有一个成立.

下面来证明 $d$ 是模 $p$ 的二次剩余的充要条件是 $d^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$.

先证必要性 $(\Rightarrow)$ 若 $d$ 是模 $p$ 的二次剩余,则必有 $x_0$ 使得 $x_0^2 \equiv d(\mathrm{mod}\ p)$,

因此有 $x_0^{p-1} = (x_0^2)^{\frac{p-1}{2}} \equiv d^{\frac{p-1}{2}}(\mathrm{mod}\ p)$.

由于 $p \quad d$, 所以 $p \quad x_0$. 由 Euler 定理知道 $x_0^{p-1} \equiv 1(\mathrm{mod}\ p)$ ,所以 $d^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$.

再证充分性,若 $d^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$. 则 $p \quad d$. 考虑一次同余方程 $ax \equiv d(\mathrm{mod}\ p)$. 对模 $p$ 的绝对最小既约剩余系 $-\frac{p-1}{2}, -\frac{p-1}{2}+1, \cdots, -1, 1, \cdots, \frac{p-1}{2}-1, \frac{p-1}{2}$.

中的每个 $j$ ,当 $a = j$ 时,必有唯一的 $x = x_j$ 属于模 $p$ 的绝对最小既约剩余系,使得 $ax \equiv d(\mathrm{mod}\ p)$.

若 $d$ 不是模 $p$ 的二次剩余,则必有 $j \ne x_j$. 这样模 $p$ 的绝对最小既约剩余系中的 $p-1$ 个数就可按 $j, x_j$ 作为一对,两两配完.因此有 $(p-1)! \equiv (-\frac{p-1}{2})(-\frac{p-1}{2}+1)\cdots(-1)1\cdots(\frac{p-1}{2}-1)\frac{p-1}{2} \equiv d^{\frac{p-1}{2}}(\mathrm{mod}\ p)$.

由 Wilson 定理知 $(p-1)! \equiv -1(\mathrm{mod}\ p)$ ,所以 $d^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\ p)$ 这与 $d^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$ 矛盾.

$d$ 是模 $p$ 的二次剩余的充要条件是 $d^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$, 与对任一 $d, p \quad d$,

$d^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p), d^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\ p)$ 有且仅有一个成立.可以推得 $d$ 是模 $p$ 的二次非剩余的充要条件是

$d^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\, p).$

3. 若素数 $p>2,$证明： $-1$是模 $p$ 的二次剩余的充要条件是 $p \equiv 1(\mathrm{mod}\, 4).$

当 $p \equiv 1(\mathrm{mod}\, 4)$时,$\left(\pm\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1(\mathrm{mod}\, p).$

证明：由 Euler 判别法知道$-1$是模 $p$ 的二次剩余的充要条件是$(-1)^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p).$

又 $p>2$ ,所以$(-1)^{\frac{p-1}{2}} = 1.$即 $p \equiv 1(\mathrm{mod}\, 4).$

由 Wilson 定理,$(p-1)! \equiv -1.$

$$-1 \equiv (p-1)! \equiv (-\frac{p-1}{2})(-\frac{p-1}{2}+1)\cdots(-1)1\cdots(\frac{p-1}{2}-1)\frac{p-1}{2} = (-1)^{\frac{p-1}{2}}\left(\left(\frac{p-1}{2}\right)!\right)^2 (\mathrm{mod}\, p)$$

当 $p \equiv 1(\mathrm{mod}\, 4)$时,$\left(\pm\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1(\mathrm{mod}\, p).$

4.设 $p$ 是奇素数,证明： $1,2,\cdots,p-1$ 中全体模 $p$ 的二次剩余之和 $S = \frac{p(p^2-1)}{24} - p\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{j^2}{p}\right].$

由此可以证明当 $p \equiv 1(\mathrm{mod}\, 4)$时, $p\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{j^2}{p}\right] = \frac{p(p^2-1)}{24} - \frac{p(p-1)}{4}.$

证明：因为 $d$ 是模 $p$ 的二次剩余当且仅当 $d \equiv 1^2,\cdots,(\frac{p-1}{2}-1)^2,(\frac{p-1}{2})^2(\mathrm{mod}\, p).$

设 $j^2 = pq_j + r_j(1 \le r_j < p),1 \le j \le \frac{p-1}{2}.$则 $q_j = \left[\frac{j^2}{p}\right].$

于是 $S = \sum_{j=1}^{\frac{p-1}{2}} r_j = \sum_{j=1}^{\frac{p-1}{2}} j^2 - p\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{j^2}{p}\right] = \frac{\frac{p-1}{2}(\frac{p-1}{2}+1)(p-1+1)}{6} - p\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{j^2}{p}\right] = \frac{p(p^2-1)}{24} - p\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{j^2}{p}\right].$

若 $p \equiv 1(\mathrm{mod}\, 4),$则 $p\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{j^2}{p}\right] = \frac{p(p^2-1)}{24} - S.$

因为 $p \equiv 1(\mathrm{mod}\, 4),$由 Euler 判别法知道 $r_j$ 与 $p-r_j$ 同为二次剩余或非二次剩余.

又在模 $p$ 的一个既约剩余系中,恰好有 $\frac{p-1}{2}$ 个模 $p$ 的二次剩余,所以 $S = \frac{p}{2}\cdot\frac{p-1}{2} = \frac{p(p-1)}{4}.$

于是 $p\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{j^2}{p}\right]=\frac{p(p^2-1)}{24}-\frac{p(p-1)}{4}.$