初等数论
第四章 二次剩余

中山大学 计算机学院

4. 模素数的二次同余方程求解

计算勒让德符号可以判定二次同余方程$x^2 \equiv a \bmod p$解的存在性，其中p是奇素数. 如果二次同余方程的解是存在的，应该怎么求解？下面给出求解的一般思路是.

- 将$p-1$写成是2的幂和一个奇数的乘积形式，即$p-1=2^t \cdot s$，其中$s \geq 1$.
- 首先应用欧拉定理和欧拉判别条件，我们发现较容易求出同余方程

  $$y^{2^{t-1}} \equiv 1 \bmod p$$

  的一个形如$a^{-1}x_{t-1}^2$的解. 如果$t=1$，则$x_0 \bmod p$就是原二次同余式的一个解.
- 如果$t>1$，在$a^{-1}x_{t-1}^2$基础上，能够比较容易地求出同余方程

  $$y^{2^{t-2}} \equiv 1 \bmod p$$

  的一个形如$a^{-1}x_{t-2}^2$的解. 如果$t=2$，则求解工作可以结束.
- 如果$t>2$，在$a^{-1}x_{t-2}^2$基础上，继续类似的求解运算，即求出同余方程

  $$y^{2^{t-3}} \equiv 1 \bmod p$$

  的一个形如$a^{-1}x_{t-3}^2$的解;

- 一般地, 如果求出了同余方程

$$y^{2^{t-k}} \equiv 1 \bmod p$$

的一个形如$a^{-1}x_{t-k}^2$的解, 且$t > k$, 可以类似的求出同余方程

$$y^{2^{t-k-1}} \equiv 1 \bmod p$$

的一个形如$a^{-1}x_{t-k-1}^2$的解.

- 继续下去, 我们一定能求出同余方程

$$y^2 \equiv 1 \bmod p$$

的一个形如$a^{-1}x_1^2$的解, 从而最终能够比较容易地求出

$$y \equiv 1 \bmod p$$

的一个形如$a^{-1}x_0^2$的解.

- 至此, 将完成原二次同余方程的求解, 即一个解$x_0 \bmod p$, 另一个是$-x_0 \bmod p$.

具体求解时，先任意选取模p的一个平方非剩余n，计算$b=(n^s \bmod p)$，从而有

$$b^{2^t}=(n^s)^{2^t}=n^{s\cdot 2^t}=n^{p-1}\equiv 1 \bmod p$$

$$b^{2^{t-1}}=(n^s)^{2^{t-1}}=n^{s\cdot 2^{t-1}}=n^{\frac{p-1}{2}}\equiv -1 \bmod p$$

给定$p-1=2^t\cdot s$，同余方程$y^{2^{t-1}}\equiv 1 \bmod p$的一个形如$a^{-1}x_{t-1}^2$的解(其中的$x_{t-1}$)是

$$x_{t-1}=(a^{\frac{s+1}{2}} \bmod p).$$

这是因为

$$(a^{-1}x_{t-1}^2)^{2^{t-1}}\equiv (a^{-1}(a^{\frac{s+1}{2}})^2)^{2^{t-1}}=(a^{-1}a^{s+1})^{2^{t-1}}=a^{s\cdot 2^{t-1}}\equiv a^{\frac{p-1}{2}}\equiv 1 \bmod p.$$

如果$t=1$，则$x_0^2\equiv a^{s+1}\equiv a \bmod p$，即$x_0 \bmod p$就是原二次同余式的一个解.

如果$t>1$，下面是找出方程$y^{2^{t-2}}\equiv 1 \bmod p$的一个形如$a^{-1}x_{t-2}^2$的解的方法.
由于$(a^{-1}x_{t-1}^2)^{2^{t-1}}\equiv 1 \bmod p$，而且$(a^{-1}x_{t-1}^2)^{2^{t-1}}=[(a^{-1}x_{t-1}^2)^{2^{t-2}}]^2$
所以必定有

$$(a^{-1}x_{t-1}^2)^{2^{t-2}}\equiv 1 \bmod p \quad 或 \quad (a^{-1}x_{t-1}^2)^{2^{t-2}}\equiv -1 \bmod p.$$

case 1: 如果$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \bmod p$, 则令$x_{t-2} = x_{t-1}$, 且有

$$(a^{-1}x_{t-2}^2)^{2^{t-2}} = (a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \bmod p$$

即$a^{-1}x_{t-2}^2$是同余方程$y^{2^{t-2}} \equiv 1 \bmod p$的解.

case 2: 如果$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv -1 \bmod p$, 则令$x_{t-2} = x_{t-1} \cdot b^{2^0} = x_{t-1} \cdot b$, 且有

$$\begin{aligned}(a^{-1}x_{t-2}^2)^{2^{t-2}} &= (a^{-1}x_{t-1}^2 b^2)^{2^{t-2}} = (a^{-1}x_{t-1}^2)^{2^{t-2}}(b^2)^{2^{t-2}} \\ &= (a^{-1}x_{t-1}^2)^{2^{t-2}} b^{2^{t-1}} \equiv 1 \bmod p\end{aligned}$$

即$a^{-1}x_{t-2}^2$是同余方程$y^{2^{t-2}} \equiv 1 \bmod p$的解.

如果$t = 2$, 则$x_0^2 \equiv a \bmod p$, 即$x_0 \bmod p$就是原二次同余式的一个解.

所以, 不论$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \bmod p$还是$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv -1 \bmod p$, 总能利用方程

$$y^{2^{t-1}} \equiv 1 \bmod p$$

一个形如$a^{-1}x_{t-1}^2$的解, 计算出方程

$$y^{2^{t-2}} \equiv 1 \bmod p$$

的一个形如$a^{-1}x_{t-2}^2$的解.

类似地，如果$t > 2$，必定有

$$(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \bmod p \quad \text{或} \quad (a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv -1 \bmod p.$$

case 1：如果$(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \bmod p$，则令$x_{t-3} = x_{t-2}$，且有

$$(a^{-1}x_{t-3}^2)^{2^{t-3}} = (a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \bmod p$$

即$a^{-1}x_{t-3}^2$是同余方程$y^{2^{t-3}} \equiv 1 \bmod p$的解.

case 2：如果$(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv -1 \bmod p$，则令$x_{t-3} = x_{t-2} \cdot b^{2^1}$，则$x_{t-3}^2 = x_{t-2}^2 \cdot b^{2^2}$，且有

$$\begin{aligned}(a^{-1}x_{t-3}^2)^{2^{t-3}} &= (a^{-1}x_{t-2}^2 b^{2^2})^{2^{t-3}} = (a^{-1}x_{t-2}^2)^{2^{t-3}}(b^{2^2})^{2^{t-3}} \\ &= (a^{-1}x_{t-2}^2)^{2^{t-3}} b^{2^{t-1}} \equiv 1 \bmod p\end{aligned}$$

即$a^{-1}x_{t-3}^2$是同余方程$y^{2^{t-3}} \equiv 1 \bmod p$的解.
如果$t = 3$，则$x_0^2 \equiv a \bmod p$，即$x_0 \bmod p$就是原二次同余式的一个解.

类似地，如果$t > 3$，必定有

$$(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \bmod p \quad 或 \quad (a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv -1 \bmod p.$$

case 1: 如果$(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \bmod p$，则令$x_{t-4} = x_{t-3}$，且有

$$(a^{-1}x_{t-4}^2)^{2^{t-4}} = (a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \bmod p$$

即$a^{-1}x_{t-4}^2$是同余方程$y^{2^{t-4}} \equiv 1 \bmod p$的解.

case 2: 如果$(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv -1 \bmod p$，则令$x_{t-4} = x_{t-3} \cdot b^{2^2}$，则$x_{t-4}^2 = x_{t-3}^2 \cdot b^{2^3}$，且有

$$\begin{aligned}(a^{-1}x_{t-4}^2)^{2^{t-4}} &= (a^{-1}x_{t-3}^2 b^{2^3})^{2^{t-4}} = (a^{-1}x_{t-3}^2)^{2^{t-4}}(b^{2^3})^{2^{t-4}} \\ &= (a^{-1}x_{t-3}^2)^{2^{t-4}} b^{2^{t-1}} \equiv 1 \bmod p\end{aligned}$$

即$a^{-1}x_{t-4}^2$是方程$y^{2^{t-4}} \equiv 1 \bmod p$的解.
如果$t = 4$，则$x_0^2 \equiv a \bmod p$，即$x_0 \bmod p$就是原二次同余式的一个解.
如果$t > 4$，则继续找出方程$y^{2^{t-5}} \equiv 1 \bmod p$的一个形如$a^{-1}x_{t-5}^2$的解.

示例：求解$x^2 \equiv 186 \bmod 401$
计算$(\frac{186}{401}) = 1$，说明原方程有解.

$$a = 186, p = 401, p-1 = 2^4 \cdot 25, t = 4, s = 25, a^{-1} \equiv 235 \bmod 401.$$

取一个模p的非平方剩余$n = 3$，计算$b = n^s = 3^{25} \equiv 268 \bmod 401$
计算$y^{2^{t-1}} \equiv 1 \bmod p$的解:

$$x_{t-1} = (a^{\frac{s+1}{2}}), \quad x_3 = (186^{\frac{25+1}{2}} \bmod 401) = 103$$

$$a^{-1}x_3^2 = (235 \cdot 103^2 \bmod 401) = 98$$

计算$y^{2^{t-2}} \equiv 1 \bmod p$的解:

$$\because (a^{-1}x_3^2)^{2^{t-2}} \equiv 98^4 \equiv -1 \bmod 401$$

$$\therefore x_{t-2} = x_{t-1}b, \quad x_2 = (x_3 b \bmod p) = (103 \cdot 268 \bmod 401) = 336$$

$$a^{-1}x_{t-2}^2 = (235 \cdot 336^2 \bmod 401) = 400 \equiv -1 \bmod 401$$

计算$y^{2^{t-3}} \equiv 1 \bmod p$的解:

$$\because (a^{-1}x_2^2)^{2^{t-3}} \equiv (-1)^2 \equiv 1 \bmod 401$$

$$\therefore x_{t-3} = x_{t-2}, \quad x_1 = x_2 = 336$$

$$a^{-1}x_{t-3}^2 = (235 \cdot 336^2 \bmod 401) = 400 \equiv -1 \bmod 401$$

计算$y^{2^{t-4}} \equiv 1 \bmod p$, 即$y \equiv 1 \bmod p$ 的解:

$$\because (a^{-1}x_1^2)^{2^{t-4}} \equiv -1 \bmod 401$$

$$\therefore x_{t-4} = x_{t-3}b^{2^{3-1}}, \quad x_0 = (x_1 b^4 \bmod 401) = (336 \cdot 268^4 \bmod 401) = 304$$

这就是我们要求的原方程的解: $x \equiv \pm 304 \bmod 401$.

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$f'(x_1) = 2x_1$，其解数为$(f'(x_1), p) = 1$. 类似地，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$t_5 = 0, \pm1, \pm2 \ldots$, 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

$$\pm(1+4t_3), \quad t_3 = 0, \pm1, \pm2 \ldots$$

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

$$\pm(5+0\cdot 2^3+t_5\cdot 2^4) = \pm(5+t_5\cdot 2^4), \quad t_5 = 0, \pm1, \pm2 \ldots.$$

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

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

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.