

关于一类广义 Ramanujan-Nagell 方程的正整数解

张正萍¹, 赵开明²

(1. 重庆科技学院数理学院, 重庆 401331)

(2. 重庆求精中学, 重庆 400015)

摘要: 本文研究了一类广义 Ramanujan-Nagell 方程有正整数解的条件. 利用二次域中的重要理论, 给出了一个典型的 Ramanujan-Nagell 方程的所有正整数解, 推广了文献 [1] 和 [2] 的结果.

关键词: 广义 Ramanujan-Nagell 方程; 正整数解; 二次域

MR(2010) 主题分类号: 11D45; 11D75

中图分类号: O156.7

文献标识码: A

文章编号: 0255-7797(2016)05-1077-06

1 引言

设 Z 和 N 分别表示全体整数和正整数组成的集合, p 是奇素数, D 是适合 $p \nmid D$ 的正整数. 此时, 方程

$$x^2 + D = p^n, \quad x, n \in N \quad (1.1)$$

是一类基本而重要的广义 Ramanujan-Nagell 方程. 多年来, 关于该类方程的整数解一直是指数 Diophantus 方程的一个引人关注的问题, 但主要是其解数 $N(D, p)$ 的上界估计, 乐茂华^[1] 证明了当 $(D, p) = (2, 3)$ 或 $(3s^2 + 1, 4s^2 + 1)$, 其中 s 是正整数时方程 (1.1) 恰有 2 组正整数解, 否则, 该方程至多有 1 组正整数解; 曹珍富^[2] 仅给出了方程 $x^2 + 2 = 3^n$ 仅有 $(1, 1)$ 、 $(5, 3)$ 两组正整数解.

作为代数数论中的重要组成部分, 二次域的有关类数、理想等相关性质和理想数唯一分解定理对研究该类方程的整数解有着重要作用. 对某些 $D > 0$, $Q(\sqrt{-D})$ 不是 Euclid 域, 若其类数 $h(Q(\sqrt{-D})) = 1$, 可以利用代数整数环中唯一分解定理的相关知识去研究方程的整数解问题; 若其类数 $h(Q(\sqrt{-D})) \neq 1$, 可以利用二次域中整数环上的理想唯一分解定理去研究方程的整数解问题. 为此, 先引入同余式、二次域的有关类数、理想及其相关性质和理想唯一分解定理.

定义 1.1^[3] 若 ε 和 ε^{-1} 都是代数整数, 则 ε 称为单位数.

定义 1.2^[4] 环 R 的非空子集 S 叫做 R 的理想, 是指满足下面条件: (1) 如果 $a, b \in S$, 则 $a \pm b \in S$; (2) 如果 $r \in R, a \in S$, 则 $ar, ra \in S$.

定义 1.3^[4] 由一个元素 $x \in R$ 生成的理想 (x) 叫做环 R 的主理想, 如果 R 是整环, 并且 R 中每个理想都是主理想 $(x) = xR$, 则 R 叫做主理想整环.

*收稿日期: 2014-10-08

接收日期: 2014-12-24

基金项目: 重庆市自然科学基金项目 (cstc2013jcyjA10049); 重庆科技学院本科教育教学改革研究项目 (201249).

作者简介: 张正萍 (1973-), 女, 四川泸州, 讲师, 研究方向: 数论.

定义 1.4 ^[5] 数域 K 的子集 I 叫做 K 的分式理想, 是指存在 $0 \neq \mu \in O_k$ (数域 K 的整数环), 使得 μI 为 O_k 的非零理想, 用 $I(K)$ 表示 K 的全体分式理想组成的集合, 且 $I(K)$ 构成群, 叫做数域 K 的分式理想群; 对于 $\alpha \in K$, 称 αO_k ($0 \neq \alpha \in O_k$) 为主分式理想, 而 $I(K)$ 中主分式理想的全体构成一个群, 叫做 K 的主分式理想群, 记作 $P(K)$; 商群 $C(K) = I(K)/P(K)$, 叫做 K 的 (分式) 理想类群, $C(K)$ 中的每一个元素叫做 K 的 (分式) 理想类.

定义 1.5 ^[5] 理想类群的阶 $h(K) = |C(K)|$ 叫做数域 K 的类数.

定义 1.6 ^[6] 设 $\tilde{F}$ 是一个代数整数环, $\alpha_1, \alpha_2, \dots, \alpha_s \in \tilde{F}$, 把集合

$$x_1\alpha_1 + x_2\alpha_2 + \dots + x_s\alpha_s, \quad x_1, x_2, \dots, x_s \in \tilde{F}$$

称为是由 $\alpha_1, \alpha_2, \dots, \alpha_s$ 生成的 $\tilde{F}$ 中的理想数.

定义 1.7 ^[6] 设 $\alpha, \beta \in M$, 若存在 ε 使 $\beta = \varepsilon \odot \alpha$, 则称 β 是 α 的相伴数, 记作 $\beta \sim \alpha$.

定理 1.1 ^[7] 若 $a \equiv b \pmod{m_i}$, 其中 $i = 1, 2, \dots, n$, 则 $a \equiv b \pmod{[m_1, m_2, \dots, m_n]}$.

引理 1.1 ^[6] $\alpha \in A_2$ (全体 Q 上的 2 次代数数组成的集合) 的充要条件是 $\alpha = r + s\sqrt{D}$, 其中 $r, s \in Q$, $s \neq 0$ 以及 $D \neq 0$ 是无平方因子的有理整数; $\alpha \in \widetilde{A_2}$ (全体 Q 上的 2 次代数整数组成的集合) 的充要条件是除以上所说的外还要满足 $2r \in Z$, $r^2 - Ds^2 \in Z$.

引理 1.2 ^[6] 设 D 满足引理 1.1 的条件, 及

$$\omega = \begin{cases} \sqrt{D}, & D \equiv 2, 3 \pmod{4}, \\ (-1 + \sqrt{D})/2, & D \equiv 1 \pmod{4}. \end{cases}$$

那么 α 是二次代数整数的充要条件是它可以表为

$$\alpha = m + n\omega, \quad m, n \in Z, \quad n \neq 0. \quad (1.2)$$

定理 1.2 ^[6] 当 $D \leq -1$ 时, 仅当 $D = -1, -3$ 时才有形如 (1.2) 的单位数. 仅当 $D = -1$ 时, 这种单位数是 $\pm i$, 当 $D = -3$ 时, 这种单位数是 $\pm(1 \pm \sqrt{3})/2$.

定理 1.3 ^[6] 主理想整环是唯一分解整环.

定理 1.4 ^[6] 设 M 是唯一分解环, 正整数 $k \geq 2$, 以及 $\alpha, \beta \in M$, $(\alpha, \beta) = \bar{1}$, 那么若 $\alpha\beta = \gamma^k$, $\gamma \in M$, 则有 $\alpha = \varepsilon_1\mu^k$, $\beta = \varepsilon_2\nu^k$, $\mu, \nu \in M$, 其中 $\varepsilon_1, \varepsilon_2$ 是 M 中的单位, 且 $\varepsilon_1\varepsilon_2 = \varepsilon^k$, ε 为单位.

2 $x^2 + 5 = p^n$ ($n \in N$) 有正整数解的必要条件

利用二次域中整数环上的理想唯一分解定理, 以下证明广义 Ramanujan-Nagell 方程

$$x^2 + 5 = p^n, \quad n \in N \quad (2.1)$$

有正整数解的必要条件.

结论 设 p 是奇素数, D 是适合 $p \nmid D$ 的正整数, 若方程 (2.1) 有解, 则一定存在 $a, b \in Z$ 使得 $p = a^2 + 5b^2$, 且 $b = \pm 1$.

证 情形 (1) 若 n 是偶数, 则由 (2.1) 式可得

$$\begin{cases} p^{\frac{n}{2}} \pm x = 5, \\ p^{\frac{n}{2}} \mp x = 1, \end{cases}$$

两式相加即有 $p^{\frac{n}{2}} = 3$, 由 p 是奇素数非平方, 显然方程 (2.1) 无解.

情形 (2) 若 n 是奇数, 在虚二次域中, 由定义 1.4 和定义 1.5 可得 $Q(\sqrt{-5})$ 的类数 $h(Q\sqrt{-5}) = 2$, 且有单位数 ± 1 , 其中 1 和 $(-1 + \sqrt{-5})/2$ 是一组整基^[6], 从而整环 $Q(\sqrt{-5})$ 的整数形如 $a + b\sqrt{-5}$ 的形式, 其中 $a, b \in \mathbb{Z}$. 由此可得方程 (2.1) 的理想分解为

$$(x + \sqrt{-5})(x - \sqrt{-5}) = p^n,$$

其中 $x + \sqrt{-5}$ 和 $x - \sqrt{-5}$ 均是 $Q(\sqrt{-5})$ 的理想数. 令

$$d = (x + \sqrt{-5}, x - \sqrt{-5}).$$

显然 $d|x$ 且 $d|\sqrt{-5}$. 因为 $\sqrt{-5}$ 是素数, 所以 $d = 1$ 或 $\sqrt{-5}$, 但 $d = \sqrt{-5}$ 不可能, 因为此时必有 $-5|x$, 而这样的 x 显然不是解, 于是 $d = 1$, 即理想数 $x + \sqrt{-5}$ 和 $x - \sqrt{-5}$ 互素, 于是

$$(x + \sqrt{-5})(x - \sqrt{-5}) = (a + b\sqrt{-5})^n(a - b\sqrt{-5})^n,$$

其中 $a^2 + 5b^2 = p$. 从而由定理 1.4 得

$$x + \sqrt{-5} = (a \pm b\sqrt{-5})^n = A^n,$$

其中 A 是 $Q\sqrt{-5}$ 中的理想数. 又因为 $(h(Q\sqrt{-5}), n) = 1$, 即存在有理数 u, v 使得

$$uh(\sqrt{-5}) + vn = 1,$$

于是有

$$A = (A^n)^v (A^{h(\sqrt{-5})})^u \sim (A^n)^v 1^u,$$

由 $A^n \sim 1$ 得 $A \sim 1^v$, $1^u \sim 1$, 即 A 是 $Q\sqrt{-5}$ 中的主理想. 又由 $Q\sqrt{-5}$ 中的单位数是 ± 1 , 则有

$$\begin{cases} x + \sqrt{-5} = \pm(a \pm b\sqrt{-5})^n, \\ x - \sqrt{-5} = \pm(a \mp b\sqrt{-5})^n, \end{cases}$$

进而有

$$(a + b\sqrt{-5})^n - (a - b\sqrt{-5})^n = \pm 2\sqrt{-5},$$

则

$$\binom{n}{1} a^{n-1} b - 5 \binom{n}{3} a^{n-3} b^3 + \cdots \pm 5^{\frac{n-1}{2}} \binom{n}{n} b^n = \pm 1.$$

即

$$b \left[\binom{n}{1} a^{n-1} - 5 \binom{n}{3} a^{n-3} b^2 + \cdots \pm 5^{\frac{n-1}{2}} \binom{n}{n} b^{n-1} \right] = \pm 1,$$

从而 $b = \pm 1$, 得证.

3 $x^2 + 5 = p^n$ ($n \in N$) 正整数解的证明

以下证明广义 Ramanujan-Nagell 方程

$$x^2 + 5 = 21^n, \quad n \in N \quad (3.1)$$

仅有正整数解 $(4, 1)$.

证 情形 (1) 若 n 是偶数, 则由 (3.1) 式可得

$$\begin{cases} 21^{\frac{n}{2}} \pm x = 5, \\ 21^{\frac{n}{2}} \mp x = 1, \end{cases}$$

两式相加即有 $21^{\frac{n}{2}} = 3$, 显然方程 (3.1) 无解.

情形 (2) 若 n 是奇数, 在虚二次域中, $Q(\sqrt{-5})$ 的类数 $h(Q\sqrt{-5}) = 2$, 整环 $Q(\sqrt{-5})$ 的整数形如 $a + b\sqrt{-5}$ 的形式. 由此可得方程 (3.1) 的理想分解为

$$(x + \sqrt{-5})(x - \sqrt{-5}) = 21^n,$$

其中 $x + \sqrt{-5}$ 和 $x - \sqrt{-5}$ 均是 $Q(\sqrt{-5})$ 的理想数. 由前面结论知 $x + \sqrt{-5}$ 和 $x - \sqrt{-5}$ 互素, 且

$$(x + \sqrt{-5})(x - \sqrt{-5}) = (4 + \sqrt{-5})^n (4 - \sqrt{-5})^n,$$

从而有

$$x + \sqrt{-5} = (4 \pm \sqrt{-5})^n = A^n,$$

其中 A 是 $Q\sqrt{-5}$ 中的理想数, 且是 $Q\sqrt{-5}$ 中的主理想. 又由 $Q\sqrt{-5}$ 中的单位数是 ± 1 , 则有

$$\begin{cases} x + \sqrt{-5} = \pm(4 \pm \sqrt{-5})^n, \\ x - \sqrt{-5} = \pm(4 \mp \sqrt{-5})^n. \end{cases}$$

进而有

$$(4 + \sqrt{-5})^n - (4 - \sqrt{-5})^n = \pm 2\sqrt{-5}. \quad (3.2)$$

若 (3.2) 式右边的负号成立的话, 设 $\alpha = 4 + \sqrt{-5}$, $\beta = 4 - \sqrt{-5}$, 则有 $\alpha^n - \beta^n = \pm(\alpha - \beta)$. 即 $\alpha^n + \alpha = \beta^n + \beta$, 亦即 $\alpha(\alpha^{n-1} + 1) = \beta(\beta^{n-1} + 1)$, 从而有 $\alpha | \beta^{n-1} + 1$. 又因为 $\alpha + \beta = 8$, 故 $\alpha | (8 - \alpha)^{n-1} + 1$. 则 $\alpha | 8^{n-1} + 1$, 两边同时取范数得 $21 | 8^{2n-2} + 2 \cdot 8^{n-1} + 1$, 显然不成立, 从而 (3.2) 式右边的负号不成立, 从而仅有

$$\binom{n}{1} 4^{n-1} - 5 \binom{n}{3} 4^{n-3} + \cdots \pm 5^{\frac{n-1}{2}} \binom{n}{n} = 1.$$

所以 $n \cdot 4^{n-1} \equiv 1 \pmod{5}$. 故 $n \cdot (-1)^{n-1} \equiv 1 \pmod{5}$. 令 $f(n) \equiv n \cdot (-1)^{n-1} \pmod{5}$, 由于其周期为 10. 即 $f(10n + k) \equiv f(k) \pmod{5}$. 故 $n \equiv 1, 4 \pmod{10}$, 又由条件 n 是奇

数知 $n \equiv 1 \pmod{2}$, 从而由定理 1.1 得 $n \equiv 1 \pmod{10}$. 当 $n = 1$ 时, 方程有正整数解 $(x, n) = (4, 1)$.

下证方程 (3.1) 的指数 n 不能有两个不同的解 n_1 和 n_2 , 满足 $n_1 - n_2 \equiv 0 \pmod{10}$. 否则, 可设

$$n_1 - n_2 = 5^l \cdot 2 \cdot h, \quad 5 \nmid h.$$

令 $\alpha = 4 + \sqrt{-5}$, 则

$$\alpha^{n_2} = \alpha^{n_1} \alpha^{n_2 - n_1} = \alpha^{n_1} (4 + \sqrt{-5})^{n_2 - n_1},$$

对于 5^{l+1} 的方幂实行数学归纳法可证

$$(4 + \sqrt{-5})^{n_2 - n_1} \equiv 4^{n_2 - n_1} + (n_2 - n_1) \cdot 4^{n_2 - n_1 - 1} \sqrt{-5} \pmod{5^{l+1}}. \quad (3.3)$$

又因

$$\alpha^{n_1} = (4 + \sqrt{-5})^{n_1} = 4^{n_1} + n_1 \cdot 4^{n_1 - 1} \sqrt{-5} \pmod{5}, \quad (3.4)$$

由 (3.3) 式和 (3.4) 式知

$$\begin{aligned} \alpha^{n_2} &\equiv \alpha^{n_1} \cdot 4^{n_2 - n_1} + \alpha^{n_1} (n_2 - n_1) 4^{n_2 - n_1 - 1} \sqrt{-5} \pmod{5^{l+1}} \\ &\equiv \alpha^{n_1} \cdot 4^{n_2 - n_1} + (4^{n_1} + n_1 \cdot 4^{n_1 - 1} \sqrt{-5} + 5\lambda) (n_2 - n_1) 4^{n_2 - n_1 - 1} \sqrt{-5} \pmod{5^{l+1}} \\ &\equiv \alpha^{n_1} \cdot 4^{n_2 - n_1} + (n_2 - n_1) 4^{n_1 - 1} \sqrt{-5} - 5 \cdot n_1 (n_2 - n_1) 4^{n_2 - 2} \\ &\quad + (n_2 - n_1) \cdot 4^{n_2 - n_1 - 1} \cdot 5\lambda \sqrt{-5} \pmod{5^{l+1}} \\ &\equiv \alpha^{n_1} \cdot 4^{n_2 - n_1} + (n_2 - n_1) 4^{n_2 - 1} \sqrt{-5} \pmod{5^{l+1}}, \end{aligned} \quad (3.5)$$

其中 λ 是 $Q(\sqrt{-5})$ 中的代数整数. 记 α 的共轭 $4 - \sqrt{-5} = \beta$, 将 β 去替换 (3.5) 式中的 α 得

$$\beta^{n_2} \equiv \beta^{n_1} \cdot 4^{n_2 - n_1} + (n_2 - n_1) 4^{n_2 - 1} \sqrt{-5} \pmod{5^{l+1}},$$

由于 (3.2) 式中的右端不能够取负号, 即 $\alpha^{n_1} - \beta^{n_1} = \alpha^{n_2} - \beta^{n_2}$. 故

$$\alpha^{n_2} - \beta^{n_2} = 4^{n_2 - n_1} (\alpha^{n_1} - \beta^{n_1}) + 2(n_2 - n_1) \cdot 4^{n_2 - 1} \sqrt{-5} \pmod{5^{l+1}}.$$

又因为 $n_2 - n_1 \equiv 0 \pmod{10}$, $n_1 - 1 \equiv 0 \pmod{2}$, 且 $4 \mid n_2 - n_1$. 即 $4^{n_2 - n_1} \equiv 1 \pmod{5}$. 所以有 $4^{n_2 - 1} \equiv \pm 1 \pmod{5}$. 故有

$$\alpha^{n_2} - \beta^{n_2} \equiv (\alpha^{n_1} - \beta^{n_1}) \pm 2 \cdot (n_2 - n_1) \sqrt{-5} \pmod{5^{l+1}}.$$

进而有

$$(n_2 - n_1) \sqrt{-5} \equiv 0 \pmod{5^{l+1}}.$$

即

$$(n_2 - n_1) \sqrt{-5} = 5^{l+1} (\alpha + \beta \sqrt{-5}).$$

亦即

$$(n_2 - n_1) \sqrt{-5} = 5^{l+1} \alpha + 5^{l+1} \beta \sqrt{-5}.$$

于是得

$$n_2 - n_1 = 5^{l+1}\beta.$$

即 $n_2 - n_1 \equiv 0 \pmod{5^{l+1}}$. 与 $5^l \nmid n_2 - n_1$ 矛盾. 故方程 (3.1) 的正整数解唯一, 仅有 $(x, n) = (4, 1)$, 证毕.

参 考 文 献

- [1] 乐茂华. 关于广义 Ramanujan-Nagell 方程 $x^2 + D = p^n$ 的解数 [J]. 常德师范学院学报 (自然科学版), 2002, 14(1): 1-2.
- [2] 曹珍富. 丢番图方程引论 [M]. 哈尔滨: 哈尔滨工业大学出版社, 2012.
- [3] 华罗庚. 数论导引 [M]. 北京: 科学出版社, 1979.
- [4] 张禾瑞. 近世代数基础 (修订本) [M]. 北京: 高等教育出版社, 2010.
- [5] 冯克勤. 代数数论 [M]. 北京: 科学出版社, 2000.
- [6] 潘承洞, 潘承彪. 代数数论 (第二版) [M]. 济南: 山东大学出版社, 2001.
- [7] 闵嗣鹤, 严士健. 初等数论 (第三版) [M]. 北京: 高等教育出版社, 2003.
- [8] 杨仕椿. 广义 Ramanujan-Nagell 方程 $x^2 + D^m = p^n$ 的解的注记 [J]. 数学学报, 2007, 50(4): 943-948.
- [9] 乐茂华. 关于广义 Ramanujan-Nagell 方程的一点注记 [J]. 数学杂志, 2007, 27(2): 219-221.
- [10] 杨继明. 广义 Ramanujan-Nagell 方程 $x^2 - D = 3^n$ 的解数 [J]. 数学学报, 2008, 51(2): 351-356.
- [11] 陈候炎. 关于广义 Ramanujan-Nagell 方程的一个猜想 [J]. 数学杂志, 2010, 50(4): 567-569.
- [12] 乐茂华, 胡永忠. 广义 Lebesgue-Ramanujan-Nagell 方程研究的新进展 [J]. 数学进展, 2012, 41(4): 385-393.

ON THE POSITIVE INTEGER SOLUTIONS OF A CLASS OF GENERALIZED RAMANUJAN-NAGELL EQUATION

ZHANG Zheng-ping¹, ZHAO Kai-ming²

(1.School of Mathematics and Physics, Chongqing University of Science and Technology,
Chongqing 401331, China)

(2.Chongqing Refinement School, Chongqing 400015, China)

Abstract: In this paper, we studied the necessary condition for existence of the positive integer solutions of a class of generalized Ramanujan-Nagell equation. On the base of it, we gave all the positive integer solutions of a typical Ramanujan-Nagell equations, and generalized some results of reference [1] and [2].

Keywords: generalized Ramanujan-Nagell equation; positive integer solution; quadratic fields

2010 MR Subject Classification: 11D45; 11D75