

Министерство образования и науки Российской Федерации
Российская академия наук
Московский государственный университет им. М. В. Ломоносова
Математический институт им. В. А. Стеклова РАН
Московский педагогический государственный университет
Тульский государственный педагогический университет им. Л. Н. Толстого
Тульский государственный университет
Чебышевский фонд

ЧЕБЫШЕВСКИЙ СБОРНИК

Научно-теоретический журнал
Труды VI Международной конференции
“Алгебра и теория чисел: современные проблемы и приложения”
Саратовский государственный университет
им. Н. Г. Чернышевского, сентябрь 2004 г.



ТОМ V

ВЫПУСК 4 (12)

Тула 2004

ББК 22.13

УДК 511

Ч 34

Печатается по решению VI Международной конференции
“Алгебра и теория чисел: современные проблемы и приложения”

Главный редактор В. Н. Чубариков

Ответственный секретарь С. А. Пихтильков

Редакционная коллегия:

В. А. Артамонов, Г. И. Архипов, В. Н. Безверхний, М. М. Глухов,
Е. С. Голод, Н. М. Добровольский (зам. гл. редактора), А. Р. Есяян,
А. М. Зубков, В. И. Иванов, В. Н. Латышев, Д. А. Митькин,
А. В. Михалев (зам. гл. редактора), Ю. В. Нестеренко, А. Л. Шмелькин

Чебышевский сборник. Т. V. Вып. 4(12): Тр. VI Междунар. конф. “Алгеб-
Ч 34 ра и теория чисел: современные проблемы и приложения”. — Тула: Изд-во
Тул. гос. пед. ун-та им. Л. Н. Толстого, 2004. — 190 с.

ISBN 5-87954-368-4

Журнал “Чебышевский сборник” выходит один раз в год в одном томе из
четырёх выпусках.

В журнале публикуются оригинальные и обзорные работы по всем разделам
современной математики, а также информационные материалы.

ББК 22.13

УДК 511

Выпуск осуществлен при финансовой поддержке РФФИ, грант № 04-01-10055.

ISBN 5-87954-368-4

© Тульский государственный
педагогический университет
им. Л. Н. Толстого, 2004

СОДЕРЖАНИЕ

Том 5 Выпуск 4

ПЛЕНАРНЫЕ ДОКЛАДЫ

- А. А. Карацуба. О приближениях $\pi(X)$ 5
- В. А. Исковских. О факторизации бирациональных отображений 21
- М. О. Авдеева. Оценка количества локальных минимумов целочисленных решеток 35
- Е. В. Аладова, А. В. Гришин, Е. А. Киреева. Т-пространства. История вопроса, приложения и последние результаты 39
- И. Н. Балаба. Радикалы в категории градуированных по полугруппе колец 58
- Н. В. Бударина. Деформации диофантовых систем для квадратичных форм шахматных решеток D_n 65
- М. М. Глухов. О применении колец целых алгебраических чисел к построению криптосхем с открытым ключом 75
- С. А. Гриценко. Оценка линейной тригонометрической суммы по простым числам, представимым заданной квадратичной формой 82
- А. В. Месянжин, Ю. А. Блинков. Об одном алгоритме решения системы полиномиальных уравнений 90
- А. В. Михалев, И. А. Пинчук. Автоморфизмы и дифференцирования конформных алгебр Ли и их центральные расширения 98
- А. В. Михалев, М. Х. Хоссейни. Жесткость Гельдера для колец матриц над телом 115
- Х. Хессами Пилеруд, Т. Хессами Пилеруд. О диофантовом уравнении $x^2 + 3 = py^{p-1}$ 118
- А. В. Шутов. Перенормировки вращений окружности 125
- R. Ivanauskaitė, A. Laurinćikas. The lognormal distribution law for zeta - functions of certain cusp forms 144
- Sergei Konyagin, Izabella Laba. Distance sets of well-distributed planar sets for polygonal norms 155

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 5 Выпуск 4 (2004)

УДК 511

О ДИОФАНТОВОМ УРАВНЕНИИ $x^2 + 3 = py^{p-1}$

Х. Хессами Пилеруд, Т. Хессами Пилеруд (Иран, г. Табриз)

Abstract

Let p be an odd prime such that $p-3$ is not a perfect square. In this paper we prove that the equation $x^2+3 = py^{p-1}$ has no solutions in rational numbers x, y . The proof depends on the unique factorization in the ring of algebraic integers of $\mathbb{Q}(\sqrt{-3})$ and on certain congruence arguments. Furthermore, the equation $x^2 + 3 = py^6$ in rationals x, y is also considered.

1 Введение

В настоящей заметке мы доказываем следующие утверждения.

ТЕОРЕМА 1.1. Пусть p нечетное простое, и $p-3$ не является полным квадратом. Тогда уравнение

$$x^2 + 3 = py^{p-1} \tag{1}$$

не имеет решений в рациональных числах x, y .

Если, кроме того, простое число $p \equiv 1 \pmod{4}$, то уравнение

$$x^2 + 3 = py^{\frac{p-1}{2}} \tag{2}$$

неразрешимо в рациональных числах x, y .

ТЕОРЕМА 1.2. Пусть p нечетное простое число. Если уравнение

$$x^2 + 3 = py^6 \tag{3}$$

разрешимо в рациональных числах x, y , то существуют такие целые положительные числа A, B , что $p = A^2 + 3B^2$, число B является кубическим вычетом по модулю p , и либо $B \equiv 0 \pmod{9}$, либо $B \equiv \pm 1 \pmod{9}$.

Заметим, что для простых p вида $p = a^2 + 3$, $a \in \mathbb{Z}$, уравнение (1) имеет по крайней мере тривиальные решения $(\pm a, \pm 1)$.

При $p = 5$ уравнение (2) сводится к $x^2 + 3 = 5y^2$, которое неразрешимо в рациональных числах согласно теореме Лежандра (см. [2, p.269]).

¹Работа выполнена при финансовой поддержке **Research Institute for Fundamental Sciences Tabriz, Iran**.

Уравнения, подобные (1), (2) были рассмотрены ранее в работах [1], [5], где была доказана неразрешимость уравнения вида $x^2 + 3 = y^n$ в положительных целых числах $x, y, n \geq 3$, а также найдены все положительные целочисленные решения (x, q, m, n) уравнения $x^2 = 4q^m - 4q^n + 1$ и, в частности, уравнения $x^2 + 3 = 4q^m$.

Заметим, что уравнения (1), (2), (3) представляют собой частный случай более общего уравнения $ax^2 + bx + c = dy^n$ при $b = 0, acd \neq 0$ и $n \geq 3$, которое имеет конечное число целочисленных решений (см. [8], [4], [6]), ограниченных эффективно вычислимой постоянной, обычно очень большой ([7, Теорема 12.2]).

Заметим также, что при $p \geq 11$ по теореме Фалтингса [3, с.367] уравнения (1), (2), рассмотренные как алгебраические кривые по крайней мере рода 2, имеют конечное число рациональных решений.

В дальнейшем нам понадобится следующая лемма.

ЛЕММА 1.1. Пусть $V, S \in \mathbb{Z}$, и $V(S^2 - V^2)$ не делится на 3, тогда $S \equiv 0 \pmod{3}$.

ДОКАЗАТЕЛЬСТВО. Действительно, если $(S, 3) = 1$, то $S^2 \equiv 1 \pmod{3}$. А так как любое целое число V либо делится на 3, либо $V^2 \equiv 1 \pmod{3}$, то получаем, что $V(S^2 - V^2) \equiv 0 \pmod{3}$, и лемма доказана.

2 Доказательство Теоремы 1.1

ДОКАЗАТЕЛЬСТВО. Пусть $x = X/Q, y = Y/T$ — решение (1) или (2), где X, Y, Q, T целые числа, $Q \geq 1, T \geq 1$ и

$$(X, Q) = (Y, T) = 1. \quad (4)$$

Определим

$$n = \begin{cases} 0, & \text{если } p \equiv 3 \pmod{4}, \\ 1, & \text{если } p \equiv 1 \pmod{4}. \end{cases}$$

Тогда уравнения (1), (2) перепишутся в виде

$$X^2 T^{\frac{p-1}{2n}} + 3Q^2 T^{\frac{p-1}{2n}} = pQ^2 Y^{\frac{p-1}{2n}} \quad (5)$$

или

$$X^2 T^{\frac{p-1}{2n}} = Q^2 \left(pY^{\frac{p-1}{2n}} - 3T^{\frac{p-1}{2n}} \right),$$

откуда, учитывая (4), получаем

$$T^{\frac{p-1}{2n}} \equiv 0 \pmod{Q^2}. \quad (6)$$

Аналогично из (4) и соотношения

$$pQ^2 Y^{\frac{p-1}{2n}} = T^{\frac{p-1}{2n}} (X^2 + 3Q^2)$$

находим

$$pQ^2 \equiv 0 \pmod{\Gamma^{\frac{p-1}{2^n}}}. \quad (7)$$

Так как $(p-1)/2^n$ четно, то из (6) и (7) следует, что $Q^2 = \Gamma^{\frac{p-1}{2^n}}$. Тогда (5) примет вид

$$X^2 + 3\Gamma^{\frac{p-1}{2^n}} = pY^{\frac{p-1}{2^n}}, \quad (8)$$

откуда следует, что

$$(X, p) = (\Gamma, p) = (X, \Gamma) = (Y, \Gamma) = (X, Y) = (X, 3) = 1. \quad (9)$$

Перепишем уравнение (8) в следующем виде

$$\left(X + i\sqrt{3}\Gamma^{\frac{p-1}{2^n+1}}\right) \left(X - i\sqrt{3}\Gamma^{\frac{p-1}{2^n+1}}\right) = pY^{\frac{p-1}{2^n}}. \quad (10)$$

Так как с учетом (9) целые алгебраические числа, стоящие в произведении левой части (10), взаимно просты в кольце $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$, которое является евклидовым, то получаем, что существуют такие целые рациональные числа a, b, S, V , $a \equiv b \pmod{2}$, $S \equiv V \pmod{2}$ и единица ε кольца $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$, что

$$X + i\sqrt{3}\Gamma^{\frac{p-1}{2^n+1}} = \varepsilon \cdot \frac{a + i\sqrt{3}b}{2} \cdot \left(\frac{S + i\sqrt{3}V}{2}\right)^{\frac{p-1}{2^n}}.$$

Так как существует всего 6 единиц $\pm 1, \pm\omega, \pm\omega^2$ кольца $\mathbb{Z}[\omega]$, где $\omega = e^{\frac{2\pi i}{3}} = (-1 + i\sqrt{3})/2$, то последнее соотношение может быть переписано в виде

$$X + i\sqrt{3}\Gamma^{\frac{p-1}{2^n+1}} = \frac{A + i\sqrt{3}B}{2} \cdot \left(\frac{S + i\sqrt{3}V}{2}\right)^{\frac{p-1}{2^n}}, \quad (11)$$

где A и B целые рациональные числа одинаковой четности и

$$p = \frac{A^2 + 3B^2}{4}. \quad (12)$$

Далее, умножая обе части (11) на $2^{\frac{p-1}{2^n}+1} \cdot V^{\frac{p-1}{2^n}}$, получим

$$\begin{aligned} & 2^{\frac{p-1}{2^n}+1} \left(X B^{\frac{p-1}{2^n}} + i\sqrt{3}\Gamma^{\frac{p-1}{2^n+1}} V^{\frac{p-1}{2^n}} \right) \\ &= (A + i\sqrt{3}B) \left(S B + A V - (A - i\sqrt{3}B)V \right)^{\frac{p-1}{2^n}} \\ &= (A + i\sqrt{3}B) \left(U^{\frac{p-1}{2^n}} + (A - i\sqrt{3}B)(K + i\sqrt{3}R) \right) \end{aligned}$$

где $U, K, R \in \mathbb{Z}$. Сравнивая мнимые части последнего равенства и учитывая, что $p \mid A^2 + 3B^2$, найдем

$$2^{\frac{p-1}{2^n}+1} \cdot \Gamma^{\frac{p-1}{2^n+1}} \cdot B^{\frac{p-1}{2^n}} \equiv B \cdot U^{\frac{p-1}{2^n}} \pmod{p}.$$

Возводя обе части полученного сравнения в степень 2^{n+1} , согласно малой теореме Ферма получим

$$2^{2^{n+1}} \equiv B^{2^{n+1}} \pmod{p}, \quad n \in \{0, 1\}.$$

Откуда

$$(B^2 - 4)(B^2 + 4) \equiv 0 \pmod{p}.$$

Если $B^2 - 4 \equiv 0 \pmod{p}$, то $B^2 = 4 + pk \geq 0$ для некоторого целого k . Тогда из (12) имеем $4p = A^2 + 3B^2 = A^2 + 12 + 3pk$ и следовательно, $0 \leq k \leq 1$.

Если $k = 0$, то $B^2 = 4$ и тогда

$$p = \frac{A^2 + 3B^2}{4} = \left(\frac{A}{2}\right)^2 + 3,$$

т.е. $p - 3$ является точным квадратом, что невозможно.

Если $k = 1$, то $B^2 = 4 + p$ и из (12) находим $4p = A^2 + 12 + 3p$ или $p = A^2 + 12 = B^2 - 4 = (B - 2)(B + 2) > 12$, что тоже невозможно, так как p простое число.

Если $B^2 + 4 \equiv 0 \pmod{p}$, то $B^2 = -4 + pk_1 \geq 0$ для некоторого $k_1 \in \mathbb{Z}$. Используя (12), получим $4p = A^2 + 3B^2 = A^2 - 12 + 3pk_1$ или $4p - 3pk_1 + 12 \geq 0$, откуда $4 - 3k_1 \geq -12/p \geq -12/5$ и следовательно, $2 \geq k_1 \geq 1$.

Если $k_1 = 2$, то $B^2 = -4 + 2p$ и тогда $4p = A^2 + 3B^2 = A^2 - 12 + 6p$ или $0 = A^2 - 12 + 2p \geq A^2 - 2$. Откуда следует, что либо $A = 0$, либо $A = 1$. Если $A = 0$, то $0 = -12 + 2p$ и получаем противоречие с тем, что p простое. Если $A = 1$, то $0 = -11 + 2p$, что невозможно. Таким образом остается единственно возможный случай $k_1 = 1$. Тогда $B^2 = -4 + p$, $4p = A^2 + 3B^2 = A^2 - 12 + 3p$ или $p = A^2 - 12 = B^2 + 4$. Последнее равенство равносильно следующему

$$A^2 - B^2 = (A - B)(A + B) = 16,$$

откуда получаем, что $B = \pm 3, A = \pm 5, n = 1, p = 13$. В этом случае из (11) находим

$$X + i\sqrt{3}T^3 = \frac{\pm 5 \pm 3i\sqrt{3}}{2} \left(\frac{S + i\sqrt{3}V}{2} \right)^6,$$

откуда следует, что

$$\begin{aligned} 128X + 128i\sqrt{3}T^3 &= (\pm 5 \pm 3i\sqrt{3})(S_1 + i\sqrt{3}V_1)^3 \\ &= (\pm 5 \pm 3i\sqrt{3})(S_1^3 - 9S_1V_1^2 + i(3S_1^2V_1 - 3V_1^3)\sqrt{3}), \end{aligned} \quad (13)$$

где $S_1 + i\sqrt{3}V_1 = (S + \sqrt{3}V)^2 = S^2 - 3V^2 + 2i\sqrt{3}SV$. Из равенства мнимых частей соотношения (13) находим

$$128T^3 = \pm 3(S_1^3 - 9S_1V_1^2) \pm 15(S_1^2V_1 - V_1^3).$$

Откуда следует, что $T = 3T_1$, $T_1 \in \mathbb{Z}$, и следовательно,

$$128 \cdot 9T_1^3 = \pm(S_1^3 - 9S_1V_1^2) \pm 5V_1(S_1^2 - V_1^2).$$

Применяя лемму 1.1, заключаем, что $S_1 \equiv 0 \pmod{3}$ и следовательно, $V_1 \equiv 0 \pmod{3}$. Сравнивая действительные части соотношения (13), получаем, что $X \equiv 0 \pmod{3}$, и таким образом, $3|(X, T)$, что противоречит взаимной простоте чисел X и T .

Таким образом, теорема 1.1 доказана.

3 Доказательство Теоремы 1.2

ДОКАЗАТЕЛЬСТВО. Пусть $(x, y) = (X/Q, Y/T)$ — рациональное решение (3), где X, Y, Q, T целые числа, $Q > 0, T > 0$, и

$$(X, Q) = (Y, T) = 1. \quad (14)$$

Тогда из (3) имеем

$$X^2T^6 + 3Q^2T^6 = pQ^2Y^6, \quad (15)$$

откуда следует, что

$$T^6 \equiv 0 \pmod{Q^2}, \quad pQ^2 \equiv 0 \pmod{T^6}.$$

Следовательно,

$$T^6 = Q^2$$

и уравнение (15) примет вид

$$X^2 + 3T^6 = pY^6. \quad (16)$$

Из (14) и (16) легко следует, что

$$(3, X) = (X, Y) = (T, X) = (X, p) = (T, p) = 1$$

и следовательно, целые алгебраические числа $X + i\sqrt{3}T^3$, $X - i\sqrt{3}T^3$ являются взаимно простыми в кольце $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$.

Рассуждая как и ранее, получим, что существуют такие целые рациональные числа A, B, S, U , что

$$X + i\sqrt{3}T^3 = \frac{A + i\sqrt{3}B}{2} \cdot \left(\frac{S + i\sqrt{3}U}{2}\right)^3, \quad (17)$$

$$p = \frac{A^2 + 3B^2}{4},$$

и

$$A \equiv B \pmod{2}, \quad S \equiv U \pmod{2}. \quad (18)$$

Умножая обе части (17) на $16B^3$, имеем

$$\begin{aligned} 16XB^3 + 16i\sqrt{3}T^3B^3 &= (A + i\sqrt{3}B)(SB + i\sqrt{3}UB)^3 \\ &= (A + i\sqrt{3}B)(SB + AU - (A - i\sqrt{3}B)U)^3. \end{aligned}$$

Сравнивая мнимые части и учитывая, что $(p, T) = (p, B) = (p, 2) = 1$, получим

$$16T^3B^3 \equiv B \cdot (SB + AU)^3 \pmod{p},$$

откуда следует, что $4B$ является кубическим вычетом по модулю p .

Кроме того, из (17) находим

$$16T^3 = A(3S^2U - 3U^3) + B(S^3 - 9SU^2), \quad (19)$$

$$16X = A(S^3 - 9SU^2) + 9B(U^3 - S^2U). \quad (20)$$

Заметим, что $(S, 3) = 1$. Действительно, в противном случае если $S \equiv 0 \pmod{3}$, то из (19), (20) следует, что $T \equiv 0 \pmod{3}$ и $X \equiv 0 \pmod{3}$, а это противоречит тому, что $(T, X) = 1$. Так как $(S, 3) = 1$, то по лемме 1.1 заключаем, что $U(S^2 - U^2)$ делится на 3. Тогда из (19) следует, что

$$-2T^3 \equiv BS^3 \pmod{9}.$$

Так как $(S, 3) = 1$, то из последнего сравнения получаем, что

$$\text{либо } B \equiv 0 \pmod{9}, \quad \text{либо } B \equiv \pm 2 \pmod{9}. \quad (21)$$

Для завершения доказательства осталось заметить, что A и B являются четными, т.е. $A = 2A_1, B = 2B_1, A_1, B_1 \in \mathbb{Z}$, и следовательно, $p = A_1^2 + 3B_1^2$; тогда равенство $\left(\frac{4B}{p}\right)_3 = 1$ равносильно $\left(\frac{B_1}{p}\right)_3 = 1$ и сравнения (21) примут вид

$$\text{либо } B_1 \equiv 0 \pmod{9}, \quad \text{либо } B_1 \equiv \pm 1 \pmod{9}.$$

Докажем, что числа A и B четные. Действительно, если согласно (18) S и U одновременно четные, т.е. $S = 2S_1, U = 2U_1$, то из (19), (20) имеем

$$2T^3 = 3AU_1(S_1^2 - U_1^2) + BS_1(S_1^2 - 9U_1^2), \quad (22)$$

$$2X = AS_1(S_1^2 - 9U_1^2) + 9BU_1(U_1^2 - S_1^2). \quad (23)$$

Если $U_1 + S_1$ нечетно, то из (22), (23) следует, что $2|B$ и $2|A$.

Если $U_1 + S_1$ четно, то из (22), (23) заключаем, что $2|T$ и $2|X$, а это противоречит тому, что $(X, T) = 1$.

Если S и U оба нечетные, то перепишем (19) в следующем виде

$$16T^3 = B(S + AU/B)^3 - 3AU^3 - 9BSU^2 - 3SA^2U^2/B - A^3U^3/B^2,$$

или

$$16B^2T^3 = (BS + AU)^3 - 3AB^2U^3 - 9B^3SU^2 - 3BA^2SU^2 - A^3U^3.$$

Заменим $BS + AU$ на Z в последнем соотношении, получим

$$Z^3 - 3(A^2 + 3B^2)ZU^2 + 2A(A^2 + 3B^2)U^3 = 16B^2T^3. \quad (24)$$

Учитывая, что $A^2 + 3B^2 = 4p$, заключаем, что Z четно, т.е. $Z = 2Z_1$, $Z_1 \in \mathbb{Z}$, и тогда (24) примет вид

$$Z_1^3 - 3pZ_1U^2 + ApU^3 = 2B^2T^2.$$

Так как p и U нечетны, отсюда легко следует, что A четно и, следовательно, согласно (18) B четно.

Это завершает доказательство теоремы 1.2.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] J.H.E. Cohn, The diophantine equation $x^2 + 3 = y^n$, Glasgow Math. J. 35 (1993), 203–206.
- [2] E. Grosswald, Topics from the theory of numbers, 2.ed., Birkhäuser Boston, 1984.
- [3] M. Hindry and J.H. Silverman, Diophantine geometry: an introduction, Springer-Verlag New York, 2000.
- [4] E. Landau and A. Ostrowski, On the diophantine equation $ay^2 + by + c = dx^n$, Proc. London Math. Soc., (2), 19 (1920), 276–280.
- [5] F. Luca, On the diophantine equation $x^2 = 4q^m - 4q^n + 1$, Proc. American Math. Soc., (5), 131 (2002), 1339–1345.
- [6] L.J. Mordell, Diophantine equations, Academic Press, London, 1969.
- [7] T.N. Shorey and Tijdeman, Exponential Diophantine equations, Cambridge University Press, 1986.
- [8] A. Thue, Über die Unlösbarkeit der Gleichung $ax^2 + bx + c = dy^n$ in grossen ganzen Zahlen x und y , Arch. Math. Naturv. Kristiania, Nr.16, 34 (1917).

Research Institute for Fundamental Sciences, Tabriz, Iran.

Mathematics Department, Shahrekord University, Shahrekord, P.O. Box 115.

Поступило 16.11.2004 г.