第4章 二次同余方程

引 子

在第3章介绍一次同余方程时, 讨论了形如 $ax \equiv b \pmod m$的同余方程有解的条件. 相似地, 二次同余方程$x^2 \equiv a \pmod m$ 有的有解, 有的无解, 下面举例说明.

【例4.1.1】 判断$x^2 \equiv 3 \pmod 5$是否有解.

解: 将模5的一个完全剩余系中的剩余逐个代入方程, 若有解, 则必有一个剩余满足方程. 这里取模5的最小非负完全剩余系{0,1,2,3,4}, 由于

$$0^2 \equiv 0,\quad 1^2 \equiv 4^2 \equiv 1,\quad 2^2 \equiv 3^2 \equiv 4.$$

可知方程无解.

引子

对于二次同余方程$x^2 \equiv a(\mathrm{mod}\, m)$, 由于$x^2 \equiv (m-x)^2(\mathrm{mod}\, m)$, 故只需代入0, 1, ..., $\left\lfloor\frac{m}{2}\right\rfloor$到方程中计算即可.

【例4.1.2】 判断$x^2 \equiv 5(\mathrm{mod}\ 11)$是否有解.

解: 方法如【例4.1.1】, 可知方程的解为$x \equiv 4, 7(\mathrm{mod} 11)$.

当m较小的时候, 穷举的方法可以判断$x^2 \equiv a(\mathrm{mod}\, m)$是否有解, 当$m$较大的时候, 这种方法的效率就比较低了. 下面讨论更为有效的办法.

平方剩余-定义

【定义4.1.1】 设$a \in Z, (a,m) = 1$, 如果同余方程$x^2 \equiv a (\mathrm{mod}\ m)$有解, 则$a$叫做模$m$的平方剩余, 否则叫做模$m$的平方非剩余.

平方剩余也叫二次剩余。

二次非剩余译自quadratic nonresidue, 也有教材称之为非二次剩余.

由【例4.1.1】和【4.1.2】知, 3是模5的平方非剩余, 而5是模11的平方剩余.

判断二次同余方程$x^2 \equiv a(\mathrm{mod}\ m)$ 是否有解, 也即判断a是否是模m的平方剩余. 我们先要判断a与m是否互素, 若互素, 再判断同余方程$x^2 \equiv a(\mathrm{mod}\ m)$是否有解. 例如, 虽然同余方程$x^2 \equiv 4(\mathrm{mod}\ 8)$有解, 但4不叫做模8的平方剩余, 因为(4,8)=4≠1.

平方剩余-例题

【例4.1.3】 求模7的平方剩余.

对于同余方程$x^2 \equiv a(\mathrm{mod} 7)$, 满足$(a, 7) = 1$的$a$有1, 2, 3, 4, 5, 6共6种取值, 采用【例4.1.1】的方法, 其解在集合{0, 1, 2, 3, 4, 5, 6}中, 故进行如下计算:

a取1时, $x^2 \equiv 1(\mathrm{mod}\ 7)$的解为$x \equiv 1,6(\mathrm{mod}\ 7)$.

a取2时, $x^2 \equiv 2(\mathrm{mod}\ 7)$的解为$x \equiv 3,4(\mathrm{mod}\ 7)$.

a取3时, $x^2 \equiv 3(\mathrm{mod}\ 7)$无解.

a取4时, $x^2 \equiv 4(\mathrm{mod}\ 7)$的解为$x \equiv 2,5(\mathrm{mod}\ 7)$.

a取5时, $x^2 \equiv 5(\mathrm{mod}\ 7)$无解.

a取6时, $x^2 \equiv 6(\mathrm{mod}\ 7)$无解.

故1, 2, 4为模7的平方剩余, 而3, 5, 6为模7的平方非剩余.

平方剩余-欧拉判别条件

下面讨论模数为奇素数的二次剩余问题，即 $x^2 \equiv a(\mathrm{mod}p), p$为奇素数时的二次剩余问题.

【定理4.1.1】 设p为奇素数，设$a \in Z, (a, p) = 1$, 则

a是模p的平方剩余的充要条件是: $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$;

a是模p的平方非剩余的充要条件是: $a^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\, p)$.

且当a是模p的平方剩余时，同余方程恰有两个解. 这个结论称为欧拉判别条件.

由于定理的证明涉及到高次同余方程求解的相关知识, 这里仅对a是模p的平方剩余的必要条件是$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$做简单推导, 说明$a^{\frac{p-1}{2}} \pmod{p}$的值为什么要么是-1, 要么是1, 以方便理解.

因p为奇素数, 故$p-1$为偶数, $\frac{p-1}{2}$为整数. 因$(a,p)=1$, 由Fermat定理, $a^{p-1} \equiv 1 \pmod{p}$, 故

$$a^{p-1}-1 \equiv (a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1) \equiv 0 \pmod{p}.$$

即$p|a^{\frac{p-1}{2}}-1$或$p|a^{\frac{p-1}{2}}+1$. 故若a是模p的平方剩余, 则存在$(x')^2 \equiv a(\bmod p)$, 故

$$a^{\frac{p-1}{2}} \equiv ((x')^2)^{\frac{p-1}{2}} \equiv (x')^{p-1} \equiv 1 \pmod{p}.$$

平方剩余-例题

【例4.1.4】 用欧拉判别条件判断5是否为模13的平方剩余.

解: 由于$5^{\frac{13-1}{2}} \equiv 5^6 \equiv (5^2)^3 \pmod{13} \equiv (-1)^3 \equiv -1$, 故5是模13的平方非剩余.

由此可见, 用欧拉判别条件进行判断, 比用【例4.1.1】的方法易于得到结果. 另外, 用欧拉判别条件进行判断时, 通常会结合模重复平方法简化运算.

平方剩余-性质

【定理4.1.2】 设p为奇素数, 模p的平方剩余和平方非剩余的数量各为$\frac{p-1}{2}$个, 而且$\frac{p-1}{2}$个平方剩余分别与序列$1^2, 2^2, \ldots, (\frac{p-1}{2})^2$中之一数同余, 且仅与一数同余.

例如:

取p为3, 则平方剩余为1, 平方非剩余为2;

取 p 为5, 则平方剩余为$1^2=1$, $2^2=4$, 平方非剩余为2, 3;

取p为7, 则平方剩余为$1^2=1$, $2^2=4$, $3^2=9\equiv 2 \pmod 7$, 平方非剩余为3, 5, 6;

证明 易知若$x_1 + x_2 = p$. 则$x_1^2 \equiv x_1^2 (\mathrm{mod}\, p)$, 即$1^2 \equiv (p-1)^2, 2^2 \equiv (p-2)^2, \ldots, (\frac{p-1}{2})^2 \equiv (\frac{p+1}{2})^2$, 共有$(\frac{p-1}{2})$个数. 下面证明这$\left(\frac{p-1}{2}\right)$个数模$p$两两不同余.

反证法 不妨设$0 < x_1 < x_2 < p$, 且$x_1 + x_2 \neq p$. 此时若$x_1^2 \equiv x_2^2 (\mathrm{mod}\, p)$, 则$p | x_2^2 - x_1^2$. 即$p | (x_1 + x_2)(x_2 - x_1)$. 注意到$0 < x_1 + x_2 < 2p$, $0 < x_2 - x_1 < p$. 即$x_1 + x_2$与p互素, $x_1 - x_2$与p互素, $p | (x_1 + x_2)(x_2 - x_1)$不成立. 故若$x_1 + x_2 \neq p$, 则$x_1^2 \not\equiv x_2^2 \ (\mathrm{mod}\, p)$.

平方剩余-性质

【定理4.1.3】 设p为奇素数,

（1）若a_1,a_2均为模p的平方剩余, 则a_1a_2仍为模p的平方剩余.

（2）若a_1为模p的平方剩余, a_2为模p的平方非剩余, 则a_1a_2为模p的平方非剩余.

（3）若a_1,a_2均为模p的平方非剩余, 则a_1a_2为模p的平方剩余.

证明:（1）因a_1, a_2均为模p的平方剩余，故

$$a_1^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p), a_2^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p).$$

于是有

$$a_1^{\frac{p-1}{2}} \times a_2^{\frac{p-1}{2}} \equiv (a_1 a_2)^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p).$$

说明$a_1 a_2$是模p的平方剩余, 故得证.

第（2）（3）条结论类似可证.

4.2 Legendre（勒让得）符号

【定义4.2.1】 设p为奇素数, $a \in Z, (a,p)=1$,
定义**勒让得符号**如下:

$$\left(\frac{a}{p}\right)=\begin{cases} 1, & 若a是模p的平方剩余 \\ -1, & 若a是模p的平方非剩余 \end{cases}$$

勒让得符号$\left(\frac{a}{p}\right)$读作a对p的勒让得符号.

欧拉判别法

【定理4.2.1】（欧拉判别法）设p是奇素数, 则对任意整数a, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\bmod\, p)$.

由勒让得符号和二次剩余的定义可知, p是奇素数, $a \in Z, (a, p) = 1$, 下面三个描述是等价的:

（1）同余方程$x^2 \equiv a(\bmod p)$有解;

（2）a是模p的平方剩余;

（3）$\left(\frac{a}{p}\right) = 1$.

勒让得符号-性质

由定理4.2.1可以直接得到下面的推论.

【推论1】 设p是奇素数, 则

（1） $\left(\frac{1}{p}\right)=1.$

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

推论的证明由定理4.2.1即得. 其中（1）式表示方程$x^2\equiv 1(\bmod p)$有解, 结论是显然的.

勒让得符号-性质

由推论1的第(2)个性质易得:

【推论2】 设p是奇素数, 那么

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

勒让得符号-性质

【定理4.2.2】 设p是奇素数, 则

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

（2） $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

（3）设$(a,p)=1$, 则$\left(\frac{a^2}{p}\right)=1$.

证明: (1) 勒让得符号$\left(\frac{a+p}{p}\right)$的取值为判断同余方程$x^2 \equiv a+p \pmod p$解的情况, 勒让得符号$\left(\frac{a}{p}\right)$的取值为判断同余方程$x^2 \equiv a \pmod p$解的情况. 而同余方程$x^2 \equiv a+p \pmod p$与$x^2 \equiv a \pmod p$等价, 故得证.

(2) 由欧拉判别法, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\ p)$, $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} (\mathrm{mod}\ p)$, 以及$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} (\mathrm{mod}\ p) = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} (\mathrm{mod}\ p) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, 故得证.

(3) 因$(a, p) = 1$, 故判断$\left(\frac{a^2}{p}\right)$的值, 即是判断方程$x^2 \equiv a^2 (\mathrm{mod}\ p)$是否有解. 方程$x^2 \equiv a^2 (\mathrm{mod}\ p)$显然是有解的, 故$\left(\frac{a^2}{p}\right) = 1$.

勒让得符号-性质

【定理4.2.3】 设p是奇素数, 则

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

【推论】 设p是奇素数, 那么

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

勒让得符号-例题

【例4.2.1】 举几个p较小的例子验证【定理4.2.3】.

（1）$\left(\frac{2}{3}\right)$即是判断$x^2 \equiv 2 \pmod 3$是否有解. 通过穷举的方式易得,

$$1^2 \equiv 2^2 \equiv 1 \pmod 3.$$

故方程无解. 即$\left(\frac{2}{3}\right) = -1.$

由【定理4.2.3】,

$$\left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1.$$

结论相符.

勒让得符号-例题

（2）$\left(\frac{2}{7}\right)$即是判断$x^2 \equiv 2 \pmod 7$是否有解. 通过穷举的方式易得,

$1^2 \equiv 6^2 \equiv 1 \pmod 7$, $2^2 \equiv 5^2 \equiv 4 \pmod 7$, $3^2 \equiv 4^2 \equiv 2 \pmod 7$.

故方程有解. 即$\left(\frac{2}{7}\right) = 1$.

由【定理4.2.3】,

$$\left(\frac{2}{7}\right) = (-1)^{\frac{7^2-1}{8}} = 1.$$

结论相符.

二次互反律-性质

【定理4.2.4】 (二次互反律) 若p与q是互素的奇素数, 则

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

二次互反律的发现和证明是一段有趣的掌故. 欧拉和勒让得发现了二次互反律, 高斯花费了许多精力来寻求证明. 自从1796年得到第一个证明后, 高斯继续寻求证明此定理的不同方法, 至少给出了六种证明方法. 他寻求更多证明的目的是找到一种可以推广到更高次幂的方法, 特别地, 他对素数的三次或四次剩余很感兴趣. 他的第六个证明可以推广到高次幂的情形.

不止高斯寻求二次互反律的新的证明方法, 另外如柯西、狄利克雷、埃森斯坦等著名数学家都给出了二次互反律的原创性证明. 据统计, 在1921年有56个不同的证明, 1963年有152个证明, 2004年已有207个证明.

二次互反律-例题

【例4.2.2】 举几个p和q都较小的例子验证【定理4.2.4】.

（1）设二次同余方程为$x^2 \equiv 3(\bmod 7)$, 3和7是互素的奇素数. 通过穷举的方式可以得到下面的计算结果:

$1^2 \equiv 6^2 \equiv 1(\bmod 7)$，$2^2 \equiv 5^2 \equiv 4(\bmod 7)$，$3^2 \equiv 4^2 \equiv 2(\bmod 7)$.

故可知同余方程无解.

由二次互反律,

$$\left(\frac{3}{7}\right) = (-1)^{\frac{3-1}{2}\times\frac{7-1}{2}}\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

结论相符.

二次互反律-例题

（2）设二次同余方程为$x^2 \equiv 3(\mathrm{mod}\ 13)$, 3和13是互素的奇素数. 通过穷举的方式可以得到下面的计算结果:

$1^2 \equiv 12^2 \equiv 1(\mathrm{mod}\ 13)$, $2^2 \equiv 11^2 \equiv 4(\mathrm{mod}\ 13)$, $3^2 \equiv 10^2 \equiv 9(\mathrm{mod}\ 13)$. $4^2 \equiv 9^2 \equiv 3(\mathrm{mod}\ 13)$, $5^2 \equiv 8^2 \equiv 12(\mathrm{mod}\ 13)$, $6^2 \equiv 7^2 \equiv 10(\mathrm{mod}\ 13)$.

故可知同余方程有解.

由二次互反律,

$$\left(\frac{3}{13}\right) = (-1)^{\frac{3-1}{2} \times \frac{13-1}{2}} \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

结论相符.

勒让得符号-例题

【例题4.2.3】 已知107是素数，判断二次同余方程$x^2 \equiv 56 (\mathrm{mod}\ 107)$是否有解.

解: $\left(\frac{56}{107}\right)=\left(\frac{4}{107}\right)\left(\frac{2}{107}\right)\left(\frac{7}{107}\right)$

$=(-1)^{\frac{107^2-1}{8}} \times (-1)^{\frac{7-1}{2}\times\frac{107-1}{2}} \times \left(\frac{107}{7}\right)$

$=(-1)\times(-1)\times\left(\frac{107}{7}\right)=\left(\frac{2}{7}\right)=1.$

原同余方程有解.

勒让得符号-例题

【例4.2.4】 判断二次同余方程$x^2 \equiv 41 \pmod{1357}$ 是否有解.

解: 同余方程$x^2 \equiv 41 \pmod{1357}$等价于

$$\begin{cases} x^2 \equiv 41 \pmod{23} \\ x^2 \equiv 41 \pmod{59} \end{cases}.$$

也即是说, 方程$x^2 \equiv 41 \pmod{23}$有解, 并且方程$x^2 \equiv 41 \pmod{59}$也有解, 原同余方程$x^2 \equiv 41 \pmod{1357}$才有解.

因为$\left(\frac{41}{23}\right) = \left(\frac{23+18}{23}\right) = \left(\frac{18}{23}\right) = \left(\frac{2\times 3^2}{23}\right) = \left(\frac{2}{23}\right) = \left(\frac{2+23}{23}\right) = \left(\frac{25}{23}\right) = 1$,

$\left(\frac{41}{59}\right) = \left(\frac{41+59}{59}\right) = \left(\frac{100}{59}\right) = 1$.

故同余方程$x^2 \equiv 41 \pmod{1357}$有解.

勒让得符号-例题

【例4.2.4】 判断二次同余方程 $x^2 \equiv 41 (\mathrm{mod}\ 161)$ 是否有解.

解: 同余方程$x^2 \equiv 41 (\mathrm{mod}\ 161)$等价于

$$\begin{cases} x^2 \equiv 41 (\mathrm{mod} 23) \\ x^2 \equiv 41 (\mathrm{mod} 7) \end{cases}.$$

由【例4.2.3】知$\left(\frac{41}{23}\right) = 1$, 而$\left(\frac{41}{7}\right) = \left(\frac{6}{7}\right)$, 用穷举的方法易得, $\left(\frac{6}{7}\right) = -1$, 故同余方程 $x^2 \equiv 41 (\mathrm{mod}\ 161)$无解.

勒让得符号-例题

【例4.2.5】 判断二次同余方程$5x^2 \equiv 41 (\mathrm{mod}\,161)$ 是否有解.

解: 同余方程$5x^2 \equiv 41(\mathrm{mod}\,161)$等价于

$$\begin{cases} 5x^2 \equiv 41 \equiv -5(\mathrm{mod}23) \\ 5x^2 \equiv 41 \equiv 6(\mathrm{mod}7) \end{cases}.$$

因为(5, 23)=1, 故由$5x^2 \equiv -5(\mathrm{mod}23)$得$x^2 \equiv -1(\mathrm{mod}23)$.

又$5^{-1}(\mathrm{mod}\,7) = 3$, 故由$5x^2 \equiv 6(\mathrm{mod}7)$得$x^2 \equiv 5^{-1} \times 6 \equiv 3 \times 6 \equiv 4(\mathrm{mod}7)$.

即整理该同余方程组得

$$\begin{cases} x^2 \equiv -1(\mathrm{mod}23) \\ x^2 \equiv 4(\mathrm{mod}7) \end{cases}.$$

容易计算$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{-1}{23}\right) = (-1)^{\frac{23-1}{2}} = -1$.

4.3 扩展阅读

在这一节介绍两个扩展的知识点.

（1）二次同余方程的一般形式: $ax^2+bx+c\equiv 0(\mathrm{mod}\, m),(a,m)=1$, 为什么只介绍了$x^2\equiv a(\mathrm{mod}\, p)$的情形?

（2）在计算勒让得符号时, 如果把奇合数的模数当成了奇素数会出现什么问题?

下面介绍第（1）个问题涉及的相关知识.

首先, 二次同余方程的一般形式为

$$ax^2+bx+c\equiv 0 \pmod{m}, (a,m)=1 \quad （4.3.1）$$

用$4a$乘（4.3.1）式再加上b^2得:

$$4a^2x^2+4abx+b^2\equiv b^2-4ac \pmod{m}.$$

即$(2ax+b)^2\equiv b^2-4ac \pmod{m}$.

若令$y=2ax+b, d=b^2-4ac$则上式变为

$$b^2\equiv d \pmod{m}. \quad （4.3.2）$$

若m为奇素数, 设$p = m$. 若$x \equiv x_0 \pmod p$是方程（4.3.1）的一个解, 则$y \equiv 2ax_0 + b \pmod p$为方程（4.3.2）的解；反之, 若$y \equiv y_0 \pmod p$为（4.3.2）的解, 由$y \equiv 2ax + b \pmod p$知, $x \equiv (2a)^{-1}(y_0 - b) \pmod p$. 因$(a, p) = 1$, 故$(2a)^{-1} \pmod p$存在.

若m为奇合数, 由算术基本定理和中国剩余定理, $m = {p_1}^{s_1}{p_2}^{s_2}\ldots{p_k}^{s_k}$, 因$(a, m) = 1$, 故$(a, {p_i}^{s_i}) = 1$, 只需要考虑下面同余方程:

$$x^2 \equiv a(mod\ p^s), (a, p) = 1, s > 0.$$

由现有研究结果, 有下面结论.

【定理4.3.1】 设p是奇素数, 则同余方程有解的充分必要条件是a是模p的平方剩余, 且有解时的解数为2.

也就是说, 同余方程$x^2 \equiv a(mod\ p^s)$, $(a, p) = 1$, $s > 0$有解条件与$x^2 \equiv a(mod\ p)$, $(a, p) = 1$是等同的.

所以, 对于二次同余方程, 仅需要研究$x^2 \equiv a(mod\ p)$, $(a, p) = 1$的情形.

下面介绍第(2)个问题涉及的相关知识.

在4.2节中, 如果把合数当成了奇素数会出现什么样的情况呢？实际上, 在数论中, 这是在计算雅可比符号.

雅可比符号有很多与勒让得符号相似的性质, 可以去参考其他关于初等数论的书籍.

关于雅可比符号的一个结论是: 当雅可比符号为-1时, 原方程无解；当雅可比符号为1时, 原方程不一定有解. 下面举例说明.

【例4.3.1】 判断同余方程$x^2 \equiv 88 \pmod{105}$是否有解.

解: 105=3×5×7为合数, 直接计算雅可比符号

$$\left(\frac{88}{105}\right)=\left(\frac{4}{105}\right)\left(\frac{2}{105}\right)\left(\frac{11}{105}\right)$$

$$=(-1)^{\frac{105^2-1}{8}}\times(-1)^{\frac{105-1}{2}\times\frac{11-1}{2}}\left(\frac{105}{11}\right)=\left(\frac{6}{11}\right)=-1.$$

所以, 原方程无解.

实际上, 原方程等价于方程组

$$\begin{cases} x^2 \equiv 88 \pmod 3 \\ x^2 \equiv 88 \pmod 5. \\ x^2 \equiv 88 \pmod 7 \end{cases}$$

而方程组有解的充分必要条件是每个方程都有解, 但现在$\left(\frac{88}{3}\right)\left(\frac{88}{5}\right)\left(\frac{88}{7}\right) = \left(\frac{88}{105}\right)$=-1, 说明$\left(\frac{88}{3}\right), \left(\frac{88}{5}\right), \left(\frac{88}{7}\right)$三者中至少有一个为-1, 即方程组中至少有一个方程无解, 从而原方程无解.

【例4.3.2】 判断同余方程$x^2 \equiv 38(\mathrm{mod}\,385)$是否有解.

解: 易知385=7×5×11为合数, 直接计算雅可比符号

$$\left(\frac{38}{385}\right)=\left(\frac{2}{385}\right)\left(\frac{19}{385}\right)=(-1)^{\frac{385^2-1}{8}}\times(-1)^{\frac{385-1}{2}\times\frac{19-1}{2}}\left(\frac{385}{19}\right)=\left(\frac{5}{19}\right)=(-1)^{\frac{5-1}{2}\times\frac{19-1}{2}}\left(\frac{19}{5}\right)$$

$$=\left(\frac{4}{5}\right)=1.$$

$\left(\frac{38}{315}\right)$=1并不能肯定原方程是否有解, 还须判断方程组

$$\begin{cases} x^2 \equiv 38 (\bmod 5) \\ x^2 \equiv 38 (\bmod 7) \\ x^2 \equiv 38 (\bmod 11) \end{cases}$$

中的每个方程是否有解. 通过计算可知, 勒让得符号$\left(\frac{38}{5}\right)$=$\left(\frac{3}{5}\right)$=-1, 因此方程$x^2 \equiv 38 (\bmod 5)$无解, 说明原方程无解.

由上面的例题可知，当雅可比符号为-1时，意味着二次同余方程

$$x^2 \equiv a(\operatorname{mod} m), (a,m) = 1,$$

$$m = {p_1}^{s_1}{p_2}^{s_2} \dots {p_k}^{s_k}$$

所对应的等价方程组

$$x^2 \equiv a(mod\ p^s), (a,p) = 1, s > 0$$

中，至少有一个二次同余方程无解. 因而原方程无解；当雅可比符号为1时，原方程对应的等价方程组中可能存在偶数个二次同余方程无解，即勒让得符号为-1，因而原方程不一定有解.

作业

判断二次同余方程$x^2 \equiv 41(\bmod 23 \times 67)$ 是否有解