第12卷 第4期 华侨大学学报自然科学版 Vol. 12 №. 4
JOURNAL OF HUAQIAO UNIVERSITY
1991年10月 (NATURAL SCIENCE) Oct. 1991

两个不定方程的素数解

王 志 雄
(管理信息科学系)

摘要 本文利用二次同余方法，给出Pell方程解的素因子形式和方程有素数解的一个必要条件。并对一种特殊情况，给出Hall方程素数解的范围。

关键词 素数，素因子，同余式，方程

0 引言

Pell方程

$$x^2 - 2y^2 = -1 \tag{1}$$

和Hall方程

$$x^m = y^n + 2 (m, n > 1) \tag{2}$$

是否有无限多组素数解?这是两个很著名的未解决的问题[1]。设

$$x_n = [(1+\sqrt{2})^n + (1-\sqrt{2})^n]/2, \tag{3}$$

$$y_n = [(1+\sqrt{2})^n - (1-\sqrt{2})^n]/2\sqrt{2}, \tag{4}$$

熟知，方程(1)的全部正整数解为(x_{2n+1}, y_{2n+1})，$(n=0,1,2,\cdots)$。迄今为止，仅知，当$x, y < 10^{15}$时，方程(1)仅有三组素数解(x_3, y_3)，(x_5, y_5)和(x_{29}, y_{29})。而且，(x_{2n+1}, y_{2n+1})为素数解的一个必要条件是$(2n+1)$为素数[2]

关于方程(2)，除$x=3, y=5 (m=3, n=2)$之外，还没有找到其它的素数解。Nagell和曹珍富等人对一些特殊情况给出了一些结果。[3]本文将证明：

定理1 若素数$p \equiv 3 \pmod 4$，$p>3$，(x_p, y_p)是方程(1)的素数解，则$(2p-1)$和$(2p+1)$均非素数。

定理2 当素数$p \equiv 1 \pmod 4$时，x_p的素数因子必有形式$8hp+1$或$8hp+6p+1$；当素数$p \equiv 3 \pmod 4$时，x_p的素因子必有形式$8hp+1$或$8hp+2p+1$。

本文1990—04—13收到。

定理3 当素数 $p\equiv1(\mathrm{mod}4)$时，y_n 的素数因子必有形式$8hp+1$或$8hp+6p-1$；当素数 $p\equiv3(\mathrm{mod}4)$时，y_n 的素因子必有形式$8hp+1$或$8hp+2p-1$。

定理4 当 m 为偶数，n 为奇数时，方程(2)的素数解(x,y)中，必有 $y\equiv-1(\mathrm{mod}8)$。

1 定理1的证明

引理1 对一切素数 q 及整数 $j(1\leqslant j\leqslant q-1)$，恒有$\binom{q-1}{j}\equiv(-1)^j(\mathrm{mod}q)$。

证 因$(q-1)(q-2)\cdots(q-j)\equiv(-1)(-2)\cdots(-j)\equiv(-1)^j\cdot j!(\mathrm{mod}q)$，$(j!,q)=1$，故得。

引理2 若 $p\equiv3(\mathrm{mod}4)$，p 和$2p+1$都是素数，则 $x_p\equiv0(\mathrm{mod}2p+1)$。

证 由式(3)并利用引理1得

$$x_p^2=\sum_{i=1}^{p}{}'\binom{2p}{2i}2^{i-1}\equiv\sum_{i=1}^{p}{}'2^{i-1}\equiv2^p-1(\mathrm{mod}2p+1),$$

又因 $p\equiv3(\mathrm{mod}4)$，故$2p+1\equiv-1(\mathrm{mod}8)$，即2是 $\mathrm{mod}2p+1$的平方剩余，得$2^p\equiv1(\mathrm{mod}2p+1)$，从而 $x_p^2\equiv0(\mathrm{mod}2p+1)$。

同理可证

引理3 若 $p\equiv3(\mathrm{mod}4)$，p 和$2p-1$都是素数，则 $y_p\equiv0(\mathrm{mod}2p-1)$。

定理1的证明 因 $p>3$，$p\equiv3(\mathrm{mod}4)$，故 $p\geqslant7$，从而 $x_p>y_p>(1+\sqrt{2})^p/2\sqrt{2}>2p+1$。由引理2，若$2p+1$是素数，则 x_p 有真因子$2p+1$；由引理3，若$2p-1$是素数，则 y_p 有真因子$2p-1$。证得：若 x_p,y_p 都是素数，则$2p-1$和$2p+1$均非素数。

推论 当 $p=7,11,19,23,31,79,83,131,139,179,191,199\cdots$时，$(x_p,y_p)$不是方程(1)的素数解。

2 定理2和定理3的证明

引理4 当素数 $q\equiv\pm3\mathrm{mod}8$时，$y_{q+1}\equiv0(\mathrm{mod}q)$；当素数 $q\equiv\pm1(\mathrm{mod}8)$时，$y_{q-1}\equiv0(\mathrm{mod}q)$。

证明 见文[2]。

引理5 $y_{(m,n)}=(y_m,y_n)$。

证 由式(2)、(3)，当 $m>n$ 时，$y_m=x_ny_{m-n}+x_{m-n}y_n$，故$(y_m,y_n)=(x_ny_{m-n},y_n)$，又因 $x_n^2-2y_n^2=(-1)^n$，故$(x_n,y_n)=1$，从而，$(y_m,y_n)=(y_{m-n},y_n)$。由辗转相除法得证。

定理2的证明 设 q 是 x_p 的素因子，显然，x_p 为奇数，故 q 也为奇数。因$2y_p^2=x_p^2+1\equiv1(\mathrm{mod}q)$，即2是 $\mathrm{mod}q$ 的平方剩余，故 $q\equiv\pm1(\mathrm{mod}8)$，由引理4，$y_{q-1}\equiv0(\mathrm{mod}q)$。又因 $y_{2p}=2x_py_p\equiv0(\mathrm{mod}q)$，由引理5，$y_d\equiv0(\mathrm{mod}q)$，其中，$d=(2p,q-1)$。

显然，$y_1=1$，$y_2=2$均不能被 q 整除，$(x_p,y_p)=1$，故 y_p 也不能被 q 整除，从而，$d=2p$，即$2p|(q-1)$，设 $q=2kp+1$。当 $q\equiv1(\mathrm{mod}8)$时，q 必有形式$8hp+1$。当 $q\equiv-1(\mathrm{mod}8)$时，若 $p\equiv1(\mathrm{mod}4)$，则由$2kp+1\equiv q\equiv-1(\mathrm{mod}8)$，得 $k\equiv3(\mathrm{mod}4)$，故 q 必有形式$8hp+6p+1$，若 $p\equiv3(\mathrm{mod}4)$，则由$2kp+1\equiv-1(\mathrm{mod}q)$得 $k\equiv1(\mathrm{mod}4)$，故 q 必有形式$8hp+2p+1$。

定理3　同理可证。

3　定理4的证明

当 $m=2k$ 为偶数时，由方程(2)得

$$x^{2m} \equiv 2(\mathrm{mod}y),$$

即2是素数 y 的平方剩余，故

$$(2/y) = (-1)^{\frac{y^2-1}{8}} = 1,$$

从而

$$y^2 - 1 \equiv 0(\mathrm{mod}16).$$

得 $y \equiv \pm 1(\mathrm{mod}8)$，但 $x^{2m}-2 \equiv -1(\mathrm{mod}8)$，故 $y \equiv -1(\mathrm{mod}8)$，证毕。

参　考　文　献

〔1〕柯召、孙琦、群论，组合论和代数数论中的一些不定方程问题，数学的研究和评论，2(1983)，131—134.

〔2〕屈明华，关于丢番图方程 $p^2-2q^2=-1$，四川大学学报(自然科学版)，2(1986)，1—9.

〔3〕曹珍富，丢番图方程引论，哈尔滨工业大学出版社，(1989).

The Prime Solution of Two Indefinite Equation

Wang　Zhixiong

Department of Management Information Science)

Abstract　By making use of quadratic congruence method, the author gives the form of prime factor for solving pell's equation and a necessary condition for the prime solution of this equation. As a special case, the range of the prime solution for Hall's equation is given here as well.

Key words　prime number, prime divisor, congruence, equations