Open Access Library Journal
2025, Volume 12, e13656
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Research on Rational Quadratic Residues

Zhongqi Zhou

Hubei Coal Geology Bureau, Wuhan, China
Email: zhouzongqi1058@163.com

How to cite this paper: Zhou, Z.Q. (2025) Research on Rational Quadratic Residues. *Open Access Library Journal*, **12**: e13656.
https://doi.org/10.4236/oalib.1113565

Received: May 6, 2025
Accepted: June 15, 2025
Published: June 16, 2025

Abstract

This paper introduces the concept of rational quadratic residues, namely fractional quadratic residues. It also presents a method for determining quadratic residues with fractions as moduli, as well as computational symbols for rational quadratic residues and formulas for converting rational Legendre symbols to general Legendre symbols. Formulas for calculating the number of rational quadratic residues and rational quadratic non-residues are derived. Additionally, several practical application examples of rational quadratic residues are highlighted. The paper further examines the discrimination and applications of rational quadratic residues. Finally, several conjectures related to rational quadratic residues are proposed.

Subject Areas

Integral Equation, Number Theory

Keywords

Rational k-th Residues, Determination Method for Rational Quadratic Residues, Rational Quadratic Non-Residues, Binary Quadratic Indeterminate Equations, Necessary and Sufficient Conditions for Solutions to Indeterminate Equations, Conjectures

1. 引言

整数 a 何时为模数 p 的平方数呢？伟大的数论学家欧拉、勒让德和高斯对于这一问题及相关的许多问题的研究，导致了现代数论很多方面的发展[1]，现在的“二次剩余”在所有的数论教科书中是不可缺少的内容，它是求解二次同余方程的有力工具，在不定方程的判定有无整数解方面也很有作用。但一般来说，以往的模数 p 的二次剩余，指的都是整数。在此文中作者提出了有理 k 次剩余的概念(包括有理二次剩余)，即分数 k 次剩余。

文中给出了分数为模数 p 的二次剩余的判定方法和有理二次剩余的计算

符号以及从有理勒让德符号转换为一般勒让德符号的计算公式。推导了有理二次剩余和有理二次非剩余个数的计算公式。还重点给出了有理二次剩余的多个实际应用的范例。

文章后半部分对有理 k 次剩余 $(k\geq 3)$ 的判别和应用作了一些研究。最后提出了几个与有理二次剩余有关的猜想。

2. 引理

引理 1. [2]设 p 为奇素数，m 为整数，$(m,p)=1$，则必存在 x,y $(x,y)=1$，使

$$mx\equiv y(\mathrm{mod}\, p)$$

式中：$1\leq x<\sqrt{p}$，$1\leq |y|<\sqrt{p}$。

引理 2. [3]

1) 设 a,b,m 为给定的正整数，$(a,b)=1,n\geq 2$，如果 $az^n\equiv -b(\mathrm{mod}\, m)$ 无整数解，则

$$m=ax^n+by^n$$

无正整数解。其中 $(x,y)=1$。

2) 设 a,b,m 为给定的正整数，$(a,b)=1,n\geq 2$，如果 $az^n\equiv (b \bmod m)(\mathrm{mod}\, m)$ 无整数解，则

$$m=ax^n-by^n$$

无正整数解。其中 $(x,y)=1$。

3. 定理及定义

有理二次剩余的定义：

设 $m,a,b\in N^+$，若 $(ab,m)=(a,b)=1$，且同余方程 $ax^2\equiv b(\mathrm{mod}\, m)$ 有解，则称 $\frac{b}{a}$ 是 m 的有理二次剩余。

若同余方程 $ax^2\equiv b(\mathrm{mod}\, m)$ 无解，则称 $\frac{b}{a}$ 是 m 的有理二次非剩余。

定理 1. 设 p 是奇素数，$a,b\in N^+$，且 $(ab,p)=(a,b)=1$，则 $\frac{b}{a}$ 是模 p 的有理二次剩余的充分必要条件是

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

证：设 $\frac{b}{a}$ 是模 p 的有理二次剩余，根据定义，则 $ax^2\equiv b(\mathrm{mod}\, p)$ 有一个整数解，设为 x_1，即有 $ax_1^2\equiv b(\mathrm{mod}\, m)$，$x_1^2\equiv \frac{b}{a}(\mathrm{mod}\, p)$，由费尔马小定理可得 $\left(\frac{b}{a}\right)^{\frac{p-1}{2}}\equiv \left(x_1^2\right)^{\frac{p-1}{2}}=x_1^{p-1}\equiv 1(\mathrm{mod}\, p)$，因此，若 $\frac{b}{a}$ 是 p 的有理二次剩余，则

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

反之，设$\left(\frac{b}{a}\right)^{\frac{p-1}{2}} \equiv 1\left(\mathrm{mod}\, p\right)$，$g$是$p$的一个原根，则有$\frac{p-1}{2} ind_g\left(\frac{b}{a}\right) \equiv \frac{p-1}{2}\left(ind_g(b) - ind_g(a)\right) \equiv 0\left(\mathrm{mod}\, p-1\right)$，即$ind_g(b) - ind_g(a) \equiv 0\left(\mathrm{mod}\, 2\right)$，因此，$2 \left| ind_g(b) - ind_g(a) = ind_g\left(\frac{b}{a}\right)\right.$。

即$\frac{b}{a}$是模数p的一个有理2次剩余。

定理 2. 设p是奇素数，$a,b \in N^+$，且$(ab,p)=(a,b)=1$，如果$\frac{b}{a}$是模p的有理二次非剩余，则

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

证：如果$\frac{b}{a}$为p的有理二次非剩余，此时同余式$ax^2 \equiv b\left(\mathrm{mod}\, p\right)$无解，由费尔马小定理知：$b^{p-1} \equiv 1\left(\mathrm{mod}\, p\right)$，$a^{p-1} \equiv 1\left(\mathrm{mod}\, p\right)$，所以$\left(\frac{b}{a}\right)^{p-1} \equiv 1\left(\mathrm{mod}\, p\right)$。由此可得：

$$\left(\left(\frac{b}{a}\right)^{\frac{p-1}{2}} + 1\right)\left(\left(\frac{b}{a}\right)^{\frac{p-1}{2}} - 1\right) = \left(\left(\frac{b}{a}\right)^{p-1} - 1\right) \equiv 0\left(\mathrm{mod}\, p\right).$$

因此$\left(\frac{b}{a}\right)^{\frac{p-1}{2}} \equiv 1$或$\left(\frac{b}{a}\right)^{\frac{p-1}{2}} \equiv -1\left(\mathrm{mod}\, p\right)$成立。假如他们同时成立，则得$1 \equiv -1\left(\mathrm{mod}\, p\right)$，此不可。因模$p$的有理二次非剩余不满足$\left(\frac{b}{a}\right)^{\frac{p-1}{2}} \equiv 1\left(\mathrm{mod}\, p\right)$，那么必满足

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

定理 3. 设p为奇素数，$p_i(+1)$为p的所有整数二次剩余集合中的第i个数(从小到大排序)，$p_j(+1)$为p的所有整数二次剩余集合中的第j个数(从小到大排序)，$i \neq j$，$\left(p_i(+1), p_j(+1)\right) = 1$，则$\frac{p_i(+1)}{p_j(+1)}$为$p$的有理二次剩余。

证：因为$\left(p_i(+1)\right)^{\frac{p-1}{2}} \equiv 1\left(\mathrm{mod}\, p\right)$，$\left(p_j(+1)\right)^{\frac{p-1}{2}} \equiv 1\left(\mathrm{mod}\, p\right)$，所以

$$\left(\frac{p_i(+1)}{p_j(+1)}\right)^{\frac{p-1}{2}} \equiv 1\left(\mathrm{mod}\, p\right),$$

根据定理 1 知$\frac{p_i(+1)}{p_j(+1)}$是p的有理二次剩余。

定理 4. 设 p 为奇素数，$p_i(-1)$ 为 p 的所有整数二次非剩余集合中的第 i 个数(从小到大排序)，$p_j(-1)$ 为 p 的所有整数二次非剩余集合中的第 j 个数(从小到大排序)，$i \neq j$，$\left(p_i(-1), p_j(-1)\right)=1$，则 $\dfrac{p_i(-1)}{p_j(-1)}$ 为 p 的有理二次剩余。

证：因为 $\left(p_i(-1)\right)^{\frac{p-1}{2}} \equiv -1 \pmod p$，$\left(p_j(-1)\right)^{\frac{p-1}{2}} \equiv -1 \pmod p$，所以

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

根据定理 1 知 $\dfrac{p_i(-1)}{p_j(-1)}$ 是 p 的有理二次剩余。

定理 5. 设 p 为奇素数，$p_i(+1)$ 为 p 的所有整数二次剩余集合中的第 i 个数(从小到大排序)，$p_j(-1)$ 为 p 的所有整数二次非剩余集合中的第 j 个数(从小到大排序)，$\left(p_i(+1), p_j(-1)\right)=1$，则 $\dfrac{p_i(+1)}{p_j(-1)}$ 为 p 的有理二次非剩余。

证：因为 $\left(p_i(+1)\right)^{\frac{p-1}{2}} \equiv 1 \pmod p$，$\left(p_j(-1)\right)^{\frac{p-1}{2}} \equiv -1 \pmod p$，所以

$$\left(\frac{p_i(+1)}{p_j(-1)}\right)^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

根据定理 2 知 $\dfrac{p_i(+1)}{p_j(-1)}$ 是 p 的有理二次非剩余。

定义：用 $\varphi_k\{\text{正整数的集合}\}$ 表示集合中第 k 个数与这个集合中的数互素的个数。集合中的数按从小到大顺序排列。

例：$\varphi_3\{1,2,3,8,9\}=3$；$\varphi_1\{1,5,6,7,11,13\}=6$，
$\varphi_5\{11\text{的全体整数二次剩余}\}=3$。

定理 6. 设 p 为奇素数，

1) p 的全部有理二次剩余和有理二次非剩余个数(包括整数二次剩余和非剩余)共有：

$$\sum_{k=1}^{p-1}\varphi_k\{p\text{的完全剩余系}\}$$

2) p 的全部有理二次剩余个数(包括整数二次剩余)共有：

$$\sum_{i=1}^{\frac{p-1}{2}}\varphi_i\{p\text{的全体整数二次剩余}\}+\sum_{j=1}^{\frac{p-1}{2}}\varphi_j\{p\text{的全体整数二次非剩余}\}.$$

3) p 的全部有理二次非剩余个数(包括整数二次非剩余)共有：

$$\sum_{k=1}^{p-1}\varphi_k\{p\text{的完全剩余系}\}-\sum_{i=1}^{\frac{p-1}{2}}\varphi_i\{p\text{的全体整数二次剩余}\}-\sum_{j=1}^{\frac{p-1}{2}}\varphi_j\{p\text{的全体整数二次非剩余}\}$$

证：根据定理 3，定理 4，定理 5 和定义即可证明。

例：求 11 的全部有理二次剩余及其剩余和非剩余个数。

11 的有理二次剩余有：

$$1^2\equiv 1,2^2\equiv 4,3^2\equiv 9,4^2\equiv 5,5^2\equiv 3,3^2\equiv\frac{7}{2},2^2\equiv\frac{1}{3},3^2\equiv\frac{5}{3},4^2\equiv\frac{4}{3},2^2\equiv\frac{5}{4}\left(\mathrm{mod}11\right)$$

$$3^2\equiv\frac{3}{4},4^2\equiv\frac{9}{4},5^2\equiv\frac{1}{4},2^2\equiv\frac{9}{5},3^2\equiv\frac{1}{5},4^2\equiv\frac{3}{5},5^2\equiv\frac{4}{5},5^2\equiv\frac{7}{6},2^2\equiv\frac{6}{7}\left(\mathrm{mod}11\right)$$

$$3^2\equiv\frac{8}{7},4^2\equiv\frac{2}{7},5^2\equiv\frac{10}{7},4^2\equiv\frac{7}{8},3^2\equiv\frac{4}{9},4^2\equiv\frac{1}{9},5^2\equiv\frac{5}{9},2^2\equiv\frac{7}{10}\left(\mathrm{mod}11\right)$$

共有 27 个。

11 的整数二次剩余有：1，3，4，5，9。

11 的整数二次非剩余有：2，6，7，8，10。

根据定理 6 可得：

11 的有理二次剩余个数

$$\sum_{i=1}^{5}\varphi_i\left\{1,3,4,5,9\right\}+\sum_{j=1}^{5}\varphi_j\left\{2,6,7,8,10\right\}=\left(5+3+4+4+3\right)+\left(1+1+4+1+1\right)=27.$$

11 的有理二次非剩余个数：

$$\sum_{k=1}^{10}\varphi_k\left\{1,2,\cdots,10\right\}-\left(\sum_{i=1}^{5}\varphi_i\left\{1,3,4,5,9\right\}+\sum_{j=1}^{5}\varphi_j\left\{2,6,7,8,10\right\}\right)$$
$$=\left(10+5+7+5+8+3+9+5+7+4\right)-27=36.$$

定义：设 p 为奇素数，$a,b\in N^+$，$\left(p,ab\right)=1$，令

$$\left(\frac{\frac{b}{a}}{p}\right)=\begin{cases}1 & \text{若}\frac{b}{a}\text{是模数 }p\text{ 的有理二次剩余}\\ -1 & \text{若}\frac{b}{a}\text{是模数 }p\text{ 的有理二次非剩余}\\ 0 & \text{若}\frac{b}{a}\equiv 0\left(\mathrm{mod}\,p\right)\end{cases}$$

函数 $\left(\frac{\frac{b}{a}}{p}\right)$ 叫做 $\frac{b}{a}$ 对 p 的有理勒让德符号。

由有理勒让德符号的定义，上面的定理 1 可改写为：设 p 是一个奇素数，$\left(p,ab\right)=1$，则

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

由于 $\frac{b}{a}\equiv\frac{d}{c}\left(\mathrm{mod}\,p\right)$ 时，$\frac{b}{a}$ 和 $\frac{d}{c}$ 同为模数 p 的有理二次剩余或同为模数 p 的有理二次非剩余，故有 $\left(\frac{\frac{b}{a}}{p}\right)=\left(\frac{\frac{d}{c}}{p}\right)$。

当$\frac{b}{a}\equiv 0\left(\mathrm{mod}\, p\right)$，如果我们定义$\left(\frac{\frac{b}{a}}{p}\right)=0$，则有下面的定理：

定理 7：对于给定的奇素数p，有理勒让德符号$\left(\frac{\frac{b}{a}}{p}\right)$是一个完全积性函数。

证：如果$\frac{b}{a}\times\frac{d}{c}\equiv 0\left(\mathrm{mod}\, p\right)$，则必有$p\left|b\right.$或$p\left|d\right.$，故$\left(\frac{\frac{b}{a}\times\frac{d}{c}}{p}\right)=\left(\frac{\frac{b}{a}}{p}\right)\left(\frac{\frac{d}{c}}{p}\right)=0$。

如果$\left(p,bd\right)=1$，$\left(p,ac\right)=1$，则

$$\left(\frac{\frac{b}{a}\times\frac{d}{c}}{p}\right)=\left(\frac{b}{a}\times\frac{d}{c}\right)^{\frac{p-1}{2}}=\left(\frac{b}{a}\right)^{\frac{p-1}{2}}\times\left(\frac{d}{c}\right)^{\frac{p-1}{2}}\equiv\left(\frac{\frac{b}{a}}{p}\right)\times\left(\frac{\frac{d}{c}}{p}\right)\left(\mathrm{mod}\, p\right)\tag{1}$$

因为$\left(\frac{\frac{b}{a}\times\frac{d}{c}}{p}\right)-\left(\frac{\frac{b}{a}}{p}\right)\times\left(\frac{\frac{d}{c}}{p}\right)=\pm 2,0$，故(1)给出$\left(\frac{\frac{b}{a}\times\frac{d}{c}}{p}\right)=\left(\frac{\frac{b}{a}}{p}\right)\times\left(\frac{\frac{d}{c}}{p}\right)$。

定理 8：设p为给定的奇素数，$\left(p,ab\right)=\left(a,b\right)=1$，则$\left(\frac{\frac{a}{b}}{p}\right)=\left(\frac{\frac{b}{a}}{p}\right)$。

证：因$\left(\frac{1}{p}\right)=\left(\frac{\frac{a}{b}\times\frac{b}{a}}{p}\right)=\left(\frac{\frac{a}{b}}{p}\right)\times\left(\frac{\frac{b}{a}}{p}\right)=1$，又因$\left(\frac{\frac{a}{b}}{p}\right)=\pm 1$，$\left(\frac{\frac{b}{a}}{p}\right)=\pm 1$，所以$\left(\frac{\frac{a}{b}}{p}\right)=\left(\frac{\frac{b}{a}}{p}\right)$。

定理 9：设p为给定的奇素数，$\left(p,ab\right)=\left(a,b\right)=1$，则$\left(\frac{\frac{a}{b}}{p}\right)=\left(\frac{a}{p}\right)\times\left(\frac{b}{p}\right)$。

证：根据以上两定理可得：

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

这是一个很重要的转换公式，可以把有理勒让德符号转换为一般勒让德符号来计算。

有理二次剩余的应用：

定理 10. 设 p 为奇素数，$a,b\in N^+$，$(ab,p)=(a,b)=(x,y)=1$，则 $p=ax^2+by^2$ 有正整数解的必要条件是：$\frac{-a}{b}$ 是 p 的有理二次剩余。

证：若 $p=ax^2+by^2$ 有正整数解，必有 $(p,x)=(p,y)=1$，因若不然，比如 $p\mid x$ 就推出 $p\mid y$，于是 $p=a(px_1)^2+b(py_1)^2$，这是不可能的，于是必有 x_1 使 $(p,x_1)=1$，$xx_1\equiv 1(\mathrm{mod}\,p)$，从而 $a(xx_1)^2+b(yx_1)^2=px_1^2\equiv 0(\mathrm{mod}\,p)$

即 $b(yx_1)^2+a\equiv 0(\mathrm{mod}\,p)$

或 $(yx_1)^2\equiv\frac{-a}{b}(\mathrm{mod}\,p).$

这表明 $\frac{-a}{b}$ 为 p 之有理二次剩余。

定理 11. 设 p 为奇素数，$p=2x^2+3y^2$ 有正整数解的充分条件是：$\left(\frac{\frac{-2}{3}}{p}\right)=1$ 和 $\left(\frac{p}{3}\right)=-1$。

证：当 $\left(\frac{\frac{-2}{3}}{p}\right)=1$ 且 $\left(\frac{p}{3}\right)=-1$，$\frac{-2}{3}$ 为 p 的有理二次剩余，即存在 $a<p$ 使 $a^2\equiv-\frac{2}{3}(\mathrm{mod}\,p)$，或有 $3a^2\equiv -2(\mathrm{mod}\,p)$。根据引理 1 有

$$ax\equiv y(\mathrm{mod}\,p),(x,y)=1.$$

$p\mid ax-y, p\mid(ax-y)(mx-3y)=amx^2+3y^2-(m+3a)xy$，令 $m=p-3a$，则 $p\mid amx^2+3y^2=a(p-3a)x^2+3y^2=apx^2-3a^2x^2+3y^2, p\mid -3a^2x^2+3y^2$。

由于 $3a^2\equiv -2(\mathrm{mod}\,p)$，则 $p\mid 2x^2+3y^2$ 或 $2x^2+3y^2=kp$，$k\geq 1$ 为整数。

由引理 1 知：$1\leq x<\sqrt{p}$，$1\leq|y|<\sqrt{p}$，所以

$$2x^2+3y^2<5p.$$

因 $2x^2+3y^2\equiv 1,2,3(\mathrm{mod}\,4)$，$2x^2+3y^2\equiv 2(\mathrm{mod}\,3)$，所以 $2x^2+3y^2\neq 3p,4p$。

如果 $2x^2+3y^2=2p$，则必有：$y=2y_1$，$2x^2+3(2y_1)^2=2p$ 或 $x^2+6y_1^2=p$，因 p 是奇素数，所以 x 为奇数，且 $(x,3)=1$，必有 $x^2+6y_1^2\equiv 1(\mathrm{mod}\,6)$，所以 $p\equiv 1(\mathrm{mod}\,6)$，但根据条件：$\left(\frac{p}{3}\right)=-1$，所以 $p\equiv 2(\mathrm{mod}\,3)$，矛盾，即 $2x^2+3y^2\neq 2p$，综上所述，只有

$$2x^2+3y^2=p.$$

定理 12. 设 p 为奇素数，则 $p=2x^2+5y^2$ 有正整数解的充分条件是 $\left(\frac{\frac{-2}{5}}{p}\right)=1$，$\left(\frac{p}{5}\right)=-1$。

证：当$\left(\frac{\frac{-2}{5}}{p}\right)=1$且$\left(\frac{p}{5}\right)=-1$，$\frac{-2}{5}$为$p$的有理二次剩余，即存在$a<p$使$a^2\equiv-\frac{2}{5}\left(\mathrm{mod}\,p\right)$，或有$5a^2\equiv-2\left(\mathrm{mod}\,p\right)$。根据引理1有

$$ax\equiv y\left(\mathrm{mod}\,p\right),\left(x,y\right)=1.$$

$p\left|ax-y,p\right|\left(ax-y\right)\left(mx-5y\right)=amx^2+5y^2-\left(m+5a\right)xy$，令$m=p-5a$，则$p\left|amx^2+5y^2=a\left(p-5a\right)x^2+5y^2=apx^2-5a^2x^2+5y^2,p\right|-5a^2x^2+5y^2$。

由于$5a^2\equiv-2\left(\mathrm{mod}\,p\right)$，则$p\left|2x^2+5y^2\right.$或$2x^2+5y^2=kp$，$k\geq1$为整数。

由引理1知：$1\leq x<\sqrt{p}$，$1\leq\left|y\right|<\sqrt{p}$，所以

$$2x^2+5y^2<7p.$$

因$2x^2+5y^2\equiv1,2,3\left(\mathrm{mod}\,4\right)$，$2x^2+5y^2\equiv1,2\left(\mathrm{mod}\,3\right)$，所以$2x^2+5y^2\neq4np$，$2x^2+5y^2\neq3np$，所以$2x^2+5y^2\neq3p,4p,6p$。

如果$2x^2+5y^2=5p$，则必有：$x=5x_1$，$2\left(5x_1\right)^2+5y^2=5p$，或$10x_1^2+y^2=p$，因$p$是奇素数，所以$y$为奇数且$\left(y,5\right)=1$，必有$10x_1^2+y^2\equiv1,4\left(\mathrm{mod}\,5\right)$，所以$p\equiv1,4\left(\mathrm{mod}\,5\right)$，但由条件知$\left(\frac{p}{5}\right)=-1$，所以$p\equiv3,2\left(\mathrm{mod}\,5\right)$，矛盾，即$2x^2+5y^2\neq5p$，

如果$2x^2+5y^2=2p$，则必有：$y=2y_1$，$2x^2+5\left(2y_1\right)^2=2p$，或$x^2+10y_1^2=p$，因$p$是奇素数，所以$x$为奇数，且$\left(x,5\right)=1$，必有$x^2+10y_1^2\equiv1,4\left(\mathrm{mod}\,5\right)$，所以$p\equiv1,4\left(\mathrm{mod}\,5\right)$，但由条件知$\left(\frac{p}{5}\right)=-1$，所以$p\equiv3,2\left(\mathrm{mod}\,5\right)$，矛盾，即$2x^2+5y^2\neq2p$，综上所述，只有

$$2x^2+5y^2=p.$$

设p为奇素数，用以上相同的方法还可以证明以下不定方程有解存在充分条件：

$2x^2+11y^2=p$：有解的充分条件：$\left(\frac{\frac{-2}{11}}{p}\right)=1,\left(\frac{2}{p}\right)=-1,\left(\frac{p}{11}\right)=-1$。

$2x^2+15y^2=p$：有解的充分条件：$\left(\frac{\frac{-2}{15}}{p}\right)=1,\left(\frac{2}{p}\right)=1,\left(\frac{-3}{p}\right)=-1,\left(\frac{5}{p}\right)=-1$。

$2x^2+21y^2=p$：有解的充分条件：$\left(\frac{\frac{-2}{21}}{p}\right)=1,\left(\frac{-2}{p}\right)=-1,\left(\frac{-3}{p}\right)=-1,\left(\frac{-7}{p}\right)=1$。

$2x^2+29y^2=p$：有解的充分条件：$\left(\frac{\frac{-2}{29}}{p}\right)=1,\left(\frac{-2}{p}\right)=-1,\left(\frac{p}{29}\right)=-1$。

$2x^2+35y^2=p$：有解的充分条件：$\left(\frac{-2}{35}\right)=1,\left(\frac{2}{p}\right)=-1,\left(\frac{p}{5}\right)=-1,\left(\frac{p}{7}\right)=1$。

$2x^2+39y^2=p$：有解的充分条件：$\left(\frac{-2}{39}\right)=1,\left(\frac{2}{p}\right)=1,\left(\frac{-3}{p}\right)=-1,\left(\frac{13}{p}\right)=-1$。

$2x^2+51y^2=p$：有解的充分条件：$\left(\frac{-2}{51}\right)=1,\left(\frac{2}{p}\right)=-1,\left(\frac{-3}{p}\right)=-1,\left(\frac{17}{p}\right)=1$。

定理 13. 设 p 为奇素数，$p=3x^2+5y^2$ 有正整数解的充分条件是：$\frac{-3}{5}$ 是 p 的有理二次剩余和$\left(\frac{p}{3}\right)=-1$以及$\left(\frac{p}{5}\right)=-1$。

证：当$\left(\frac{-3}{5}\right)^{\frac{p-1}{2}}\equiv 1\left(\mathrm{mod}\,p\right)$且$3^{\frac{p-1}{2}}\equiv -1\left(\mathrm{mod}\,p\right)$，$5^{\frac{p-1}{2}}\equiv -1\left(\mathrm{mod}\,p\right)$，$\frac{-3}{5}$ 为 p 的有理二次剩余，即存在 $a<p$ 使 $a^2\equiv -\frac{3}{5}\left(\mathrm{mod}\,p\right)$，或有 $5a^2\equiv -3\left(\mathrm{mod}\,p\right)$。根据引理 1 有

$$ax\equiv y\left(\mathrm{mod}\,p\right),\left(x,y\right)=1.$$

$p\left|ax-y,p\right|\left(ax-y\right)\left(mx-5y\right)=amx^2+5y^2-\left(m+5a\right)xy$，令 $m=p-5a$，则 $p\left|amx^2+5y^2=a\left(p-5a\right)x^2+5y^2=apx^2-5a^2x^2+5y^2,p\right|-5a^2x^2+5y^2$。

由于 $5a^2\equiv -3\left(\mathrm{mod}\,p\right)$，则 $p\left|3x^2+5y^2\right.$ 或 $3x^2+5y^2=kp$，$k\geq 1$为整数。

由引理 1 知：$1\leq x<\sqrt{p}$，$1\leq\left|y\right|<\sqrt{p}$，所以

$$3x^2+5y^2<8p.$$

如果 $3x^2+5y^2=7p$，则$\left(\frac{x}{y}\right)^2\equiv\frac{-5}{3}\left(\mathrm{mod}\,7\right)$，说明$\frac{-5}{3}$是 7 的有理二次剩余，但$\left(\frac{-5}{3}\right)^{\frac{7-1}{2}}\equiv -1\left(\mathrm{mod}\,7\right)$，矛盾，所以 $3x^2+5y^2\neq 7p$。

如果 $3x^2+5y^2=6p$，则 $y=3y_1$，可得 $3x^2+5\left(3y_1\right)^2=6p$。或 $x^2+15y_1^2=2p$，此时 x,y_1 均为奇数，所以 $x^2+15y_1^2\equiv 0\left(\mathrm{mod}\,8\right)$，即 $x^2+15y_1^2\neq 2p$，因此 $3x^2+5y^2\neq 6p$。

如果 $3x^2+5y^2=5p$，则 $x=5x_1$，可得 $3\left(5x_1\right)^2+5y^2=5p$，或 $15x_1^2+y^2=p$，此时 $\left(y,5\right)=1$，$15x_1^2+y^2=p\equiv 1,4\left(\mathrm{mod}\,5\right)$，但根据条件：$\left(\frac{p}{5}\right)=-1$，矛盾，得 $3x^2+5y^2\neq 5p$。

如果 $3x^2+5y^2=4p$，因 $\left(x,y\right)=1$，所以 x,y 均为奇数，那么 $3x^2+5y^2\equiv 0\left(\mathrm{mod}\,8\right)$，因此 $3x^2+5y^2\neq 4p$。

如果 $3x^2+5y^2=3p$，则 $y=3y_1$，可得 $3x^2+5\left(3y_1\right)^2=3p$，或 $x^2+15y_1^2=p$，此时 $\left(x,15\right)=1$，$15y_1^2+x^2=p\equiv 1\left(\mathrm{mod}\,3\right)$，但根据条件：

$\left(\frac{p}{3}\right)=-1$，矛盾，得 $3x^2+5y^2\neq 3p$。

如果 $3x^2+5y^2=2p$，因 $(x,y)=1$，所以 x,y 均为奇数，那么 $3x^2+5y^2\equiv 0\pmod 8$，因此 $3x^2+5y^2\neq 2p$。

综上所述，只有

$$3x^2+5y^2=p.$$

定理 14. 设 p 为奇素数，$p=3x^2+7y^2$ 有正整数解的充分条件是：$\frac{-3}{7}$ 是 p 的有理二次剩余和 $\left(\frac{p}{3}\right)=1$ 以及 $\left(\frac{p}{7}\right)=-1$，$\left(\frac{-1}{p}\right)=-1$。

证：当 $\left(\frac{-3}{7}\right)^{\frac{p-1}{2}}\equiv 1\pmod p$ 且 $3^{\frac{p-1}{2}}\equiv 1\pmod p$，$7^{\frac{p-1}{2}}\equiv -1\pmod p$，$p\equiv -1\pmod 4$，$\frac{-3}{7}$ 为 p 的有理二次剩余，即存在 $a<p$ 使 $a^2\equiv -\frac{3}{7}\pmod p$，或有 $7a^2\equiv -3\pmod p$。根据引理 1 有

$$ax\equiv y\pmod p,(x,y)=1.$$

$p\mid ax-y, p\mid (ax-y)(mx-7y)=amx^2+7y^2-(m+7a)xy$，令 $m=p-7a$，则 $p\mid amx^2+7y^2=a(p-7a)x^2+7y^2=apx^2-7a^2x^2+7y^2, p\mid -7a^2x^2+7y^2$。

由于 $7a^2\equiv -3\pmod p$，则 $p\mid 3x^2+7y^2$ 或 $3x^2+7y^2=kp$，$k\geq 1$ 为整数。

由引理 1 知：$1\leq x<\sqrt{p}$，$1\leq |y|<\sqrt{p}$，所以

$$3x^2+7y^2<10p.$$

如果 $3x^2+7y^2=9p$，则 $y=3y_1$，$3x^2+7(3y_1)^2=9p$，$x^2+21y_1^2=3p$，又有 $x=3x_1$，$(3x_1)^2+21y_1^2=3p$，$3x_1^2+7y_1^2=p$。这说明 $3x^2+7y^2=p$ 有解。

如果 $3x^2+7y^2=8p$，x,y 必须同奇，此时 $3x^2+7y^2\equiv 2\pmod 8$，不可。所以 $3x^2+7y^2\neq 8p$。

如果 $3x^2+7y^2=7p$，$x=7x_1$，$3(7x_1)^2+7y^2=7p$，$21x_1^2+y^2=p$，$(y,7)=1$，此时有 $21x_1^2+y^2=p\equiv 1,2,4\pmod 7$，但根据条件：$\left(\frac{p}{7}\right)=-1$，矛盾，所以 $3x^2+7y^2\neq 7p$。

如果 $3x^2+7y^2=6p$，$y=3y_1$，$3x^2+7(3y_1)^2=6p$，$x^2+21y_1^2=2p$，x,y_1 同奇，且 $(x,3)=1$，根据所设条件知：$p\equiv 1\pmod 3$，$p\equiv 3\pmod 4$，所以 $2p\equiv 2\pmod 3$，但 $x^2+21y_1^2\equiv 1\pmod 3$，矛盾，因此 $3x^2+7y^2\neq 6p$。

如果 $3x^2+7y^2=5p$，x,y 一奇一偶，$(x,15)=1$，此时 $3x^2+7y^2\equiv 0,1,4\pmod 5$，当 $3x^2+7y^2=5s$ 时，$s\equiv 2\pmod 3$，但所给条件为 $p\equiv 1\pmod 3$，矛盾，因此 $3x^2+7y^2\neq 5p$。

如果 $3x^2+7y^2=4p$，x,y 同奇，此时 $3x^2+7y^2\equiv 2\pmod 8$，所以 $3x^2+7y^2\neq 4p$。

如果 $3x^2+7y^2=3p$，则 $y=3y_1$，$3x^2+7(3y_1)^2=3p$，$x^2+21y_1^2=p$，$(x,21)=1$，x,y 一奇一偶。所以 $x^2+21y_1^2=p\equiv 1\pmod 4$，但条件所设为 $p\equiv -1\pmod 4$，矛盾，所以 $3x^2+7y^2\neq 3p$。

如果 $3x^2+7y^2=2p$， x,y 同奇，所以 $3x^2+7y^2\equiv 2(\mathrm{mod}8)$，而根据所设条件： $p\equiv -1(\mathrm{mod}4)$，所以 $2p\not\equiv 2(\mathrm{mod}8)$，矛盾，因此 $3x^2+7y^2\neq 2p$。

综上所述：只有

$$3x^2+7y^2=p.$$

设 p 为奇素数，用以上相同的方法可以证明以下不定方程有解存在充分条件：

$3x^2+8y^2=p$：有解的充分条件：$\left(\frac{-3}{8}\right)=1,\left(\frac{p}{3}\right)=-1,\left(\frac{2}{p}\right)=-1,\left(\frac{-1}{p}\right)=-1$。

$3x^2+10y^2=p$::有解的充分条件：$\left(\frac{-3}{10}\right)=1,\left(\frac{2}{p}\right)=-1,\left(\frac{p}{3}\right)=1,\left(\frac{p}{5}\right)=-1$。

$3x^2+11y^2=p$：有解的充分条件：$\left(\frac{-3}{11}\right)=1,\left(\frac{-3}{p}\right)=-1,\left(\frac{p}{11}\right)=1,\left(\frac{-1}{p}\right)=-1$。

$3x^2+14y^2=p$：有解的充分条件：$\left(\frac{-3}{14}\right)=1,\left(\frac{-2}{p}\right)=1,\left(\frac{-3}{p}\right)=-1,\left(\frac{p}{7}\right)=-1$。

$3x^2+19y^2=p$：有解的充分条件：$\left(\frac{-3}{19}\right)=1,\left(\frac{p}{3}\right)=1,\left(\frac{p}{19}\right)=-1,\left(\frac{-1}{p}\right)=-1$。

$3x^2+20y^2=p$：有解的充分条件：$\left(\frac{-3}{20}\right)=1,\left(\frac{-3}{p}\right)=-1,\left(\frac{p}{5}\right)=-1,\left(\frac{-1}{p}\right)$

$=-1$。

$3x^2+26y^2=p$：有解的充分条件：$\left(\frac{-3}{26}\right)=1,\left(\frac{2}{p}\right)=-1,\left(\frac{-3}{p}\right)=-1,\left(\frac{p}{13}\right)=1$。

$3x^2+31y^2=p$：有解的充分条件：$\left(\frac{-3}{31}\right)=1,\left(\frac{p}{3}\right)=1,\left(\frac{p}{31}\right)=-1,\left(\frac{-1}{p}\right)=-1$。

$3x^2+34y^2=p$：有解的充分条件：$\left(\frac{-3}{34}\right)=1,\left(\frac{2}{p}\right)=-1,\left(\frac{p}{3}\right)=1,\left(\frac{p}{17}\right)=-1$。

$3x^2+70y^2=p$：有解的充分条件：$\left(\frac{-3}{70}\right)=1,\left(\frac{-2}{p}\right)=1,\left(\frac{p}{3}\right)=1,\left(\frac{p}{5}\right)=-1,$

$\left(\frac{p}{7}\right)=-1$。

定理 15. 设 p 为奇素数， $p=6x^2+5y^2$ 有正整数解的充分条件是：$\frac{-6}{5}$ 是 p 的有理二次剩余和 $\left(\frac{p}{5}\right)=1$， $\left(\frac{2}{p}\right)=-1$ 及 $\left(\frac{-3}{p}\right)=-1$.

证：当 $\left(\frac{-6}{5}\right)^{\frac{p-1}{2}}\equiv 1(\bmod p)$ 且 $5^{\frac{p-1}{2}}\equiv 1(\bmod p), 2^{\frac{p-1}{2}}\equiv -1(\bmod p), (-3)^{\frac{p-1}{2}}\equiv -1$ 时， $\frac{-6}{5}$ 为 p 的有理二次剩余，即存在 $a<p$ 使 $a^2\equiv -\frac{6}{5}(\bmod p)$，或有 $5a^2\equiv -6(\bmod p)$。根据引理 1 有

$$ax\equiv y(\bmod p),(x,y)=1.$$

$p\mid ax-y, p\mid (ax-y)(mx-5y)=amx^2+5y^2-(m+5a)xy$，令 $m=p-5a,$，则 $p\mid amx^2+5y^2=a(p-5a)x^2+5y^2=apx^2-5a^2x^2+5y^2, p\mid -5a^2x^2+5y^2$。

由于 $5a^2\equiv -6(\bmod p)$，则 $p\mid 6x^2+5y^2$ 或 $6x^2+5y^2=kp$， $k\geq 1$ 为整数。

由引理 1 知：$1\leq x<\sqrt{p}$， $1\leq |y|<\sqrt{p}$，所以

$$6x^2+5y^2<11p.$$

如果 $6x^2+5y^2=10p$， $x=5x_1$， $y=2y_1$， $6(5x_1)^2+5(2y_1)^2=10p$，或 $30x_1^2+2y_1^2=p$，因 $(y_1,5)=1$，$30x_1^2+2y_1^2=p\equiv 2,3,4(\bmod 5)$，但所给条件为：$\left(\frac{p}{5}\right)=1$，矛盾，所以 $6x^2+5y^2\neq 10p$。

如果 $6x^2+5y^2=9p$，则 $y=3y_1$， $6x^2+5(3y_1)^2=9p$， $2x^2+15y_1^2=3p$，$x=3x_1$， $2(3x_1)^2+15y_1^2=3p$， $6x_1^2+5y_1^2=p$，此说明 $6x^2+5y^2=p$ 有解。

如果 $6x^2+5y^2=8p$， $y=2y_1$， $6x^2+5(2y_1)^2=8p$， $3x^2+10y_1^2=4p$，$x=2x_1$， $3(2x_1)^2+10y_1^2=4p$， $6x_1^2+5y_1^2=2p$， $y_1=2y_2$，$6x_1^2+5(2y_2)^2=2p$， $3x_1^2+10y_2^2=p$， $(x_1,10)=1$，$3x_1^2+10y_2^2=p\equiv 2,3(\bmod 5)$，但 $\left(\frac{p}{5}\right)=1$，矛盾，所以 $6x^2+5y^2\neq 8p$。

如果 $6x^2+5y^2=7p$，则 $\left(\frac{x}{y}\right)^2\equiv -\frac{5}{6}(\bmod 7)$，即 $\frac{-5}{6}$ 是 7 的有理二次剩余，但 $\left(\frac{-5}{6}\right)^{\frac{7-1}{2}}\equiv -1(\bmod 7)$，矛盾，所以 $6x^2+5y^2\neq 7p$。

如果 $6x^2+5y^2=6p$，$y=6y_1$，$6x^2+5(6y_1)^2=6p$，$x^2+30y_1^2=p$，x 为奇，$(x,30)=1$，所以 $x^2+30y_1^2=p\equiv 1(\bmod 3)$，但前设条件有：$\left(\frac{-3}{p}\right)=-1$，$p\equiv 2(\bmod 3)$，矛盾，所以 $6x^2+5y^2\neq 6p$。

如果 $6x^2+5y^2=5p$， $x=5x_1$， $6(5x_1)^2+5y^2=5p$， $30x_1^2+y^2=p$， y 为奇， $(y,30)=1$，所以， $30x_1^2+y^2=p\equiv 1(\bmod 3)$，但前设条件：

$\left(\frac{-3}{p}\right)=-1$， $p\equiv 2(\mathrm{mod}\,3)$，矛盾，所以 $6x^2+5y^2\neq 5p$。

如果 $6x^2+5y^2=4p$， $y=2y_1$， $6x^2+5(2y_1)^2=4p$， $3x^2+10y_1^2=2p$，$x=2x_1$， $3(2x_1)^2+10y_1^2=2p$， $6x_1^2+5y_1^2=p$，此说明 $6x^2+5y^2=p$ 有解。

如果 $6x^2+5y^2=3p$， $y=3y_1$， $6x^2+5(3y_1)^2=3p$， $2x^2+15y_1^2=p$，$(x,15)=1$， y 为奇，所以 $2x^2+15y_1^2=p\equiv 1,-1(\mathrm{mod}\,8)$，但前设条件有：$\left(\frac{2}{p}\right)=-1$， $p\equiv\pm 3(\mathrm{mod}\,8)$，矛盾，所以 $6x^2+5y^2\neq 3p$。

如果 $6x^2+5y^2=2p$， $y=2y_1$， $6x^2+5(2y_1)^2=2p$， $3x^2+10y_1^2=p$，$(x,10)=1$， $3x^2+10y_1^2=p\equiv 2,3(\mathrm{mod}\,5)$，但根据条件：$\left(\frac{p}{5}\right)=1$，矛盾，所以 $6x^2+5y^2\neq 2p$。

综上所述：只有

$$6x^2+5y^2=p.$$

设 p 为奇素数，用以上相同的方法可以证明以下不定方程有解存在充分条件：

$5x^2+8y^2=p$：有解的充分条件：$\left(\frac{\frac{-5}{8}}{p}\right)=1,\left(\frac{p}{5}\right)=-1,\left(\frac{2}{p}\right)=-1$。

$5x^2+12y^2=p$：有解的充分条件：$\left(\frac{\frac{-5}{12}}{p}\right)=1,\left(\frac{p}{5}\right)=-1,\left(\frac{-3}{p}\right)=-1,\left(\frac{1}{p}\right)=1$。

$5x^2+17y^2=p$：有解的充分条件：$\left(\frac{\frac{-5}{17}}{p}\right)=1,\left(\frac{p}{17}\right)=-1,\left(\frac{p}{5}\right)=-1,\left(\frac{1}{p}\right)=1$。

$5x^2+26y^2=p$：有解的充分条件：$\left(\frac{\frac{-5}{26}}{p}\right)=1,\left(\frac{-2}{p}\right)=-1,\left(\frac{p}{5}\right)=1,\left(\frac{p}{13}\right)=-1$。

$5x^2+38y^2=p$：有解的充分条件：$\left(\frac{\frac{-5}{38}}{p}\right)=1,\left(\frac{2}{p}\right)=-1,\left(\frac{p}{5}\right)=-1,\left(\frac{p}{19}\right)=1$。

$5x^2+42y^2=p$：有解的充分条件：$\left(\frac{\frac{-5}{42}}{p}\right)=1,\left(\frac{-2}{p}\right)=-1,\left(\frac{-3}{p}\right)=-1,\left(\frac{p}{7}\right)=-1$。

$5x^2+66y^2=p$：有解的充分条件：$\left(\frac{\frac{-5}{66}}{p}\right)=1,\left(\frac{-2}{p}\right)=-1,\left(\frac{-3}{p}\right)=-1,$

$\left(\frac{p}{5}\right)=1,\left(\frac{p}{11}\right)=1$。

有理 k 次剩余的定义：

设 $m,a,b\in N^+$，若 $(ab,m)=(a,b)=1$，且同余方程 $ax^k\equiv b\pmod m$ 有解，则称 $\frac{b}{a}$ 是 m 的有理 k 次剩余。$k\geq 2$。

若同余方程 $ax^k\equiv b\pmod m$ 无解，则称 $\frac{b}{a}$ 是 m 的有理 k 次非剩余。$k\geq 2$。

定理 16. 设 p 为奇素数，$a,b\in N^+$，$k>2$，$p\equiv 1\pmod k$，$(ab,p)=(a,b)=1$，$p-1=kq$，则 $\frac{b}{a}$ 是模数 p 的一个有理 k 次剩余的充分必要条件是

$$\left(\frac{b}{a}\right)^{\frac{p-1}{k}}=\left(\frac{b}{a}\right)^q\equiv 1\pmod p.$$

证：设 $\frac{b}{a}$ 是模数 p 的一个有理 k 次剩余，则存在 $(x,p)=1$ 满足 $ax^k\equiv b\pmod p$，故 $\left(ax^k\right)^q\equiv b^q\pmod p, x^{kq}=x^{p-1}\equiv\left(\frac{b}{a}\right)^q\equiv 1\pmod p.$

反之，设 $\left(\frac{b}{a}\right)^q\equiv 1\pmod p$，$g$ 是 p 的一个原根，则有 $qind_g\left(\frac{b}{a}\right)\equiv q\left(ind_g(b)-ind_g(a)\right)\equiv 0\pmod{p-1}$，即 $ind_g(b)-ind_g(a)\equiv 0\left(\mod\frac{p-1}{q}\right)$，因此，$k=\frac{p-1}{q}\left|ind_g(b)-ind_g(a)=ind_g\left(\frac{b}{a}\right)\right.$。

即 $\frac{b}{a}$ 是模数 p 的一个有理 k 次剩余。

定理 17. 设 p 为素数，$a,b\in N^+$，$k>2$，$(k,p-1)=(ab,p)=(a,b)=1$，则 $\frac{b}{a}$ 是模数 p 的一个有理 k 次剩余。

证：现证 $ax_i^k\not\equiv ax_j^k\pmod p$。设 $i,j=1,2,\cdots,p-1$。$i\neq j$，若 $ax_i^k\equiv ax_j^k\pmod p$，$(a,p)=1$，所以 $x_i^k-x_j^k\equiv 0\pmod p$，又因 $(p-1,k)=1$，因此 $x_i^k\not\equiv x_j^k\pmod p$。$ax_i^k\not\equiv ax_j^k\pmod p$。这证明：当 i 跑过 p 的完全剩余系时，ax_i^k 也跑过 p 的完全剩余系，所以，对于任意 b，$(b,a)=1$，$(ab,p)=1$，总存在一个 x 使 $ax^k\equiv b\pmod p$，故 $\frac{b}{a}$ 是模数 p 的一个有理 k 次剩余。

定理 18. 设 $k\equiv 1\pmod 2$，$(p-1,k)=1$，p 为奇素数，则 p 的全部有理 k 次剩余(包括整数 k 次剩余)共有：

$$\sum_{i=1}^{p-1}\varphi_i\{p\text{的全体整数 }k\text{ 次剩余}\}+\sum_{i=1}^{p-1}\varphi_i\{p\text{的全体整数 }k\text{ 次非剩余}\}$$

p 的全部有理 k 次非剩余(包括整数 k 次非剩余)共有：0 个。

证：由定理 17 和以上定义可证。

例：求 7 的全部有理 5 次剩余及其个数。

7 的有理 5 次剩余有：

$$1^5\equiv 1,2^5\equiv 4,3^5\equiv 5,4^5\equiv 2,5^5\equiv 3,6^5\equiv 6,2^5\equiv\frac{1}{2},3^5\equiv\frac{3}{2},6^5\equiv\frac{5}{2},3^5\equiv\frac{1}{3}\left(\mathrm{mod}\,7\right)$$

$$5^5\equiv\frac{2}{3},6^5\equiv\frac{4}{3},2^5\equiv\frac{5}{3},4^5\equiv\frac{1}{4},6^5\equiv\frac{3}{4},5^5\equiv\frac{5}{4},5^5\equiv\frac{1}{5},6^5\equiv\frac{2}{5},4^5\equiv\frac{3}{5},3^5\equiv\frac{4}{5}\left(\mathrm{mod}\,7\right)$$

$$2^5\equiv\frac{6}{5},6^5\equiv\frac{1}{6},4^5\equiv\frac{5}{6}\left(\mathrm{mod}\,7\right).$$

共有 23 个。

7 的整数 5 次剩余有：1，2，3，4，5，6。7 的整数 5 次非剩余有：0 个。

因 $\left(7-1,5\right)=1$，根据定理 15 可得：

$$\sum_{i=1}^{6}\varphi_i\left\{1,2,3,4,5,6\right\}=\left(6+3+4+3+5+2\right)=23.$$

定理 19. 设 $p\equiv 1\left(\mathrm{mod}\,k\right)$ 为奇素数，$a,b\in N^+$，$\left(p,ab\right)=\left(a,b\right)=1$，$p-1=kq$，则

$$\sum_{j=0}^{k-1}\left(\frac{b}{a}\right)^{jq}\equiv\begin{cases}k\left(\mathrm{mod}\,p\right),\text{若}\dfrac{b}{a}\text{是模数 }p\text{ 的有理 }k\text{ 次剩余}\\0\left(\mathrm{mod}\,p\right),\text{若}\dfrac{b}{a}\text{是模数 }p\text{ 的有理 }k\text{ 次非剩余}\end{cases}$$

证：因 $\left(ab,p\right)=1$，我们有

$$a^{p-1}\equiv 1\left(\mathrm{mod}\,p\right),b^{p-1}\equiv 1\left(\mathrm{mod}\,p\right),\left(\frac{b}{a}\right)^{p-1}-1=\left(\frac{b}{a}\right)^{kq}-1\equiv 0\left(\mathrm{mod}\,p\right).$$

即得

$$\left(\left(\frac{b}{a}\right)^{q}-1\right)\left(1+\left(\frac{b}{a}\right)^{q}+\left(\frac{b}{a}\right)^{2q}+\cdots+\left(\frac{b}{a}\right)^{(k-1)q}\right)\equiv 0\left(\mathrm{mod}\,p\right).$$

如果 $\dfrac{b}{a}$ 是模数 p 的一个有理 k 次剩余，则有

$$\sum_{j=0}^{k-1}\left(\frac{b}{a}\right)^{jq}\equiv k\left(\mathrm{mod}\,p\right).$$

如果 $\dfrac{b}{a}$ 是模数 p 的一个有理 k 次非剩余，则

$$\sum_{j=0}^{k-1}\left(\frac{b}{a}\right)^{jq}\equiv 0\left(\mathrm{mod}\,p\right).$$

有理 k 次剩余的应用：

定理 20：设 p 为奇素数，$a,b\in N^+$，$\left(ab,p\right)=\left(a,b\right)=\left(x,y\right)=1$，则 $p=ax^k+by^k$ 有整数解的必要条件是：$\dfrac{-a}{b}$ 是 p 的有理 k 次剩余。

证：若 $p=ax^k+by^k$ 有正整数解，必有 $\left(p,x\right)=\left(p,y\right)=1$，因若不然，比如 $p\mid x$ 就推出 $p\mid y$，于是 $p=a\left(px_1\right)^k+b\left(py_1\right)^k$，这是不可能的，于是必有 x_1 使 $\left(p,x_1\right)=1$ $xx_1\equiv 1\left(\mathrm{mod}\,p\right)$，从而

$$a(xx_1)^k + b(yx_1)^k = px_1^k \equiv 0 \pmod{p}$$

即 $b(yx_1)^k + a \equiv 0 \pmod{p}$

或 $(yx_1)^k \equiv \frac{-a}{b} \pmod{p}$.

这表明 $\frac{-a}{b}$ 为 p 之有理 k 次剩余。

定理 21. 设 p 为奇素数，$k \equiv 1 \pmod{2}$，$p \equiv 1 \pmod{k}$，$a,b \in N^+$，$(ab,p)=(a,b)=1$，如果 $\frac{-b}{a}$ 是 p 的有理 k 次非剩余，则 $p = ax^k + by^k$ 没有整数解。

证：因 $\frac{-b}{a}$ 是模数 p 的有理 k 次非剩余，$ax^k \equiv -b \pmod{p}$ 无解，根据引理 2 不定方程

$$p = ax^k + by^k$$

无整数解。

定理 22. 设 p 为奇素数，$k \equiv 1 \pmod{2}$，$p \equiv 1 \pmod{k}$，$a,b \in N^+$，$(ab,p)=(a,b)=1$，如果 $\frac{b \pmod{p}}{a}$ 是 p 的有理 k 次非剩余，则 $p = ax^k - by^k$ 没有整数解。

证：因 $\frac{b \pmod{p}}{a}$ 是模数 p 的有理 k 次非剩余，$ax^k \equiv b \pmod{p} \pmod{p}$ 无解，根据引理不定方程 $p = ax^k - by^k$ 无整数解。

4. 猜想

猜想 1：

$\varphi_k\{\text{正整数的集合}\}$ 表示集合中第 k 个数与这个集合中的所有数互素的个数。集合中的数按从小到大顺序排列。

$\varphi_i(n)$ 为不大于 n 且与 i 互素的数的个数[4]；

$\varphi(k)$ 为 k 的欧拉函数。

令 u = 素数 p 的全部有理二次剩余个数，令 v = 素数 p 的全部有理二次非剩余个数，则

1) $u < \sum_{k=1}^{p-1} \varphi(k) \le v$。

2) $\frac{u+v+1}{2} = \sum_{k=1}^{p-1} \varphi(k)$。

3) 设 $k \equiv 1 \pmod{2}$，$(p-1,k)=1$，p 为奇素数，设 p 的全部有理 k 次剩余(包括整数 k 次剩余) $= w$，则

$$w = 2\sum_{k=1}^{p-1} \varphi(k) - 1.$$

4) $m > 2$ 为偶数，则

$$\sum_{i=1}^{\frac{m}{2}} \varphi_i\left\{1,2,\cdots,\frac{m}{2}\right\} + \sum_{j=1}^{\frac{m}{2}} \varphi_j\left\{\frac{m}{2}+1,\frac{m}{2}+2,\cdots,m\right\} + 1 = \sum_{k=1}^{m} \varphi(k).$$

5) $m>1$为奇数，则

$$\sum_{i=1}^{\frac{m+1}{2}}\varphi_i\{1,3,5,\cdots,m\}=\sum_{k=0}^{\frac{m-1}{2}}\varphi(2k+1).$$

6) $m\equiv 1(\mathrm{mod}\,4)$则

$$\varphi_{\frac{m+3}{4}}\{1,3,5,\cdots,m\}=\varphi\left(\frac{m+1}{2}\right).$$

7) $m\equiv -1(\mathrm{mod}\,4)$，则

$$\varphi_{\frac{m+1}{4}}\{1,3,5,\cdots,m\}+\varphi_{\frac{m+5}{4}}\{1,3,5,\cdots,m\}=\varphi\left(\frac{m-1}{2}\right)+\varphi\left(\frac{m+3}{2}\right).$$

8) $n\geq 2$，则

$$\sum_{i=1}^{n}\varphi_i(n)+1=2\sum_{k=1}^{n}\varphi(k).$$

猜想 2：

1) 设 p 为奇素数，a,b 一奇一偶，$a,b>1$，如果不定方程 $ax^2+by^2=p$ 有解是具有充分条件的，则

$$a+b=\text{素数}.$$

2) 设 p 为奇素数，a,b 均为奇数，$a,b>1$，如果不定方程 $ax^2+by^2=p$ 有解是具有充分条件的，则

$$\frac{a+b}{2}=\text{素数}.$$

a,b 不同时等于 3 和 5。

5. 结束语

素数 p 的有理二次剩余的个数要比 p 的整数二次剩余多很多，我们可以用有理二次剩余来解决整数二次剩余不能解决的问题，如 $az^2\equiv\pm b(\mathrm{mod}\,p)$ 是否有解的判定问题，直接关系到不定方程 $ax^2\pm by^2=p$ 的整数解的问题。这其实是 $\frac{b}{a}$ 是否为 p 的二次剩余的判定问题。对于有理二次剩余用在不定方程 $ax^2\pm by^2=m$ （m 为奇数)的整数解的问题，还需要作进一步的研究。

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] 肯尼思·罗森. 初等数论及其应用[M]. 夏鸿刚, 译. 北京: 机械工业部出版社, 2009: 293.

[2] 陈景润. 初等数论[M]. 北京: 科学出版社, 1988: 190-191.

[3] Zhou, Z.Q. (2024) The Solution of the Indefinite Equation by the Method Ean Algorithm. *Open Access Library Journal*, **11**, e12011. https://doi.org/10.4236/oalib.1112011

[4] Zhou, Z.Q. and Zhou S.J. (2024) The Generalization of Combination Number . *Open Access Library Journal*, **11**, e12012. https://doi.org/10.4236/oalib.1112012

Appendix (Abstract and Keywords in Chinese)

有理二次剩余的研究

摘要：文中提出了有理二次剩余的概念，即分数二次剩余。还给出了分数为模数 p 的二次剩余的判定方法和有理二次剩余的计算符号以及从有理勒让德符号转换为一般勒让德符号的计算公式。推导了有理二次剩余和有理二次非剩余个数的计算公式。还重点给出了多个有理二次剩余的实际应用的范例。文章还对有理 k 次剩余的判别和应用作了一些研究。最后提出了几个与有理二次剩余有关的猜想。

关键词：有理 k 次剩余，有理二次剩余的判定方法，有理二次非剩余，二元二次不定方程，不定方程有解的充分必要条件，猜想