初等数论
第四章 二次剩余

中山大学 数据科学与计算机学院

5. 模为合数的二次同余方程

设$m = 2^{\delta} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, 我们知道对于一个模为合数$m$的二次方程($a$与$m$互素)

$$x^2 \equiv a \bmod m$$

这等价于一个同余式组

$$\begin{cases} x^2 \equiv a \bmod 2^{\delta} \\ x^2 \equiv a \bmod p_1^{\alpha_1} \\ x^2 \equiv a \bmod p_2^{\alpha_2} \\ \dots\dots \\ x^2 \equiv a \bmod p_k^{\alpha_k} \end{cases}$$

问题转化为: 同余方程$x^2 \equiv a \bmod 2^{\delta}$的判定与求解, 以及同余方程$x^2 \equiv a \bmod p^{\alpha}$的判定与求解.

定理

设p为奇素数, a与p互素. 同余方程$x^2 \equiv a \bmod p^\alpha$有解当且仅当$a$为模$p$的二次剩余, 且有解时解数为2.

"必要性:" 如果$x^2 \equiv a \bmod p^\alpha$有解$x_1$, 即$x_1^2 \equiv a \bmod p^\alpha$, 从而$x_1^2 \equiv a \bmod p$, 即$a$为模$p$的二次剩余.
"充分性:" 如果a为模p的二次剩余, 则存在$x \equiv x_1 \bmod p$使得$x_1^2 \equiv a \bmod p$.
取$f(x) = x^2 - a$, 则$f(x) \equiv 0 \bmod p$有解x_1. 可以求出同余方程$f(x) \equiv 0 \bmod p^2$的与x_1对应的解$x \equiv x_1 + kp \bmod p^2$, 其中$k$是

$$f'(x_1)k \equiv \frac{-f(x_1)}{p} \bmod p$$

的解. 该一次同余方程的解k是唯一的, 因为$f'(x_1) = 2x_1$, 2和x_1都与p互素, 所以其解数为$(f'(x_1), p) = 1$. 类似地, 可以验证同余方程$f(x) \equiv 0 \bmod p^2$的解唯一的对应同余方程$f(x) \equiv 0 \bmod p^3$的解, ……, 最后, $f(x) \equiv 0 \bmod p$有解x_1可以唯一地得到$f(x) \equiv 0 \bmod p^\alpha$的解.
模素数的二次同余方程$x^2 - a \equiv 0 \bmod p$只有两个解$x \equiv \pm x_1 \bmod p$. 所以二次同余方程$x^2 - a \equiv 0 \bmod p^\alpha$也只有两个解, 并且可以分别利用$x_1$和$-x_1$求出. $\diamond$

考虑同余方程$x^2 \equiv a \bmod 2^\delta$的判定与求解, 其中$(a,2)=1$.
如果$\delta=2$, 那么

$$x^2 \equiv a \bmod 4$$

有解当且仅当$a \equiv 1 \bmod 4$. 这是因为$0^2=0, 1^2=1, 2^2=4, 3^2=9$, 且$(a,2)=1$,
所以, 当且仅当$a \equiv 1 \bmod 4$时有解, 解数为2, 解为$x \equiv 1 \bmod 4, x \equiv -1 \bmod 4$.

当$\delta \geq 3$时: 同余方程$x^2 \equiv a \bmod 2^\delta$有解当且仅当$a \equiv 1 \bmod 8$. 且有解时解数为4.
"必要性:" 假设有解$x \equiv x_1 \bmod 2^\delta$. 由于$(a,2^\delta)=1$, 所以$a$必定是奇数, 从而$x_1$必定是奇数, 设$x_1 = 2l+1 (l \in \mathbb{Z})$, 则

$$a \equiv (2l+1)^2 \equiv 1+4l(l+1) \bmod 2^\delta,$$

注意到$2 \mid l(l+1)$, 从而

$$a \equiv 1+4l(l+1) \bmod 2^3,$$

即$a \equiv 1 \bmod 8$.

"充分性:" 已知$a \equiv 1 \bmod 8$,
当$\delta = 3$时, $2^\delta = 8$: 可以通过检查发现同余方程$x^2 \equiv 1 \bmod 8$的解有4个, 它们是$x \equiv \pm 1, \pm 5 \bmod 8$. 具有这种形式的所有整数可以表示为

$$\pm(1 + t_3 \cdot 2^2),$$

其中$t_3 = 0, \pm 1, \pm 2 \ldots$.
当$\delta = 4$时, $2^\delta = 16$: 设c是方程$x^2 \equiv a \bmod 16$的解, 则c是$x^2 \equiv a \bmod 8$的解, 从而也是$x^2 \equiv 1 \bmod 8$的解. 将$c = \pm(1 + t_3 \cdot 2^2)$代入同余方程$x^2 \equiv a \bmod 16$. 因为$(1 + t_3 \cdot 2^2)^2 = 1 + 8t_3 + 16t_3^2$, 所以$1 + 8t_3 \equiv a \bmod 16$, 即$8t_3 \equiv a - 1 \bmod 16$, 于是

$$t_3 \equiv \frac{a-1}{8} \bmod 2$$

这样, 方程$x^2 \equiv a \bmod 16$的解(具有这种形式的所有整数)就是:

$$\pm(1 + t_3 \cdot 2^2 + t_4 \cdot 2^3) = \pm(x_4 + t_4 \cdot 2^3)$$

其中$t_3 = 0, 1$, 且$t_4 = 0, \pm 1, \pm 2 \ldots$, 而$x_4 = 1 + t_3 \cdot 2^2$.

当$\delta = 5$时, $2^\delta = 32$: 设c是方程$x^2 \equiv a \bmod 32$的解, 则c也是$x^2 \equiv a \bmod 16$的解, 将$c = \pm(x_4 + t_4 \cdot 2^3)$代入同余方程$x^2 \equiv a \bmod 32$, 因为

$$(x_4 + t_4 \cdot 2^3)^2 = x_4^2 + 2^4 \cdot x_4 t_4 + 2^6 \cdot t_4^2,$$

且

$$2 \cdot x_4 \cdot t_4 2^3 \equiv 2(1 + t_3 \cdot 2^2) t_4 2^3 \equiv 2^4 \cdot t_4 \bmod 2^5.$$

所以$x_4^2 + 2^4 \cdot t_4 \equiv a \bmod 2^5$, 即$2^4 \cdot t_4 \equiv a - x_4^2 \bmod 2^5$, 于是

$$t_4 \equiv \frac{a - x_4^2}{2^4} \bmod 2.$$

这样, 方程$x^2 \equiv a \bmod 32$的解(具有这种形式的所有整数)就是:

$$\pm(x_4 + t_4 \cdot 2^3 + t_5 \cdot 2^4) = \pm(x_5 + t_5 \cdot 2^4)$$

其中$t_4 = 0, 1$, 且$t_5 = 0, \pm 1, \pm 2 \ldots$, 而$x_5 = x_4 + t_4 \cdot 2^3$.
上述这个过程可以继续下去, 最终求出$x^2 \equiv a \bmod 2^\delta$的解. 它们对模$2^\delta$为4个解. $\diamond$

示例: 求解$x^2 \equiv 57 \bmod 64$

首先判断解的存在性. 因为$64 = 2^6, 57 \equiv 1 \bmod 8$, 所以该同余方程有解.
从方程$x^2 \equiv 57 \bmod 2^3$开始: 其解为

$$\pm(1+4t_3), \quad t_3 = 0, \pm 1, \pm 2 \dots$$

方程$x^2 \equiv 57 \bmod 2^4$的解: 将$(1+4t_3)$代入$x^2 \equiv 57 \bmod 2^4$求出t_3,

$$t_3 \equiv \frac{57-1}{8} \equiv \bmod 2.$$

方程$x^2 \equiv 57 \bmod 2^5$的解: 将$(1+1\cdot 2^2 + t_4 \cdot 2^3)$代入$x^2 \equiv 57 \bmod 2^5$求出$t_4$, 即

$$t_4 \equiv \frac{57-5^2}{16} \equiv 0 \bmod 2.$$

所以, 同余方程$x^2 \equiv 57 \bmod 2^5$的解(具有这种形式的所有整数)为

$$\pm(5+0\cdot 2^3 + t_5 \cdot 2^4) = \pm(5+t_5\cdot 2^4), \quad t_5 = 0, \pm 1, \pm 2 \dots.$$

方程$x^2 \equiv 57 \bmod 2^6$的解: 将$(5+t_5 \cdot 2^4)$代入$x^2 \equiv 57 \bmod 2^6$求出t_5, 即

$$t_5 \equiv \frac{57-25}{32} \equiv 1 \bmod 2.$$

所以, 同余方程$x^2 \equiv 57 \bmod 2^6$的解(具有这种形式的所有整数)为

$$\pm(5+1\cdot 2^4+t_6\cdot 2^5) = \pm(21+t_6\cdot 2^5), \quad t_6 = 0, \pm 1, \pm 2 \ldots.$$

它们对模2^6为4个解, $x \equiv 21 \bmod 64$, $x \equiv 53 \bmod 64$, $x \equiv 43 \bmod 64$, $x \equiv 11 \bmod 64$.

至此, 关于二次方程我们得到的结论是:

1. 模素数的二次方程$x^2 \equiv a \bmod p$的解的判定与求解(二次剩余);
2. 模为2^δ的二次方程$x^2 \equiv a \bmod 2^\delta$的解的判定与求解(有解时解数为4, 从$x^2 \equiv a \bmod 2^3$开始求解);
3. 模为p^α的二次方程$x^2 \equiv a \bmod p^\alpha$的解的判定与求解(有解时解数为2, 从$x^2 \equiv a \bmod p$开始求解);
4. 模为合数的二次方程$x^2 \equiv a \bmod m$(a与m互素)的解的判定与求解(利用2与3).

第四章小结

1. 二次剩余的基本概念.
2. 列举模p的二次剩余.
3. 勒让德符号及其基本性质.
4. 高斯引理及二次互反律.
5. 雅可比符号及其基本性质.
6. 二次同余方程解的存在性及求解.