# 二次剩余

## Quadratic Residue

## 定义

设 $a$ 不是 $p$ 的倍数，如果 $\exists x$ 使得 $x^2 \equiv a \pmod{p}$，则称 $a$ 是模 $p$ 的**二次剩余**。

设 $b$ 不是 $p$ 的倍数，如果 $\forall x$ 都不能使得 $x^2 \equiv b \pmod{p}$ 成立，则称 $b$ 是模 $p$ 的**非二次剩余**。

求解二次剩余，即对于常数 $a$ 解以下方程：

$$x^2 \equiv a \pmod{p}$$

可通俗理解为在模意义下开方。

以下只讨论 $p$ 为**奇素数**的情形。

## 解的数量

模 $p$ 的二次剩余（即满足 $x^2 \equiv n \pmod{p}$ 有解的 $n$）有 $\frac{p-1}{2}$ 个（不包括 0），非二次剩余有 $\frac{p-1}{2}$ 个。

证：设 $u, v$ 都是 $x^2 \equiv n \pmod{p}$ 的解，那么：
$u^2 \equiv v^2 \pmod{p} \implies (u+v)(u-v) \mid p \implies u+v \mid p$，这样的数对 $(u, v)$ 有 $\frac{p-1}{2}$ 个。换句话说，指定一个 $u$，可以找到相应 $v$，它们的平方模 $p$ 相等，即对应着一个 $n$；而不对应的数字，平方模 $p$ 必不等，得到的 $n$ 不等，故 $n$ 与 $(u, v)$ 对建立了一一对应关系。$(u, v)$ 有 $\frac{p-1}{2}$ 个，$n$ 就有 $\frac{p-1}{2}$ 个。证毕。

从上述证明可以看出，所有模 $p$ 的二次剩余就是 $\left\{1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2\right\}$.

## 勒让德符号 Legendre symbol

$$\left(\frac{n}{p}\right)=\begin{cases}1 & ,p\nmid n \text{ 且 } n \text{ 是 } p \text{ 的二次剩余}\\ -1 & ,p\nmid n \text{ 且 } n \text{ 是 } p \text{ 的非二次剩余}\\ 0 & ,p\mid n\end{cases}$$

部分勒让德符号的值：

| p \ a | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 1 | -1 | 0 | 1 | -1 | 0 | 1 | -1 | 0 | 1 | -1 | 0 | 1 | -1 | 0 | 1 | -1 | 0 | 1 | -1 | 0 | 1 | -1 | 0 | 1 | -1 | 0 | 1 | -1 | 0 |
| 5 | 1 | -1 | -1 | 1 | 0 | 1 | -1 | -1 | 1 | 0 | 1 | -1 | -1 | 1 | 0 | 1 | -1 | -1 | 1 | 0 | 1 | -1 | -1 | 1 | 0 | 1 | -1 | -1 | 1 | 0 |
| 7 | 1 | 1 | -1 | 1 | -1 | -1 | 0 | 1 | 1 | -1 | 1 | -1 | -1 | 0 | 1 | 1 | -1 | 1 | -1 | -1 | 0 | 1 | 1 | -1 | 1 | -1 | -1 | 0 | 1 | 1 |
| 11 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | 0 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | 0 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 |
| 13 | 1 | -1 | 1 | 1 | -1 | -1 | -1 | -1 | 1 | 1 | -1 | 1 | 0 | 1 | -1 | 1 | 1 | -1 | -1 | -1 | -1 | 1 | 1 | -1 | 1 | 0 | 1 | -1 | 1 | 1 |
| 17 | 1 | 1 | -1 | 1 | -1 | -1 | -1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | 1 | 0 | 1 | 1 | -1 | 1 | -1 | -1 | -1 | 1 | 1 | -1 | -1 | -1 | 1 |
| 19 | 1 | -1 | -1 | 1 | 1 | 1 | 1 | -1 | 1 | -1 | 1 | -1 | -1 | -1 | -1 | 1 | 1 | -1 | 0 | 1 | -1 | -1 | 1 | 1 | 1 | 1 | -1 | 1 | -1 | 1 |
| 23 | 1 | 1 | 1 | 1 | -1 | 1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | -1 | -1 | 1 | -1 | 1 | -1 | -1 | -1 | -1 | 0 | 1 | 1 | 1 | 1 | -1 | 1 | -1 |
| 29 | 1 | -1 | -1 | 1 | 1 | 1 | 1 | -1 | 1 | -1 | -1 | -1 | 1 | -1 | -1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | 1 | 1 | 1 | -1 | -1 | 1 | 0 | 1 |
| 31 | 1 | 1 | -1 | 1 | 1 | -1 | 1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | -1 | 1 | -1 | -1 | 1 | -1 | -1 |
| 37 | 1 | -1 | 1 | 1 | -1 | -1 | 1 | -1 | 1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | -1 | -1 | -1 | 1 | -1 | -1 | -1 | 1 | 1 | 1 | 1 | -1 | 1 |
| 41 | 1 | 1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | -1 | -1 | 1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | -1 | 1 | -1 | -1 | -1 | -1 | -1 |
| 43 | 1 | -1 | -1 | 1 | -1 | 1 | -1 | -1 | 1 | 1 | 1 | -1 | 1 | 1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | -1 | -1 |
| 47 | 1 | 1 | 1 | 1 | -1 | 1 | 1 | 1 | 1 | -1 | -1 | 1 | -1 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | 1 | -1 | -1 | 1 | 1 | -1 | 1 | 1 | -1 | -1 |
| 53 | 1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | 1 | 1 | -1 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | -1 | -1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | -1 |
| 59 | 1 | -1 | 1 | 1 | 1 | -1 | 1 | -1 | 1 | -1 | -1 | 1 | -1 | -1 | 1 | 1 | 1 | -1 | 1 | 1 | 1 | 1 | -1 | -1 | 1 | 1 | 1 | 1 | 1 | -1 |
| 61 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | -1 | 1 | 1 | 1 | 1 | 1 | -1 | -1 | 1 | 1 | -1 | 1 | -1 | -1 | 1 | -1 | 1 | -1 | -1 | -1 |
| 67 | 1 | -1 | -1 | 1 | -1 | 1 | -1 | -1 | 1 | 1 | -1 | -1 | -1 | 1 | 1 | 1 | 1 | -1 | 1 | -1 | 1 | 1 | 1 | 1 | 1 | 1 | -1 | -1 | 1 | -1 |
| 71 | 1 | 1 | 1 | 1 | 1 | 1 | -1 | 1 | 1 | 1 | -1 | 1 | -1 | -1 | 1 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | 1 | -1 | 1 | -1 | 1 | 1 |
| 73 | 1 | 1 | 1 | 1 | -1 | 1 | -1 | 1 | 1 | -1 | -1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | -1 | -1 | 1 | 1 | 1 | -1 | 1 | -1 | -1 | -1 |
| 79 | 1 | 1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | 1 | 1 | -1 | 1 | -1 | -1 | 1 | -1 | 1 | 1 | 1 | 1 | 1 | 1 | -1 | 1 | 1 | -1 | -1 | -1 | -1 |
| 83 | 1 | -1 | 1 | 1 | -1 | -1 | 1 | -1 | 1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | -1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 89 | 1 | 1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | 1 | 1 | -1 | -1 | -1 | -1 | 1 | 1 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | 1 | -1 | -1 | -1 | -1 | -1 |
| 97 | 1 | 1 | 1 | 1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | -1 | -1 | -1 |
| 101 | 1 | -1 | -1 | 1 | 1 | 1 | -1 | -1 | 1 | -1 | -1 | -1 | 1 | 1 | -1 | 1 | 1 | -1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | -1 | -1 | -1 | -1 | 1 |
| 103 | 1 | 1 | -1 | 1 | -1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | 1 | 1 |
| 107 | 1 | -1 | 1 | 1 | -1 | -1 | -1 | -1 | 1 | 1 | 1 | 1 | 1 | 1 | -1 | 1 | -1 | -1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 | 1 |
| 109 | 1 | -1 | 1 | 1 | 1 | -1 | 1 | -1 | 1 | -1 | -1 | 1 | -1 | -1 | 1 | 1 | -1 | -1 | -1 | 1 | 1 | 1 | -1 | -1 | 1 | 1 | 1 | 1 | 1 | -1 |
| 113 | 1 | 1 | -1 | 1 | -1 | -1 | 1 | 1 | 1 | -1 | 1 | -1 | 1 | 1 | 1 | 1 | -1 | 1 | -1 | -1 | -1 | 1 | -1 | -1 | 1 | 1 | -1 | 1 | -1 | 1 |
| 127 | 1 | 1 | -1 | 1 | -1 | -1 | -1 | 1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 | 1 | 1 | 1 | 1 | -1 | 1 | 1 | -1 | -1 | 1 | 1 | -1 | -1 | -1 | 1 |

根据解的数量的分析，每一行都以 $p$ 为循环节，每一个循环节内部有 $\frac{p-1}{2}$ 个 $1$，$\frac{p-1}{2}$ 个 $-1$，和 $1$ 个 $0$.

# 欧拉判别准则 Euler's Criterion

$$\left(\frac{n}{p}\right)\equiv n^{\frac{p-1}{2}}\pmod p$$

换句话说，就是：

$$n \text{ 是模 } p \text{ 的二次剩余} \iff n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$
$$n \text{ 是模 } p \text{ 的非二次剩余} \iff n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

证：由费马小定理，$n^{p-1} \equiv 1 \pmod{p}$，推出：$p \mid \left(n^{\frac{p-1}{2}} - 1\right)\left(n^{\frac{p-1}{2}} + 1\right)$，故 $p \mid n^{\frac{p-1}{2}} - 1$ 或 $p \mid n^{\frac{p-1}{2}} + 1$，即 $n^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. 所以 $n^{\frac{p-1}{2}}$ 模 $p$ 只有 $\pm 1$ 两种结果。于是，上面两个等价是逆否关系，我们只需要证明第一个等价即可。

- 必要性：若 $n$ 是 $p$ 的二次剩余，那么 $\exists x$ 使得 $x^2 \equiv n \pmod{p}$，于是 $n^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$；
- 充分性：由于 $p$ 是奇素数，所以 $p$ 有原根，设 $a$ 是 $p$ 的一个原根，则 $\exists j \in [1, p-1]$ 使得 $a^j \equiv n \pmod{p}$，于是有：$n^{\frac{p-1}{2}} \equiv a^{j\frac{p-1}{2}} \equiv 1 \equiv a^{p-1} \pmod{p}$. 由原根的性质，$p-1 \mid \frac{j(p-1)}{2}$，故 $j$ 是偶数。设 $j = 2i$，则 $a^{2i} \equiv (a^i)^2 \equiv n \pmod{p}$，即 $n$ 是模 $p$ 的二次剩余。

证毕。

通过欧拉判别准则，我们可以得到勒让德符号的一些性质：

- 若 $a \equiv b \pmod{p}$，则 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. 【由定义显然】
- 勒让德符号是**完全积性**的，即：$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. 【由欧拉判别准则，$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.】
- 更多性质见**二次互反律**。

根据欧拉判别准则，我们只需要算一算 $n^{\frac{p-1}{2}} \bmod p$ 的值就知道 $n$ 是不是模 $p$ 的二次剩余了。

但是欧拉判别准则只能用来“判别”，求解二次剩余还需 **Cipolla** 算法。

# Cipolla 算法

求解 $x^2 \equiv n \pmod{p}$.

（根据“解的数量”一节的叙述，$x^2 \equiv n \pmod{p}$ 的解一定是 $\left\{1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2\right\}$ 这 $p-1$ 个数中的一个或其相反数。）

- 随机一个数 $a$ 使得 $a^2 - n$ 是模 $p$ 的非二次剩余，即 $\left(\frac{a^2-n}{p}\right) = -1$. 由于模 $p$ 的非完全剩余有 $\frac{p-1}{2}$ 个，随机一次满足条件的概率接近 $\frac{1}{2}$，故期望随机次数为 $2$；
- 建立一个类似于复数域的数域，以 $a^2 - n$ 类比 $i^2$（因为 $i^2 = -1$，而类似的，$a^2 - n \equiv -1 \pmod{p}$），记 $\sqrt{a^2 - n}$ 为虚数单位 $\omega$。于是乎，所有数都可以写成

$A+B\omega$ 的形式，$A$ 类比于实部，$B$ 类比于虚部；

- 得到答案：$x^2 \equiv n \pmod p$ 的解为 $(a+\omega)^{\frac{p+1}{2}}$.

要证明算法的正确性，先引入两个引理：

**Lemma 1**：$(a+b)^p \equiv a^p + b^p \pmod p$.

证：

$$(a+b)^p \equiv \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i \equiv a^p + b^p \pmod p$$

（注意二项式系数在 $1 \leqslant i < p$ 时都有 $p$ 因子）$\square$

**Lemma 2**：$\omega^p \equiv -\omega \pmod p$.

证：

$$\omega^p \equiv \omega^{p-1}\omega \equiv (\omega^2)^{\frac{p-1}{2}}\omega \equiv -\omega \pmod p$$

（注意 $\omega^2$ 是模 $p$ 的非二次剩余，根据欧拉判别准则，$(\omega^2)^{\frac{p-1}{2}} \equiv -1 \pmod p$）$\square$

于是乎，我们有：

$$\begin{aligned}
x^2 &\equiv (a+\omega)^{p+1} && \text{解为 } x = (a+\omega)^{\frac{p+1}{2}} \\
&\equiv a^{p+1} + \omega^{p+1} && \textbf{Lemma 1} \\
&\equiv a^2 - \omega^2 && \textbf{Lemma 2 和费马小定理} \\
&\equiv a^2 - (a^2 - n) && \omega^2 = a^2 - n \\
&\equiv n \pmod p
\end{aligned}$$

故 $x = (a+\omega)^{\frac{p+1}{2}}$ 就是我们要找的解。

# Code

```
mt19937 rnd(time(NULL));
namespace Quadratic_Residue{
    LL w; // w = omega^2 (i^2)
    struct Complex{
        LL r, i;
        Complex() {}
        Complex(LL rr, LL ii): r(rr), i(ii) {}
    };
    inline Complex mul(Complex a, Complex b, LL mod){
        Complex res;
        res.r = (a.r * b.r % mod + a.i * b.i % mod * w % mod) % mod;
```

```
        res.i = (a.r * b.i % mod + a.i * b.r % mod) % mod;
        return res;
    }
    inline Complex fpow(Complex bs, LL idx, LL mod){
        // fast pow for complex numbers
        Complex res(1, 0);
        while(idx){
            if(idx & 1) res = mul(res, bs, mod);
            bs = mul(bs, bs, mod);
            idx >>= 1;
        }
        return res;
    }
    inline int isQR(LL n, LL p){
        // return the value of Legendre symbol
        // 1: n is quadratic residue; -1: n is quadratic non-residue; 0: n%p==0
        n %= p;
        if(n == 0)  return 0;
        if(fpow(Complex(n, 0), (p-1)>>1, p).r == 1) return 1;
        else    return -1;
    }
    pair<LL, LL> solve(LL n, LL p){
        // solve x^2=n(mod p)
        if(isQR(n, p) == -1)    return mp(-1, -1);
        n %= p; if(n == 0) return mp(0, 0);
        LL a;
        while(1){
            a = uniform_int_distribution<LL>(1, p-1)(rnd);
            w = ((a * a % p - n) % p + p) % p;
            if(isQR(w, p) == -1)    break;
        }
        Complex x(a, 1);
        x = fpow(x, (p+1)>>1, p);
        if(x.r > p - x.r)   x.r = p - x.r;
        return mp(x.r, p - x.r);
    }
}
```