华东师范大学
EAST CHINA NORMAL UNIVERSITY

网络安全数学基础(一)

沈佳辰
jcshen@sei.ecnu.edu.cn

网络安全数学基础

第三章 二次同余式与二次剩余

§3.1 二次同余式

- 二次同余式的一般形式为

$$ax^2 + bx + c \equiv 0\ (mod\ m) \qquad (3.1)$$

其中$a \not\equiv 0\ (mod\ m)$。

- 设m的标准分解式为$p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$，则由定理2.4.2可知(3.1)式和同余式组

$$\begin{cases} ax^2+bx+c\equiv 0\ (mod\ p_1^{\alpha_1}) \\ ax^2+bx+c\equiv 0\ (mod\ p_2^{\alpha_2}) \\ \vdots \\ ax^2+bx+c\equiv 0\ (mod\ p_s^{\alpha_s}) \end{cases} \qquad (3.2)$$

的解相同。因此只需讨论模数为素数幂p^α时的二次同余式

$$ax^2+bx+c\equiv 0\ (mod\ p^\alpha) \qquad (3.3)$$

的求解问题，其中$a\not\equiv 0\ (mod\ p^\alpha)$。

对(3.3)配方可得

$$(2ax+b)^2 \equiv b^2-4ac\ (mod\ p^\alpha) \quad (3.4)$$

因为$a \not\equiv 0\ (mod\ p^\alpha)$，易知当$p$为奇素数时，(3.3)和(3.4)的解相同，此时令$X=2ax+b, B=b^2-4ac$，则(3.4)和同余式

$$X^2 \equiv B\ (mod\ p^\alpha) \quad (3.5)$$

的解的个数相同，即(3.3)有解当且仅当(3.5)有解。

- 定义3.1.1　给定$m \in Z^{+}$,$a \in Z, (a, m) = 1$，如果同余式

$$x^2 \equiv a \ (mod\ m) \qquad (3.6)$$

有解，则a叫做模m的二次剩余（平方剩余）；否则a叫做模m的二次非剩余（平方非剩余）

- 例：

因为$1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 2, 4^2 \equiv 2, 5^2 \equiv 4, 6^2 \equiv 1 (mod\ 7)$，所以1，2，4是模7的二次剩余，3，5，6是模7的二次非剩余。

- 例：求满足方程E：$y^2 = x^3 + x + 1\ (mod\ 7)$的所有点。

解：

对于$x = 0,1,2,3,4,5,6$,分别求出y

x	0	1	2	3	4	5	6
y^2 (mod 7)	1	3	4	3	6	5	6
y (mod 7)	1,6	无解	2,5	无解	无解	无解	无解

由此可知共有四个满足方程E的点，为别为$(1,1), (1,6), (4,2), (4,5)$。

§3.2 模数为奇素数的二次剩余和二次非剩余

- 本节讨论m为奇素数p时(3.6)是否有解的问题。

- 定理3.2.1 （欧拉判别法）设p为奇素数，$(a,p)=1$，则

(i) a是模p的二次剩余当且仅当$a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$;

(ii) a是模p的二次非剩余当且仅当$a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$。

且若a是模p的二次剩余，则同余式$x^2 \equiv a \ (mod\ p)$恰有2解。

证明：如果a是模p的二次剩余，则存在$x \equiv x_0 \ (mod\ p)$是同余式$x^2 \equiv a \ (mod\ p)$的解，显然有$x \equiv p - x_0 \ (mod\ p)$也是$x^2 \equiv a \ (mod\ p)$的解，且$p - x_0 \not\equiv x_0 (mod\ p)$，所以$x^2 \equiv a \ (mod\ p)$恰有2个解。

又因为p为奇素数，因此$x^{p-1} - 1 = \left((x^2)^{\frac{p-1}{2}} - a^{\frac{p-1}{2}}\right) + \left(a^{\frac{p-1}{2}} - 1\right) = (x^2 - a)q(x) + \left(a^{\frac{p-1}{2}} - 1\right)$，其中$q(x)$为整系数多项式。由欧拉定理知所有与$p$互素的整数都是$x^{p-1} - 1 \equiv 0 \ (mod\ p)$的解，因此也是$(x^2 - a)q(x) + \left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \ (mod\ p)$的解，所以$x^2 \equiv a \ (mod\ p)$有2个解当且仅当$a^{\frac{p-1}{2}} - 1 \equiv 0 \ (mod\ p)$至少有2个解，当且仅当$a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$。即 (i) 得证。

再来证(ii)，因为$(a,p)=1$，由欧拉定理知$a^{p-1}-1=(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1)\equiv 0\ (mod\ p)$，又由$(i)$ 知a是模p的二次剩余当且仅当$a^{\frac{p-1}{2}}\equiv 1\ (mod\ p)$，所以$a$是模$p$的二次非剩余当且仅当$a^{\frac{p-1}{2}}+1\equiv 0\ (mod\ p)$，$(ii)$ 得证。

- 推论 设p是奇素数，$a,b \in Z, (a,p)=(b,p)=1$，则

(i) 如果a,b都是模p的二次剩余，那么ab也是模p的二次剩余；
(ii)如果a,b一个是模p的二次剩余，一个是模p的二次非剩余，那么ab是模p的二次非剩余；

(iii) 如果a,b都是模p的二次非剩余，那么ab是模p的二次剩余。

例：判断3是否为模7的二次剩余

例：判断3是否为模7的二次剩余

解：计算$a^{\frac{p-1}{2}}$=$3^3 \equiv -1(mod\ 7)$，所以3为模7二次非剩余。

- 定理3.2.2 设p是奇素数，则模p的简化剩余系中，二次剩余和二次非剩余的个数都是$\frac{p-1}{2}$个，且$\frac{p-1}{2}$个二次剩余和序列

$$1^2, 2^2, \dots, (\frac{p-1}{2})^2$$

中的一个数且仅和其中一个数同余。

证明：先证第一部分。

由定理3.2.1知模p的二次剩余的个数和同余式$x^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$的解数相同，又因为$\left(x^{\frac{p-1}{2}}-1\right) | (x^{p-1}-1) \equiv (x-1)\cdots(x-p+1)(mod\ p)$，因此$x^{\frac{p-1}{2}}-1 \equiv (x-b_{i_1})(x-b_{i_2})\cdots(x-b_{i_{\frac{p-1}{2}}})\ (mod\ p)$，其中$0<b_{i_1}<b_{i_2}<\cdots<b_{i_{\frac{p-1}{2}}}<p$，因此$x^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$共有$\frac{p-1}{2}$个非零解，即模$p$的二次剩余的个数为$\frac{p-1}{2}$。又因为模$p$的缩系中共有$p-1$个数，因此模$p$的二次非剩余的个数也是$\frac{p-1}{2}$。

再证第二部分。只需证明 $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ 模 p 两两不同余即可。用反证法，设存在整数 $1 \le j < i \le \frac{p-1}{2}$，使得 $i^2 \equiv j^2\ (mod\ p)$，则$(i-j)(i+j) \equiv 0\ (mod\ p)$，由于$p$是素数，因此有$p|(i-j)$或$p|(i+j)$，又因为$1 \le j < i \le \frac{p-1}{2}$，因此$0 < i-j < \frac{p-1}{2}$和$2 \le i+j \le p-1$，所以有$p \nmid (i-j), p \nmid (i+j)$，矛盾。

- §3.1中例：因为$1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 2, 4^2 \equiv 2, 5^2 \equiv 4, 6^2 \equiv 1 (mod\ 7)$，所以1，2，4是模7的二次剩余，3，5，6是模7的二次非剩余。

§3.3 勒让德符号

- 定义3.3.1 （勒让德符号）设p为素数，则定义勒让德符号

$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{若}a\text{是模}p\text{的二次剩余}\\ -1 & \text{若}a\text{是模}p\text{的二次非剩余}\\ 0 & \text{若}p|a\end{cases}$$

- 显然同余式$x^2 \equiv a \ (mod\ p)$有非零解当且仅当$\left(\frac{a}{p}\right)$ =1。

- 显然同余式$x^2 \equiv a \ (mod\ p)$有非零解当且仅当$\left(\frac{a}{p}\right)$ =1。

- 例： 因为1，2，4是模7的二次剩余，3，5，6是模7的二次非剩余，所以$\left(\frac{1}{7}\right)$ =1，$\left(\frac{2}{7}\right)$ =1，$\left(\frac{4}{7}\right)$ =1，$\left(\frac{3}{7}\right)$ =-1，$\left(\frac{5}{7}\right)$ =-1，$\left(\frac{6}{7}\right)$ =-1。

- 此时我们可将欧拉判别法重写为：

- 定理3.3.1 （欧拉判别法）设p为奇素数，则对任意整数a，都有

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\ p)$$

- 推论：设p为奇素数，则

$$\left(\frac{1}{p}\right) = 1$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

- 推论：设p为奇素数，则

$$\left(\frac{1}{p}\right) = 1$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

或者

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & 若p \equiv 1 \ (mod\ 4) \\ -1 & 若p \equiv 3 \ (mod\ 4) \end{cases}$$

- 定理3.3.2 设p为奇素数，则

(i) $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$;

(ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$，进一步有$\left(\frac{a_1a_2\cdots a_n}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)$;

(iii) 如果$(a,p)=1$，那么$\left(\frac{a^2}{p}\right)=1$。

证明： (i)显然。

现在证 (ii) 。由欧拉判别法知$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \,(mod\,p), \left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \,(mod\,p), \left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \,(mod\,p)$，因此$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \,(mod\,p)$，所以$p \left| \left(\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right)\right.$，又因为$\left|\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right| \leq 2 < p$，所以$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0$，得证。

由(ii)可直接得(iii) 。

- 推论：

(i)若$a \equiv b \ (mod\ p)$，则$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$；

(ii) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$。

- 例：判断下列二次同余式是否有解：

$(i)\ x^2-3x+5\equiv 0\ (mod\ 7)$，

$(ii) 5x^2-7x+11\equiv 0\ (mod\ 23)$。

- 例：判断下列二次同余式是否有解：

$(i)\ x^2-3x+5\equiv 0\ (mod\ 7)$，

$(ii) 5x^2-7x+11\equiv 0\ (mod\ 23)$。

解：(i) 因为$x^2-3x+5\equiv x^2+4x+5=(x+2)^2+1\ (mod\ 7)$，因此$(i)$ 有解等价于$y^2\equiv -1\ (mod\ 7)$有解，但我们知道$\left(\frac{-1}{7}\right)=-1$，因此$-1$是模7的二次非剩余，因此二次同余式$(i)$无解。

EAST CHINA NORMAL UNIVERSITY 華東師範大學

- 例：判断下列二次同余式是否有解：

$(i)\ x^2-3x+5\equiv 0\ (mod\ 7)$，

$(ii) 5x^2-7x+11\equiv 0\ (mod\ 23)$。

解：(i) 因为$x^2-3x+5\equiv x^2+4x+5=(x+2)^2+1\ (mod\ 7)$，因此$(i)$ 有解等价于$y^2\equiv -1\ (mod\ 7)$有解，但我们知道$\left(\frac{-1}{7}\right)=-1$，因此$-1$是模7的二次非剩余，因此二次同余式$(i)$无解。

(ii)因为$5x^2-7x+11\equiv 5x^2-30x-35=5(x^2-6x-7)=5\left((x-3)^2-16\right)\ (mod\ 23)$，又因为$(5,23)=1$，因此$(ii)$有解等价于$y^2\equiv 16\ (mod\ 23)$有解，但我们知道$\left(\frac{16}{23}\right)=\left(\frac{4}{23}\right)^2=1$，因此二次同余式$(ii)$有解。

- 定理3.3.3 （高斯引理） 设p为奇素数，$(a,p)=1$，如果整数$a\ (mod\ p), 2a\ (mod\ p), \dots, \frac{p-1}{2}a\ (mod\ p)$中大于$\frac{p}{2}$的个数是$m$，则$\left(\frac{a}{p}\right)=(-1)^m$。

- 例： 计算7是不是模11的二次非剩余。

- 例： 计算7是不是模11的二次非剩余。

解：因为$p=11, a=7$，且$(a,p)=1$，计算
$a\ (mod\ p), 2a\ (mod\ p), \ldots, \frac{p-1}{2}a\ (mod\ p) = 7, 14,21,28,35 \equiv 7,3,10,6,2\ (mod\ 11)$,其中大于$\frac{p}{2}=5.5$的有3个，因此$\left(\frac{7}{11}\right) = (-1)^3 = -1$，故7是模11的二次非剩余。

- 例： 计算7是不是模11的二次非剩余。

解：因为$p=11, a=7$，且$(a,p)=1$，计算
$a\ (mod\ p), 2a\ (mod\ p), \ldots, \frac{p-1}{2}a\ (mod\ p) = 7, 14,21,28,35 \equiv$
$7,3,10,6,2\ (mod\ 11)$,其中大于$\frac{p}{2}=5.5$的有3个，因此$\left(\frac{7}{11}\right)=$
$(-1)^3=-1$，故7是模11的二次非剩余。
另一方面，我们计算 $1^2, 2^2, 3^2, 4^2, 5^2 \equiv 1,4,9,5,3\ \ (mod\ 11)$ ，因此验证了7是模11的二次非剩余。

证明定理3.3.3：

设$a_1, a_2, \dots, a_s$表示$a \pmod p, 2a \pmod p, \dots, \frac{p-1}{2} a \pmod p$中小于$\frac{p}{2}$的数，$b_1, b_2, \dots, b_m$表示大于$\frac{p}{2}$的数，则显然有$s+m=\frac{p-1}{2}$，且

$$\prod_{i=1}^{s} a_i \prod_{j=1}^{m} b_j \equiv \prod_{i=1}^{\frac{p-1}{2}} ia = \left(\frac{p-1}{2}\right)! \, a^{\frac{p-1}{2}} \pmod p$$

因为$\frac{p}{2} < b_1, b_2, \dots, b_m < p$，因此$0 < p-b_1, p-b_2, \dots, p-b_m < \frac{p}{2}$，观察$a_1, a_2, \dots, a_s, p-b_1, p-b_2, \dots, p-b_m$这$\frac{p-1}{2}$个数，我们证明它们各不相同。

否则其中有2个数x, y，使得$x \equiv y\ (mod\ p)$，则存在整数$k, l, 1 < k, l \leq \frac{p-1}{2}$，使得$x \equiv \pm ka\ (mod\ p), y \equiv \pm la\ (mod\ p)$，此时有$k^2a^2 \equiv x^2 \equiv y^2 \equiv l^2a^2\ (\mathrm{mod\ p})$，因此$p|a^2(k+l)(k-l)$，因为$p$是素数且$(a,p)=1$，$p \nmid a^2$，故$p|(k+l)(k-l)$，又因为$0 < k < l \leq \frac{p-1}{2}$，因此$0 < k+l \leq p-1, 0 < |k-l| < \frac{p-1}{2}$，所以$p \nmid (k+l), p \nmid (k-l)$，矛盾，所以$a_1, a_2, \ldots, a_s, p-b_1, p-b_2, \ldots, p-b_m$互不相同。因此

$$\prod_{i=1}^{s} a_i \prod_{j=1}^{m} (p-b_j) = \prod_{i=1}^{\frac{p-1}{2}} i = \left(\frac{p-1}{2}\right)!$$

此时有

$$\left(\frac{p-1}{2}\right)!\,a^{\frac{p-1}{2}} \equiv \prod_{i=1}^{s} a_i \prod_{j=1}^{m} b_j \equiv (-1)^m \prod_{i=1}^{s} a_i \prod_{j=1}^{m} (p-b_j) =$$

$$= (-1)^m \left(\frac{p-1}{2}\right)!\,(mod\ p)$$

由于p为素数，所以$\left(p,\left(\frac{p-1}{2}\right)!\right)=1$，故$a^{\frac{p-1}{2}} \equiv (-1)^m\ (mod\ p)$，又因为$a^{\frac{p-1}{2}}$和$(-1)^m$都为$\pm 1$，因此$\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}}=(-1)^m$。

- 定理3.3.4 设p为奇素数，则

(i) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$，

(ii) 设$(a, 2p) = 1$，则

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right]}$$

其中$[x]$表示不大于x的最大整数。

证明：因为对所有的 $k=1,2,\ldots,\frac{p-1}{2}$，都存在整数 $r_k, 0\le r_k<p$，使得$ak=p\left[\frac{ak}{p}\right]+r_k$，则

$$\sum_{k=1}^{\frac{p-1}{2}} ak=\sum_{k=1}^{\frac{p-1}{2}}(p\left[\frac{ak}{p}\right]+r_k)$$

令$a_1,a_2,\ldots,a_s,b_1,b_2,\ldots,b_m$如定理3.3.3证明中定义，则对$k=1,2,\ldots,\frac{p-1}{2}$，都有唯一一个$a_i$或$b_i$与$r_k$相等，因此上式可化为

华东师范大学 EAST CHINA NORMAL UNIVERSITY

$$\begin{aligned}\frac{p^2-1}{8}a &= \sum_{k=1}^{\frac{p-1}{2}} p\left[\frac{ak}{p}\right]+\sum_{i=1}^{s} a_i+\sum_{i=1}^{m} b_i \\ &= \sum_{k=1}^{\frac{p-1}{2}} p\left[\frac{ak}{p}\right]+\sum_{i=1}^{s} a_i+\sum_{i=1}^{m}(p-b_i)+2\sum_{i=1}^{m} b_i-mp \\ &= \sum_{k=1}^{\frac{p-1}{2}} p\left[\frac{ak}{p}\right]+\frac{p^2-1}{8}-mp+2\sum_{i=1}^{m} b_i\end{aligned}$$

所以$\frac{p^2-1}{8}(a-1) \equiv \sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right]+m \ (mod\ 2)$

若$a=2$，则对所有的$k=1,2,\ldots,\frac{p-1}{2}$，都有$0<2k<p$，因此$\left[\frac{ak}{p}\right]=0$，此时有$\frac{p^2-1}{8}\equiv m\ (mod\ 2)$，因此$\left(\frac{2}{p}\right)=(-1)^m=(-1)^{\frac{p^2-1}{8}}$。

若$(a,2p)=1$，则a为奇数，此时$\frac{p^2-1}{8}(a-1)\equiv 0\ (\mathrm{mod}\ 2)$，因此有$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right]\equiv m\ (mod\ 2)$，所以$\left(\frac{a}{p}\right)=(-1)^m=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right]}$。

- 推论 设p为奇素数，则

$$\left(\frac{2}{p}\right)=\begin{cases}1 & 若p\equiv\pm1\ (mod\ 8)\\ -1 & 若p\equiv\pm3\ (mod\ 8)\end{cases}$$

- 推论 设p为奇素数，则

$$\left(\frac{2}{p}\right)=\begin{cases}1 & 若p\equiv \pm 1\ (mod\ 8)\\ -1 & 若p\equiv \pm 3\ (mod\ 8)\end{cases}$$

- 例 因为$7\equiv -1\ (mod\ 8), 11\equiv 3\ (mod\ 8)$，因此$\left(\frac{2}{7}\right)=1$，$\left(\frac{2}{11}\right)=-1$，故2是模7的二次剩余，是模11的二次非剩余。

§3.4 二次互反律

- 定理3.4.1 （二次互反律）设p, q为不同的奇素数，则

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

- 例 判断同余式$x^2 \equiv -1 \ (mod\ 365)$是否有解，若有解，求其解数。

- 例 判断同余式$x^2 \equiv -1 \pmod{365}$是否有解，若有解，求其解数。

解：因为365的标准分解式为$365 = 5 \times 73$，故求解同余式$x^2 \equiv -1 \pmod{365}$等价于求解同余式组

$$\begin{cases} x^2 \equiv -1 \pmod{5} \\ x^2 \equiv -1 \pmod{73} \end{cases}$$

因为$\left(\frac{-1}{5}\right) = (-1)^{\frac{5-1}{2}} = 1, \left(\frac{-1}{73}\right) = (-1)^{\frac{73-1}{2}} = 1$，因此上述同余式组有解，且解数为$2 \times 2 = 4$，故同余式$x^2 \equiv -1 \pmod{365}$有解，解数为4。

- 例 判断同余式$x^2 \equiv -1 \ (mod\ 365)$是否有解，若有解，求其解数。

解：因为365的标准分解式为$365 = 5 \times 73$，故求解同余式$x^2 \equiv -1 \ (mod\ 365)$等价于求解同余式组

$$\begin{cases} x^2 \equiv -1 \ (mod\ 5) \\ x^2 \equiv -1 \ (mod\ 73) \end{cases}$$

因为$\left(\frac{-1}{5}\right) = (-1)^{\frac{5-1}{2}} = 1, \left(\frac{-1}{73}\right) = (-1)^{\frac{73-1}{2}} = 1$，因此上述同余式组有解，且解数为$2 \times 2 = 4$，故同余式$x^2 \equiv -1 \ (mod\ 365)$有解，解数为4。事实上，$x \equiv 73 \cdot 2 \cdot \pm 2 + 5 \cdot 44 \cdot \pm 27 \equiv \pm 27, \pm 173 \ (mod\ 365)$是$x^2 \equiv -1 \ (mod\ 365)$的全部解。

- 例 判断同余式$x^2 \equiv 429\ (mod\ 563)$是否有解，若有解，求其解数。

- 例 判断同余式$x^2 \equiv 429 \ (mod\ 563)$是否有解，若有解，求其解数。

解：易知563是素数，故$\left(\frac{429}{563}\right)=\left(\frac{3\cdot 11\cdot 13}{563}\right)=\left(\frac{3}{563}\right)\left(\frac{11}{563}\right)\left(\frac{13}{563}\right)$，

而$\left(\frac{3}{563}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{3}\right)=(-1)\left(\frac{2}{3}\right)=(-1)\cdot(-1)^{\frac{3^2-1}{8}}=1$,

$\left(\frac{11}{563}\right)=(-1)^{\frac{11-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{11}\right)=(-1)\left(\frac{2}{11}\right)=(-1)\cdot(-1)^{\frac{11^2-1}{8}}=1$,

$\left(\frac{13}{563}\right)=(-1)^{\frac{13-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{13}\right)=\left(\frac{4}{13}\right)=1$,

所以$\left(\frac{429}{563}\right)=1$，因此同余式$x^2 \equiv 429 \ (mod\ 563)$有解，其解数为2。

- 例 证明形如$4k+1$的素数有无穷多个。

- 例 证明形如$4k+1$的素数有无穷多个。

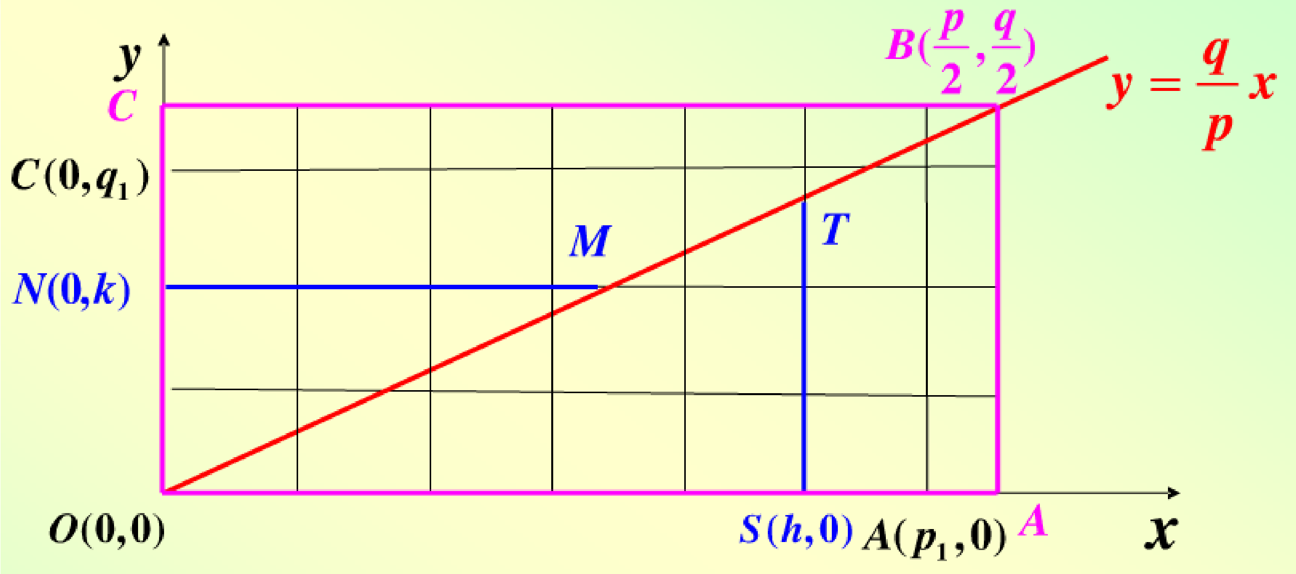
证明：用反证法，设形如$4k+1$的素数有有限多个，令其为$p_1, p_2, \ldots, p_s$，再令$n=(2p_1p_2\cdots p_s)^2+1$，显然$n$也是一个$4k+1$形的数，且对$i=1,2,\ldots,s$，都有$n>p_i$，因此$n$为合数，故必有素因子$p$，此时$\left(\frac{-1}{p}\right)=\left(\frac{-1+n}{p}\right)=\left(\frac{(2p_1p_2\cdots p_s)^2}{p}\right)=1$，由定理3.3.1推论知$p$也是形如$4k+1$的素数，因此存在$1\leq i\leq s$，使得$p=p_i$，但由$n$定义显然对所有$i=1,2,\ldots,s$，都有$(p_i,n)=1$，矛盾。

证明定理3.4.1：

显然只需证明$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$，由定理3.3.4知$\left(\frac{q}{p}\right)=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{qk}{p}\right]}$, $\left(\frac{p}{q}\right)=(-1)^{\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{pk}{q}\right]}$，因此仅需证明$\frac{p-1}{2}\cdot\frac{q-1}{2}=\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{qk}{p}\right]+\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{pk}{q}\right]$。

令$p_1=\frac{p-1}{2}, q_1=\frac{q-1}{2}$，考察长为$\frac{p}{2}$，宽为$\frac{q}{2}$的矩形$OABC$，如图所示

在直线ST上，恰有$\left[\frac{qh}{p}\right]$个正整数点，在直线$NM$上，恰有$\left[\frac{pk}{q}\right]$个正整数点，且因为$p,q$为不同的素数，因此直线$y=\frac{q}{p}x$在矩形$OABC$内无整数点，因此$\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{qk}{p}\right]+\sum_{k=1}^{\frac{q-1}{2}}\left[\frac{pk}{q}\right]$等于矩形$OABC$所有整数点的个数，显然为$\frac{p-1}{2}\cdot\frac{q-1}{2}$，得证。



- 例 求所有以3为二次剩余的奇素数p 。

- 例 求所有以3为二次剩余的奇素数p 。

解：因为$\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right)$，因此3是模$p$的二次剩余等价于$(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$=1。显然有$(-1)^{\frac{p-1}{2}}=\begin{cases}1 & 若p\equiv 1\ (mod\ 4)\\ -1 & 若p\equiv -1\ (mod\ 4)\end{cases}$和

$\left(\frac{p}{3}\right)=\begin{cases}\left(\frac{1}{3}\right)=1 & 若p\equiv 1\ (mod\ 3)\\ \left(\frac{-1}{3}\right)=-1 & 若p\equiv -1\ (mod\ 3)\end{cases}$，则3是模$p$的二次剩余的充要条件为$\begin{cases}p\equiv 1\ (mod\ 4)\\ p\equiv 1\ (mod\ 3)\end{cases}$或$\begin{cases}p\equiv -1\ (mod\ 4)\\ p\equiv -1\ (mod\ 3)\end{cases}$，由孙子定理可知，即为$p\equiv \pm 1\ (mod\ 12)$。

§3.5 雅可比符号

- 定义3.5.1 （雅可比符号）设正奇数m 表示为奇素数的乘积形式$m = p_1 p_2 \cdots p_s$，则对任意整数a，定义雅可比符号

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right)$$

其中$\left(\frac{a}{p_i}\right)$是$a$对$p_i$的勒让德符号。

- 雅可比符号是勒让德符号在一般奇数m上的推广。

- 雅可比符号是勒让德符号在一般奇数m上的推广。

- 勒让德符号的值可确定a是否是模p的二次剩余；
  但雅可比符号的值不能完全确定a是否是模m的二次剩余。

- 例：$\left(\frac{3}{119}\right)=\left(\frac{3}{7}\right)\left(\frac{3}{17}\right)=(-1)^{\frac{7-1}{2}\cdot\frac{3-1}{2}}\left(\frac{7}{3}\right)(-1)^{\frac{17-1}{2}\cdot\frac{3-1}{2}}\left(\frac{17}{3}\right)=$ $(-1)\left(\frac{1}{3}\right)\left(\frac{2}{3}\right)=(-1)(-1)=1$。

另一方面，求解同余式$x^2\equiv 3\ (mod\ 119)$等价于求解同余式组

$$\begin{cases} x^2\equiv 3\ (mod\ 7) \\ x^2\equiv 3\ (mod\ 17) \end{cases}$$

但由上式计算可知$\left(\frac{3}{7}\right)=-1$，因此同余式$x^2\equiv 3\ (mod\ 119)$无解，即3是模119的二次非剩余。

- 定理3.5.1 设m为正奇数，a为奇数，若$\left(\frac{a}{m}\right) = -1$，则$a$是模$m$的二次非剩余。

- 定理3.5.1 设m为正奇数，a为奇数，若$\left(\frac{a}{m}\right)=-1$，则$a$是模$m$的二次非剩余。

证明：设$m=p_1p_2\cdots p_s$，其中$p_1,p_2,\ldots,p_s$为奇素数，则同余式$x^2\equiv a\ (mod\ m)$等价于求解同余式组

$$\begin{cases} x^2\equiv a\ (mod\ p_1) \\ \cdots \\ x^2\equiv a\ (mod\ p_s) \end{cases}$$

又因为$\left(\frac{a}{m}\right)=-1$，因此$\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right)=-1$，所以存在$1\le k\le s$，使得$\left(\frac{a}{p_k}\right)=-1$，此时$x^2\equiv a\ (mod\ p_k)$无解，因此$x^2\equiv a\ (mod\ m)$无解，即$a$是模$m$的二次非剩余。

- 定理3.5.2 （雅可比符号的性质）

若a,b是整数，m,n是正奇数，则

(i) $\left(\frac{a+m}{m}\right)=\left(\frac{a}{m}\right)$

(ii) $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$

(iii) $\left(\frac{a^2}{m}\right)=1$

(iv) $\left(\frac{1}{m}\right)=1$

(v) $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$

(vi) $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$

(vii) $\left(\frac{n}{m}\right)=(-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}\left(\frac{m}{n}\right)$（二次互反律）

类似于勒让德符号，有了定理5.3.2的性质，我们对任意给定的正奇数m,n，都可以计算雅可比符号$\left(\frac{n}{m}\right)$，其中(i)- (iv)可由雅可比符号定义直接推出，而(v)-(vii)的证明需要如下引理：

- 引理3.5.1 设m是正奇数，且$m = p_1 p_2 \cdots p_s$是m的素因子分解，则有

(a) $\sum_{i=1}^{s}(p_i - 1) \equiv \prod_{i=1}^{s} p_i - 1 \ (mod\ 4)$

(b) $\sum_{i=1}^{s}(p_i^2 - 1) \equiv \prod_{i=1}^{s} p_i^2 - 1 \ (mod\ 16)$

证明：因为m是正奇数，则显然$p_i, 1 \leq i \leq s$都是奇素数，则存在正整数$k_i, 1 \leq i \leq s$，使得$p_i = 2k_i + 1$，

(a) 此时有$\prod_{i=1}^{s} p_i - 1 = \prod_{i=1}^{s}(2k_i + 1) - 1 \equiv \sum_{i=1}^{s}(2k_i) + 1 - 1 = \sum_{i=1}^{s}(2k_i) = \sum_{i=1}^{s}(p_i - 1)\ (mod\ 4)$

(b) 也有$\prod_{i=1}^{s} p_i^2 - 1 = \prod_{i=1}^{s}(2k_i + 1)^2 - 1 = \prod_{i=1}^{s}(4k_i(k_i + 1) + 1) - 1 \equiv \sum_{i=1}^{s}\big(4k_i(k_i + 1)\big) + 1 - 1 = \sum_{i=1}^{s}\big(4k_i(k_i + 1)\big) = \sum_{i=1}^{s}\big(p_i^2 - 1\big)\ (mod\ 16)$

由引理5.3.1(a)可得 $\sum_{i=1}^{s}\frac{p_i-1}{2}\equiv\frac{\prod_{i=1}^{s}p_i-1}{2}\ (mod\ 2)$，因此有$\left(\frac{-1}{m}\right)=\prod_{i=1}^{s}\left(\frac{-1}{p_i}\right)=\prod_{i=1}^{s}(-1)^{\frac{p_i-1}{2}}=(-1)^{\sum_{i=1}^{s}\frac{p_i-1}{2}}=(-1)^{\frac{\prod_{i=1}^{s}p_i-1}{2}}=(-1)^{\frac{m-1}{2}}$，定理5.3.2$(v)$得证；

类似的，由引理5.3.1(b)可得$\sum_{i=1}^{s}\frac{p_i^2-1}{8}\equiv\frac{\prod_{i=1}^{s}p_i^2-1}{8}\ (mod\ 2)$，进一步有$\left(\frac{2}{m}\right)=\prod_{i=1}^{s}\left(\frac{2}{p_i}\right)=\prod_{i=1}^{s}(-1)^{\frac{p_i^2-1}{8}}=(-1)^{\sum_{i=1}^{s}\frac{p_i^2-1}{8}}=(-1)^{\frac{\prod_{i=1}^{s}p_i^2-1}{8}}=(-1)^{\frac{m^2-1}{8}}$，定理5.3.2$(vi)$得证；

再设$n=q_1q_2\cdots q_t$是n的标准分解式，仍由引理5.3.1(a)可知 $\sum_{j=1}^{t}\frac{q_j-1}{2}\equiv\frac{\prod_{j=1}^{t}q_j-1}{2}\ (mod\ 2)$，从而有 $\sum_{i=1}^{s}\frac{p_i-1}{2}\cdot\sum_{j=1}^{t}\frac{q_j-1}{2}\equiv\frac{\prod_{i=1}^{s}p_i-1}{2}\cdot\frac{\prod_{j=1}^{t}q_j-1}{2}\ (mod\ 2)$，因此$\left(\frac{n}{m}\right)\cdot\left(\frac{m}{n}\right)=\prod_{i=1}^{s}\prod_{j=1}^{t}\left(\left(\frac{q_j}{p_i}\right)\cdot\left(\frac{p_i}{q_j}\right)\right)=\prod_{i=1}^{s}\prod_{j=1}^{t}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}=(-1)^{\sum_{i=1}^{s}\sum_{j=1}^{t}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}=(-1)^{\frac{\prod_{i=1}^{s}p_i-1}{2}\cdot\frac{\prod_{j=1}^{t}q_j-1}{2}}=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$，定理5.3.2$(vii)$得证。

华东师范大学
EAST CHINA NORMAL UNIVERSITY

- 例 判断同余式$x^2 \equiv 286 \ (mod\ 563)$是否有解。

- 例 判断同余式$x^2 \equiv 286 \ (mod\ 563)$是否有解。

解：求286对563的雅可比符号，

$$\left(\frac{286}{563}\right) = \left(\frac{2\cdot 143}{563}\right) = \left(\frac{2}{563}\right)\left(\frac{143}{563}\right) = (-1)^{\frac{563^2-1}{8}}(-1)^{\frac{143-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{143}\right)$$

$$= (-1)\cdot(-1)\cdot\left(\frac{-9}{143}\right) = \left(\frac{-1}{143}\right)\left(\frac{3^2}{143}\right) = (-1)^{\frac{143-1}{2}}\cdot 1 = -1,$$

所以同余式$x^2 \equiv 286 \ (mod\ 563)$无解。

- 算法3.1（模p平方根算法）设p为奇素数，a为整数，且$\left(\frac{a}{p}\right)=1$，则同余式$x^2 \equiv a\ (mod\ p)$的算法如下：

令$p-1=2^t\cdot s$，其中s为奇数，且$t\geq 1$，计算$x_{t-1}=a^{\frac{s+1}{2}}\ (mod\ p)$

(i) 如果$t=1$，则有$x_{t-1}^2=x_0^2\equiv a^{s+1}=a^{\frac{p-1}{2}}\cdot a\equiv\left(\frac{a}{p}\right)\cdot a=a\ (mod\ p)$，因此$x_0$即为同余式$x^2\equiv a\ (mod\ p)$的解。

(ii) 否则，任取模p的二次非剩余n，则$\left(\frac{n}{p}\right)=-1$，计算$b=n^s\ (mod\ p)$，则有$b^{2^t}\equiv n^{2^t\cdot s}=n^{p-1}\equiv 1\ (mod\ p)$，且$b^{2^{t-1}}=n^{\frac{p-1}{2}}\equiv -1\ (mod\ p)$。同理可知$(a^{-1}x_{t-1}^2)^{2^{t-1}}\equiv 1\ (mod\ p)$。

(iii) 设已求得$x_{t-1}, x_{t-2}, \ldots, x_{t-k}$，满足$(a^{-1}x_{t-i}^2)^{2^{t-i}} \equiv 1 \pmod p, i = 1,2,\ldots,k$，现在计算$x_{t-k-1}$使得$(a^{-1}x_{t-k-1}^2)^{2^{t-k-1}} = 1 \pmod p$：

(a) 若$(a^{-1}x_{t-k}^2)^{2^{t-k-1}} = 1 \pmod p$，则令$j_{k-1} = 0, x_{t-k-1} \equiv x_{t-k} = x_{t-k} b^{j_{k-1} \cdot 2^{k-1}} \pmod p$，

(b) 否则有$(a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv -1 \equiv (b^{-2^k})^{2^{t-k-1}} \pmod p$，令$j_{k-1}$ =1, $x_{t-k-1} \equiv x_{t-k} b^{2^{k-1}} = x_{t-k} b^{j_{k-1} \cdot 2^{k-1}} \pmod p$，此时有

$$(a^{-1}x_{t-k-1}^2)^{2^{t-k-1}} \equiv \left(a^{-1}x_{t-k}^2 b^{2^k}\right)^{2^{t-k-1}} = \left(a^{-1}x_{t-k}^2\right)^{2^{t-k-1}} \cdot \left(b^{2^k}\right)^{2^{t-k-1}} \equiv \left(b^{-2^k}\right)^{2^{t-k-1}} \cdot \left(b^{2^k}\right)^{2^{t-k-1}} \equiv 1 \pmod p$$

(iv) 特别的，当$k=t-1$时，(iii)计算得到的x_0满足$(a^{-1}x_0^2)^{2^0}=1\ (mod\ p)$，即$x_0$为同余式$x^2\equiv a\ (mod\ p)$的解。此时

$$x_0\equiv x_1 b^{j_{t-2}\cdot 2^{t-2}}\equiv\cdots\equiv x_{t-1}b^{j_{t-2}\cdot 2^{t-2}+\cdots+j_0\cdot 2^0}$$
$$\equiv a^{\frac{s+1}{2}}b^{j_{t-2}\cdot 2^{t-2}+\cdots+j_0\cdot 2^0}(mod\ p)$$

- 例 求解同余式$x^2 \equiv 186\ (mod\ 401)$。

- 例 求解同余式$x^2 \equiv 186\ (mod\ 401)$。

解：易知401为素数，计算$\left(\frac{186}{401}\right) = \left(\frac{2}{401}\right)\left(\frac{3}{401}\right)\left(\frac{31}{401}\right) = (-1)^{\frac{401^2-1}{8}} \cdot (-1)^{\frac{3-1}{2}\cdot\frac{401-1}{2}}\left(\frac{401}{3}\right) \cdot (-1)^{\frac{31-1}{2}\cdot\frac{401-1}{2}}\left(\frac{401}{31}\right) = 1 \cdot 1 \cdot \left(\frac{2}{3}\right) \cdot 1 \cdot \left(\frac{-2}{31}\right) = \left(\frac{2}{3}\right)\left(\frac{-1}{31}\right)\left(\frac{2}{31}\right) = (-1) \cdot (-1) \cdot 1 = 1$，因此同余式$x^2 \equiv 186\ (mod\ 401)$有2个解。

因为$p - 1 = 400 = 2^4 \cdot 25$，即$t = 4, s = 25$，取一个模$p$的二次非剩余3，计算$b = 3^{25} \equiv 268\ (mod\ 401), x_3 = 186^{\frac{25+1}{2}} \equiv 103\ (mod\ 401), 186^{-1} \equiv 235\ (mod\ 401)$。

计算$(186^{-1}\cdot x_3^2)^{2^2}\equiv(235\cdot 103^2)^4\equiv -1\ (mod\ 401)$，因此令$j_0=1, x_2=x_3 b^{j_0}\equiv 103\cdot 268\equiv 336\ (mod\ 401)$;

再计算$(186^{-1}\cdot x_2^2)^{2^1}\equiv(235\cdot 336^2)^2\equiv 1\ (mod\ 401)$，因此令$j_1=0, x_1=x_2 b^{j_1\cdot 2}=336\ (mod\ 401)$;

最后计算$(186^{-1}\cdot x_1^2)^{2^0}\equiv(235\cdot 336^2)^1\equiv -1\ (mod\ 401)$，因此令$j_2=1, x_0=x_1 b^{j_2\cdot 4}\equiv 336\cdot 268^4\equiv 304\ (mod\ 401)$。

所以$x\equiv \pm x_0\equiv 304,97\ (mod\ 401)$是同余式$x^2\equiv 186\ (mod\ 401)$的所有解。