模 p 法讨论丢番图方程

方 辉,林慧敏
(黄山学院 数学系,安徽 黄山 245021)

摘 要:利用模 p(或 p 的方幂)法,结合数论中关于素数 p 的基本性质和结论,非常有效的讨论了几类丢番图方程无解,及求解等问题。

关键词:素数;模法;二次互反律;丢番图方程
中图分类号:O156 **文献标识码**:A **文章编号**:1672-447X(2008)05-0005-05

1 引言

丢番图方程是讨论整系数方程 $f(x_1,x_2,\cdots,x_n)=0$ 的整数解和有理解问题。公元 3 世纪,古希腊数学家丢番图(Diophantus)所著的《算术》中研究了一次与二次方程(组)有理数解和整数解的各种方法。

丢番图的《算术》一书于 1621 年被译成拉丁文。17 和 18 世纪的大数学家 Fermat,Euler,Legendre 等都研究了丢番图方程。1637 年,Fermat 在阅读此书中讨论 Pythagorean 方程 $x^2+y^2=z^2$ 的那一页空白处写了一个评注。他认为每个整数 $n(\geq 3)$,方程 $x^n+y^n=z^n$ 都没有正整数解,并声称给出了这一猜想的一个巧妙的证明,但空白处太小写不下。自那以后,人们只看到 Fermat 对 $n=4$ 的证明。直到 1995 年才由 Andre Wiles 给出完整的证明。文献[1]给出 300 多年来,为了解决 Fermat 猜想,引进了一系列深刻的数学概念,建立了一个又一个重要的数学理论,人类的智慧得以充分的体现,因此丢番图方程的研究一直是数论中一个重要分支。

所谓模 P(或 P 的方幂)法:关于整数的命题(含丢番图方程,整系数多项式,整系数矩阵,群的阶等问题),通过模素数 P(或 P 的方幂)进行计算,判定命题正确与否的方法。

文献[2]和[3]是丢番图方程的专业论著,为讨论丢番图方程提出了因式分解法、不等式法、无穷递降法,二次互反律法、模 P(或 P 的方幂)法、连分数法、理想分解法、局部域法、椭圆曲线法等等方法。本文应用模 P(或 P 的方幂)法,讨论几类丢番图方程解的判定问题。

2 丢番图方程问题

我们将讨论丢番图方程 $f(x_1,x_2,\cdots,x_n)=0$ 无解或无非平凡解的问题,利用下面的事实:若 $f(x_1,x_2,\cdots,x_n)=0$ 有解,则同余式 $f(x_1,x_2,\cdots,x_n)\equiv 0(\mathrm{mod}\,p^s)$ 必有解。即同余式 $f(x_1,x_2,\cdots,x_n)\equiv 0(\mathrm{mod}\,p^s)$ 无解,则丢番图方程 $f(x_1,x_2,\cdots,x_n)=0$ 无非平凡解或无解。因此就可以利用上述的结论去探讨一些简单的丢番图方程,文献[4]给出下面需要的一些结论。

命题 1 欧拉判别法则设 p 为奇素数,

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

其中 $\left(\frac{a}{p}\right)$ 为 Legendre 符号。

收稿日期:2008-08-30
基金项目:安徽省教育厅教研基金资助(2007jyxm113)
作者简介:方辉(1963-),安徽休宁人,黄山学院数学系副教授,研究方向为代数与数论。
林慧敏(1974-),安徽怀远人,黄山学院数学系讲师,研究方向为典型群与代数。

命题 2 设 p 为奇素数,则

(ⅰ) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1, p\equiv 1(\mathrm{mod}\,4)\\-1, p\equiv -1(\mathrm{mod}\,4)\end{cases}$

(ⅱ) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, p\equiv \pm 1(\mathrm{mod}\,8)\\-1, p\equiv \pm 3(\mathrm{mod}\,8)\end{cases}$

命题 3 (二次互反律)设 p 和 q 是两个不同的奇素数,则 $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}=\begin{cases}1, p(\text{或}q)\equiv 1(\mathrm{mod}\,4)\\-1, p\equiv q\equiv 3(\mathrm{mod}\,4)\end{cases}$

命题 4 正整数

$$n=x^2+y^2 \Leftrightarrow n=2^{\alpha}\left(\prod_{i=1}^{r}p_i^{\beta}\right)\left(\prod_{j=1}^{s}q_j^{\gamma_j}\right)$$

其中 $p_i\equiv 1(\mathrm{mod}\,4), i=1,2,\cdots,r$, $q_j\equiv 3(\mathrm{mod}\,4), \gamma_j \equiv 0(\mathrm{mod}\,2), j=1,2,\cdots,s$。特别地,$4k+1$ 型素数可以表为两平方数之和,$4k+3$ 型素数不可以表为两平方数之和,又称为表二平方和问题。

2.1 模 2(或 2^{α})的基本类型

类型(1):方程 $x^2+y^2=4z+3$ (1)

无整数解。

证明:因为 $x^2\equiv 0,1(\mathrm{mod}\,4)$, $y^2\equiv 0,1(\mathrm{mod}\,4)$, 则 $x^2+y^2\equiv 0,1,2\not\equiv 3(\mathrm{mod}\,4)$ 所以方程(1)式没有整数解。

变式(ⅰ)当 a 为整数, n 为非负整数时,方程

$$x^2+y^2\equiv(4a+3)^{2n+1}z^2 \quad (2)$$

仅有平凡解 $x=y=z=0$ 。

证明:当 $a<0$ 时,(2)两边一正一负,故此时无解。当 $a>0$ 时,假设 x,y,z 是方程(2)的非平凡解,且满足 $(x,y,z)=1$ 对(2)式。两边模 4,可得

$z\equiv 0(\mathrm{mod}\,2)$ (否则 $x^2+y^2\equiv 3(\mathrm{mod}\,4)$,矛盾)

$\Rightarrow x^2+y^2\equiv 0(\mathrm{mod}\,4)$ 即 $x\equiv y\equiv 0(\mathrm{mod}\,2)$ 与 $(x,y,z)=1$ 矛盾。

注:类型(1)和变式(ⅰ)都是命题 4 的特殊情形推出。

变式(ⅱ)方程 $x^2+2y^2=8z+5$ 或 $8z+7$ 和 $x^2-2y^2=8z+3$ 或 $8z+5$ 没有整数解。

变式(ⅲ)方程 $x^2+y^2+z^2=4^{\alpha}(8w+7)$ (3)

无整数解。

证明:当 $\alpha\geq 1$ 时, $x^2+y^2+z^2\equiv 0(\mathrm{mod}\,4)\Rightarrow x\equiv y\equiv z\equiv 0(\mathrm{mod}\,2)$。所以我们只需验证 $\alpha=0$ 的情形,由于 $n^2\equiv 0,1(\mathrm{mod}\,2^3)$,可得:

$x^2+y^2+z^2\not\equiv 7(\mathrm{mod}\,2^3)$。所以方程(3)式无整数解。

类型(2) 当 $a\equiv b\equiv c\equiv 1(\mathrm{mod}\,2)$ 和; $a\equiv b\equiv c(\mathrm{mod}\,4)$ 或 $\frac{a}{2}\equiv b\equiv c\equiv 1(\mathrm{mod}\,2)$ 和 $b+c\equiv a,4(\mathrm{mod}\,8)$ 时。

方程 $ax^2+by^2+cz^2=0 \quad abc\neq 0 \quad (x,y,z)=1$ (4)

无非平凡解。

证明:当 $a\equiv b\equiv c\equiv 1(\mathrm{mod}\,2)$ 和 $a\equiv b\equiv c(\mathrm{mod}\,4)$ 时,及 $(x,y,z)=1$,则 $ax^2+by^2+cz^2\equiv x^2+y^2+z^2\not\equiv 0(\mathrm{mod}\,4)$, 故方程无非平凡解。

当 $\frac{a}{2}\equiv b\equiv c\equiv 1(\mathrm{mod}\,2)$ 和 $b+c\equiv a,4(\mathrm{mod}\,8)$ 时,及 $(x,y,z)=1$ 。

由条件知 $a+b+c\not\equiv 0(\mathrm{mod}\,8)$,故 x,y,z 不可能都是奇数,只能是二奇一偶或二偶一奇。

若 x 为奇数 (即 $x^2\equiv 1(\mathrm{mod}\,8)$), y,z 为偶数时,推出 $a+by^2+cz^2\equiv 0(\mathrm{mod}\,8)$,可得 $a\equiv 0(\mathrm{mod}\,4)$ 与条件不符。若 x,y 为偶数, z 为奇数时,可以推出 $by^2+c\equiv 0(\mathrm{mod}\,8)$,即得 c 是偶数,矛盾。可以类似地讨论 y 为奇数,x,z 为偶数的情形也不发生。

若 x 为偶数, y,z 为奇数时,

$ax^2+by^2+cz^2\equiv b+c\equiv 2\not\equiv 0(\mathrm{mod}\,8)$,

矛盾。若 x,y 为奇数, z 为偶数时,

$ax^2+by^2+cz^2\equiv a+b+cz^2\equiv 0(\mathrm{mod}\,8)$,可得 $a+b\equiv 0(\mathrm{mod}\,4)$,与条件也不符。若 y 为奇数,x,z 为偶数时, $ax^2+by^2+cz^2\equiv a+by^2+c\equiv 0(\mathrm{mod}\,8)$,可得 $a+c\equiv 0(\mathrm{mod}\,4)$,也与条件不符。综上所得方程(4)式无非平凡解。

注:若丢番图方程的次数是齐次的,则有平凡解。

变式(ⅰ)当 $a+b\equiv 0(\mathrm{mod}\,2), cd\equiv 1(\mathrm{mod}\,4), k\equiv 1(\mathrm{mod}\,2)$ 时方程 $z^2=(ax^2+by^2)^2-2k(cx^2+dy^2)^2$ (5)

仅有平凡解。

变式(ⅱ)当 $a\equiv b\equiv c\equiv \pm 1(\mathrm{mod}\,4)$ 时

方程 $ax^2+by^2+cz^2=2dxyz$ (6)

仅有平凡解。

变式(ⅲ)当 $a_i,b_i,c_i,d_i(i=1,2,3,4)$ 都是奇数，$a_1\equiv a_2\equiv a_3\equiv a_4(\mathrm{mod}\,8)$，$b_1\equiv b_2\equiv b_3\equiv b_1(\mathrm{mod}\,8)$，$(c_1+c_2+c_3+c_4)(d_1+d_2+d_3+d_4)\equiv 0(\mathrm{mod}\,2^4)$；则方程 $(\sum_{i=1}^{1}a_ix_i^2)(\sum_{i=1}^{1}b_ix_i^2)=2k(\sum_{i=1}^{1}c_ix_i^2)(\sum_{i=1}^{1}d_ix_i^2)$(7) 仅有平凡解。

注：1.变式的证明方法与类型(2)的证明方法雷同；2.我们对这些变式的系数赋值，可以得到一些具体的丢番图方程，例如：方程 $x^2+y^2+z^2=2xyz$ 仅有平凡解，等等。

2.2　模 3(或 3^α)的基本类型

类型　当 $c\not\equiv 0(\mathrm{mod}\,3)$ 时，方程 $(3a+1)x^2+(3b+1)y^2=c$(8) 无整数解。

证明：假设(8)有解 x,y 我们对(8)式两边模 3 可得：$x^2+y^2\equiv 0(\mathrm{mod}\,3)\Rightarrow x\equiv y\equiv 0(\mathrm{mod}\,3)$，即推出 $c\equiv 0(\mathrm{mod}\,3)$，矛盾。

变式(ⅰ)方程 $x^2+y^2+z^2=9w\pm 4$　　(9) 无整数解。

变式(ⅱ)方程 $x^3+3y^3+9z^3-9xyz=0$ 和 $x^3+2y^3+4z^3=9w^3$ 仅有平凡解。

变式(ⅲ)当 $a\equiv d\equiv 4(\mathrm{mod}\,3^2)$，$b\equiv 0(\mathrm{mod}\,3)$，$c\equiv\pm 1(\mathrm{mod}\,3)$ 时，则方程 $ax^3+3bx^2y+3cxy^2+dy^3=z^3$ (10) 仅有平凡解。

证明：假设方程(10)式有非平凡解 x,y,z，且 $(x,y,z)=1$，可知 $xy\not\equiv 0(\mathrm{mod}\,3)$ (否则可推出 $3\mid(x,y,z)$，与 $(x,y,z)=1$，矛盾)，且 $3\nmid z$，由 $x^2\equiv y^2\equiv z^2\equiv 1(\mathrm{mod}\,3)\Rightarrow z\equiv ax+dy(\mathrm{mod}\,3)$，将它代入(10)式得 $z^3\equiv a^3x^3+3a^2dx^2y+3ad^2xy^2+d^3y^3(\mathrm{mod}\,3^2)$，可得 $\left(\frac{a-a^3}{3}\right)x^3+\left(b-a^2d\right)x^2y+\left(c-ad^2\right)xy^2+\left(\frac{d-d^3}{3}\right)y^3\equiv 0(\mathrm{mod}\,3)$ 由于费马小定理知 $x^3\equiv x(\mathrm{mod}\,3)$，$y^3\equiv y(\mathrm{mod}\,3)$，及 $x^2\equiv 1(\mathrm{mod}\,3)$，$y^2\equiv 1(\mathrm{mod}\,3)$ 我们有 $x+(b-1)y+(c-1)x+y\equiv 0(\mathrm{mod}\,3)\Rightarrow x\equiv 0(\mathrm{mod}\,3)$ 与 $xy\not\equiv 0(\mathrm{mod}\,3)$ 矛盾，故方程(10)式无非平凡解。

2.3　模 7(或 7^α)的基本类型

类型方程

$(7a+1)x^3+(7b+2)y^3+(7c+4)z^3+(7d+1)xyz=0$(11) 仅有平凡解。

证明：设方程(11)式有非平凡解 x,y,z，且 $(x,y,z)=1$ 对(11)式两边模 7 可得：$x^3+2y^3+4z^3+xyz\equiv 0(\mathrm{mod}\,7)$，注意到 $n^3\equiv 0,\pm 1(\mathrm{mod}\,7)$，其中 n 为任意整数。

若 $z\equiv 0(\mathrm{mod}\,7)\Rightarrow x^3+2y^3\equiv 0(\mathrm{mod}\,7)$，有 $x\equiv y\equiv 0(\mathrm{mod}\,7)$，矛盾。

故 $z\not\equiv 0(\mathrm{mod}\,7)$，可设 $x\equiv x_1z,y\equiv y_1z$，则 $x_1^3+2y_1^3+x_1y_1+4\equiv 0(\mathrm{mod}\,7)$，很明显 $x_1y_1\not\equiv 0(\mathrm{mod}\,7)$，因此 $x_1^3\equiv\pm 1(\mathrm{mod}\,7)$，$y_1^3\equiv\pm 1(\mathrm{mod}\,7)$。我们需要验证下面几种情况都是不可能的。

① $x_1^3\equiv y_1^3\equiv 1(\mathrm{mod}\,7)\Rightarrow x_1y_1\equiv 0(\mathrm{mod}\,7)$，与 $x_1y_1\not\equiv 0(\mathrm{mod}\,7)$ 矛盾；

② $x_1^3\equiv y_1^3\equiv 1(\mathrm{mod}\,7)\Rightarrow x_1y_1\equiv -1(\mathrm{mod}\,7)$，于是 $1\equiv x_1^3y_1^3\equiv -1(\mathrm{mod}\,7)$，矛盾；

③ $x_1^3\equiv y_1^3\equiv 1(\mathrm{mod}\,7)\Rightarrow x_1y_1\equiv 4(\mathrm{mod}\,7)$，于是 $-1\equiv x_1^3y_1^3\equiv 1(\mathrm{mod}\,7)$，矛盾；

④ $x_1^3\equiv y_1^3\equiv 1(\mathrm{mod}\,7)\Rightarrow x_1y_1\equiv 2(\mathrm{mod}\,7)$，于是 $-1\equiv x_1^3y_1^3\equiv 1(\mathrm{mod}\,7)$，矛盾。

所以方程(11)式无非平凡解。

变形方程 $x^3+2y^3=7(z^3+2w^3)$　　(12) 无非平凡解。

证明：设方程(12)的非平凡解，满足 $(x,y,z,w)=1$，若 $7\nmid y$，则 $y^3\equiv\pm 1(\mathrm{mod}\,7)$，于是有 $(\pm x)^3+2\equiv 0(\mathrm{mod}\,7)$，这是不可能的；故 $7\mid y\Rightarrow 7\mid x$，再对(12)式两边模 7^2 可得 $z^3+2w^3\equiv 0(\mathrm{mod}\,7)$，用上面同样的方法可推出：$7\mid z,7\mid w$ 与 $(x,y,z,w)=1$ 矛盾，所以方程(12)仅有平凡解。

2.4　模 p (或 p^α)的基本类型

类型(1)当 $p\equiv 3(\mathrm{mod}\,4)$ 时，方程 $x^2+1=py$ (13) 无整数解。

证明：当 $p\equiv 3(\mathrm{mod}\,4)$，由命题 2 知：$\left(\frac{-1}{p}\right)=-1$，则二次同余方程 $x^2+1\equiv 0(\mathrm{mod}\,p)$ 无解，所以方程(13)无整数解。

变式(ⅰ)当 a 有素因子 p，且 $p\equiv 3(\mathrm{mod}\,4)$ 时；

则方程 $x^2+1=ay$ 无整数解。

变式(ⅱ)当 a 无平方因子含素因子 p，且 $p\equiv 3(\mathrm{mod}\,4)$ 时；则方程 $x^2+y^2=az^2$ 仅有零解。

变式(ⅲ)当 a 无平方因子且含素因子 p，满足 $p\equiv\pm 3(\mathrm{mod}\,8)$，则方程：$x^2-2y^2=az^2$ 仅有零解。

变式(ⅳ)当 a 无平方因子且含素因子 p，满足 $p\equiv 5,7(\mathrm{mod}\,8)$，则方程：$x^2+2y^2=az^2$ 仅有零解。

证明：设方程 $x^2+2y^2=az^2$ 有非平凡解，对方程两边模 p 得 $x^2\equiv -2y^2(\mathrm{mod}\ p)$，则由 $p\equiv 5,7(\mathrm{mod}\,8)$ 及命题 7 知：

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}=-1$$，矛盾，所以原方程仅有平凡解。

注：变式(ⅲ)可以用同样的方法证明。

类型(2)当 p,q 是素数，且满足 $p\equiv 3(\mathrm{mod}\,4)$，$q\equiv 1(\mathrm{mod}\,4)$ 时，方程 $x^2+qy^2=p$ (14) 无整数解。 x,y

证明：设方程(14)有解 x,y，由(8)式的两边分别模 p 和 q，可得 $\left(\frac{p}{q}\right)=1$，$\left(\frac{-q}{p}\right)=1$；当 $p\equiv 3(\mathrm{mod}\,4)$，$q\equiv 1(\mathrm{mod}\,4)$ 时，由命题 3 知：

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

与 $\left(\frac{p}{q}\right)\left(\frac{-q}{p}\right)=1$ 不符，故方程(14)无整数解。

注：利用方程(14)式无整数解，我们可以编写以下练习：

①设 $11\nmid a$，b 为任意整数，则 $11\nmid(a^2+5b^2)$。

②证明：方程 $x^2+17y^2=19$ 无整数解。

③若 p 和 $p+2$ 是孪生素数，且 p 可表为二平方和，证明方程 $x^2+py^2=p+2$ 无整数解。

证明：由命题 4 知 $p\equiv 1(\mathrm{mod}\,4)$，再根据(14)式知方程 $x^2+py^2=p+2$ 无整数解。

关于利用高次同余的基本性质及模 p (或 p 的方幂)法，讨论一些特殊的丢番图方程，这里不再给出，请参阅文献[3]。

我们在解丢番图方程时，有时模几个不同素数，有时会和分解因式法，无穷递降法，二次互反律等方法联合使用，会产生奇效，使问题的解决更简洁。

例 1 证明丢番图方程 $15x^2-7y^2=9$ 无整数解。

证明：对方程两边模 3，可得 $y\equiv 0(\mathrm{mod}\,3)$，再模 9 可得 $x\equiv 0(\mathrm{mod}\,3)$，令 $x=3x_1$，$y=3y_1$ 代入方程，化为 $15x_1^2-7y_1^2=1$，由 $y_1^2\equiv 0,\pm 1(\mathrm{mod}\,5)$，则 $2y_1^2+1\not\equiv 0(\mathrm{mod}\,5)$，故方程 $15x_1^2-7y_1^2=1$ 无整数解。

例 2 证明丢番图方程 $y^2+4=x^5$ 无整数解。

证明：由费马小定理知 $(x^5)^2=x^{10}\equiv 0,1(\mathrm{mod}\,11)$

$\Rightarrow x^5\equiv 0,\pm 1(\mathrm{mod}\,11)$；

由 $y^2\equiv 0,1,3,4,5,9(\mathrm{mod}\,11)$ 可得 $y^2+4\equiv 2,4,5,7,8,9(\mathrm{mod}\,11)$ 于是方程两边模 11 不相等，故方程无整数解。

例 3 设 m,n 是正整数，满足 $3mA=(m+3)^n+1$，A 是整数，证明 A 是奇数。

证明：当 m 是奇数时，显然 A 是奇数。当 m 是偶数时，由于 A 是整数，我们有 $0\equiv(m+3)^n+1\equiv m^n+1(\mathrm{mod}\,3)$

$\Rightarrow n=2k+1$，$m\equiv -1(\mathrm{mod}\,3)$，讨论下面情形：

①设 $m\equiv 0(\mathrm{mod}\,8)$，则 $(m+3)^n+1=3^{2k+1}+1\equiv 4(\mathrm{mod}\,2^3)$ 与 $3mA\equiv 0(\mathrm{mod}\,2^3)$ 矛盾。

②设 $m=4m_1$，m_1 是正奇数，从 $m\equiv -1(\mathrm{mod}\,3)$，则存在 m 的一个奇的素因子 p，满足 $p\equiv -1(\mathrm{mod}\,3)$，由于 A 是整数知，$(m+3)^n+1\equiv 3^{2k+1}+1\equiv 0(\mathrm{mod}\ p)$，可得 $(3^{k+1})^2\equiv -3(\mathrm{mod}\ p)$，注意到 $\left(\frac{p}{3}\right)=\left(\frac{-1}{3}\right)=-1$ 及 $\left(\frac{-3}{p}\right)=1$，然而命题 1，命题 3 知

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

$=(-1)^{p-1}\left(\frac{p}{3}\right)=-1$ 矛盾。

③设 $m=2m_1$，m_1 是正奇数，即 $m\equiv 2(\mathrm{mod}\,4)$，则 $3m\equiv 2(\mathrm{mod}\,4)$ 及 $(m+3)^n+1\equiv(2+3)^n+1\equiv 2(\mathrm{mod}\,4)$。所以 A 是奇数。

例 4 设 $n>1$，则丢番图方程 $y^3=4^n+x^2,(x,y)=1$(15) 仅有正整数解 $(x,y,z)=(11,5,1)$。

证明：如果(15)有正整数解，则显然有 $x\equiv 1(\mathrm{mod}\,2)$，$y\equiv 1(\mathrm{mod}\,4)$。由(15)得

$(2^z+x\sqrt{-1})(2^z+x\sqrt{-1})=y^3$，由于$\mathbb{Z}[\sqrt{-1}]$是唯一分解环，且$2\nmid x$，故$(2^z+x\sqrt{-1},2^z+x\sqrt{-1})=1$，因此可设$2^z+x\sqrt{-1}=(u+v\sqrt{-1})^3$，$y=u^2+v^2$

$\Rightarrow 2^z=u(u^2-3v^2)$，由于$y\equiv 1(\mathrm{mod}\,4)$可知$u,v$一奇一偶，可令$u=\pm 2^z, u^2-3v^2=\pm 1\Rightarrow 2^{2z}-3v^2=1$，再由$v^2\equiv 1(\mathrm{mod}\,8)$，即$z=1$，$v^2=1\Rightarrow y=5, x=11$。所以方程仅有正整数解$(x,y,z)=(11,5,1)$。

参考文献：

[1]冯克勤.代数数论简史[M].长沙：湖南教育出版社，2002.

[2]L.J.Mordell.DIOPHANTINEEQUATIONS[M].Academic Press London and New York, 1969:3-11.

[3]曹珍富.丢番图方程引论[M].哈尔滨：哈尔滨工业大学出版社，1987:13-17.

[4] Daniel E. Flath. Introduction to Number Theory [M].A Wiley-Interscience Publishing New York,1989.

责任编辑：胡德明

The Application of Mod P Method to Diophantine Equations

Fang Hui, Lin Huimin

(Department of Mathematics, Huangshan University, Huangshan245021, China)

Abstract: In this paper, the solution to several types of Diophantine equations is discussed by using mod p or mod idea with other prime properties.

Keywords: prime; congruence; mod p method; Quadratic Reciprocity Law

·徽州文化小资料·

歙砚的产生时期

歙砚始于唐代。据北宋治平年间(1064-1067 年)婺源县令唐积《婺源砚图谱》载："婺源砚在唐开元中，因猎人叶氏逐兽至长城里，见叠石如城垒状，莹洁可爱，因携之以归，刊粗成砚，温润大过端溪者。后数世，叶氏诸孙持以与令，令爱之，访得匠手琢为砚，由是天下始传。"歙砚石的主要产地在婺源县龙尾山。由此可知，歙砚砚石发现于唐开元年间(713-741 年)。稍后，歙砚即名闻天下。1976 年合肥出土的唐开成五年(840 年)箕形歙砚，石质细润，色泽清纯，是早期歙砚的珍贵遗存。南唐时期，歙砚大受宠遇，中主李璟精意翰墨，宝重歙石，专门在歙州设置"歙砚务"，选砚工高手李少微为砚官，并令其招徒传艺。后主李煜更对歙砚极为推崇，把歙砚与澄心堂纸、李廷珪墨誉为天下冠。宋代以后，歙砚获得更大发展，砚石开采规模扩大，歙砚精品不断涌现，名色之多、质地之细、雕镂之精，为诸砚之冠。宋代文学家、书法家黄庭坚曾探赏歙砚佳石后写下《砚山行》诗篇。蔡襄将歙砚与"和氏璧"相媲美，认为歙石价值连城。欧阳修赞誉歙砚"远出端溪上"、"世所罕见"。苏东坡为歙砚题咏了《龙尾砚歌》。