Записки научных
семинаров ПОМИ
Том 470, 2018 г.

Б. Б. Лурье, А. М. Порецкий

О КОНГРУЭНТНОСТИ УДВОЕННЫХ ПРОСТЫХ ЧИСЕЛ

§1. Введение

Настоящая работа является продолжением исследований [1].

Рациональное число q называется конгруэнтным, если существует прямоугольный треугольник с рациональными сторонами и площадью q. Сразу отметим, что конгруэнтность q равносильна конгруэнтности qw^2, что позволяет рассматривать только натуральные бесквадратные числа, что мы и будем делать в дальнейшем. Нетрудно показать, что для конгруэнтного числа q существует бесконечно много искомых треугольников с площадью q.

1.1. История задачи. Проблема конгруэнтности рациональных чисел восходит к Древней Греции, но окончательно была сформулирована, по всей видимости, арабскими математиками 10-го века [2]. Пьер Ферма использовал метод спуска для получения следующей теоремы.

Теорема 1.1 (Ферма)**.** *Единица не является конгруэнтным числом.*

Аналогично доказывается, что 2 и 3 не конгруэнтны. Минимальное конгруэнтное число – 5, стороны соответствующего треугольника – $\frac{3}{2}$, $\frac{20}{3}$ и $\frac{41}{6}$.

Особую роль играет сведение вопроса о конгруэнтности n к существованию рациональных точек на эллиптических кривых.

Теорема 1.2. *Натуральное число n конгруэнтно тогда и только тогда когда кривая*

$$nY^2 = X(X+1)(X-1)$$

содержит нетривиальную рациональную точку.

Иначе говоря, конгруэнтность n равносильна существованию арифметической прогрессии длины 3 с шагом n в квадратах натуральных чисел [2].

Ключевые слова: конгруэнтные числа, эллиптические кривые.

Исследуя эллиптические кривые с использованием аналитических методов, Туннел доказал [8] критерий определения конгруэнтности числа по модулю ослабленной гипотезы Бёрча–Суиннертон-Дайера (BSD):

Теорема 1.3 (Туннел)**.**

- *Пусть n нечетно. Положим*

$$N_1 := \sharp\{x^2 + 2y^2 + 8z^2 = n \mid z \equiv 0 \pmod 2\};$$

$$N_2 := \sharp\{x^2 + 2y^2 + 8z^2 = n \mid z \equiv 1 \pmod 2\}.$$

  Если $N_1 \neq N_2$, то n не конгруэнтно, в ином случае n конгруэнтно по модулю гипотезы BSD.
- *Пусть n четно, то есть $n = 2k$ (при этом k нечетно). Положим*

$$M_1 := \sharp\{x^2 + 4y^2 + 8z^2 = k \mid z \equiv 0 \pmod 2\};$$

$$M_2 := \sharp\{x^2 + 4y^2 + 8z^2 = k \mid z \equiv 1 \pmod 2\}.$$

  Если $M_1 \neq M_2$, то n не конгруэнтно, в ином случае n конгруэнтно по модулю гипотезы BSD.

Замечание 1.4. *До существования этого критерия было неясно как по числу определять конгруэнтное оно или нет. Например,* 157 *– конгруэнтное число, но первая пифагорова тройка содержит* 48*-значные числа, поэтому простой перебор пифагоровых троек не подходит. С другой стороны, проверка критерия Туннела осуществима за $O(n)$.*

Следствие 1.5. *Нечетные числа вида $8k + 5$ и $8k + 7$ являются конгруэнтными по модулю ослабленной гипотезы Бёрча–Суиннертон-Дайера.*

Действительно, для таких чисел число соответствующих представлений – нулевое.

В препринтах [6] и [7] Тиан показал, что конгруэнтное число n может иметь произвольное количество простых делителей.

1.2. Конгруэнтность простых и полупростых чисел. Для краткости обозначаем через p_1, p_3, p_5 и p_7 простые числа с соответствующим остатком по модулю 8.

Бёрч [3] и Хигнер [4] показали, что $2p_3$ и $2p_7$ – конгруэнтные числа. Монски нашел [5] общий метод доказательства *достаточных* условий конгруэнтности для чисел с малым числом простых делителей.

Теорема 1.6 (Монски)**.** *Следующие числа конгруэнтны*:

$$p_5,\ p_7,\ 2p_7,\ 2p_3,\ p_3p_7,\ 2p_3p_7,\ p_3p_5,\ 2p_3p_5; \tag{1}$$

$$p_1p_5,\ \textit{если}\ \left(\frac{p_1}{p_5}\right) = -1; \tag{2}$$

$$p_1p_7\ \textit{и}\ 2p_1p_7,\ \textit{если}\ \left(\frac{p_1}{p_7}\right) = -1; \tag{3}$$

$$2p_1p_3,\ \textit{если}\ \left(\frac{p_1}{p_3}\right) = -1. \tag{4}$$

Совсем недавно Лурье нашел элементарные *необходимые* условия конгруэнтности p_1 в терминах квадратичных вычетов. Согласно статье [1]:

Теорема 1.7. *Для того чтобы p_1 было конгруэнтным необходимо чтобы $\alpha \pm 1$ было квадратичным вычетом по модулю p_1, где $\alpha^2 \equiv -1 \pmod{p_1}$.*

Мы переносим использованные методы на удвоенные простые числа и доказываем следующую теорему.

§2. Основная теорема

Теорема 2.1. *Если число $2p_1$ конгруэнтно, то $p_1 \equiv 1 \pmod{16}$. Число $2p_5$ не может быть конгруэнтным.*

Воспользуемся вспомогательной теоремой из статьи [1].

Теорема 2.2. *Число n конгруэнтно тогда и только тогда, когда уравнение*

$$ab(a+b)(a-b) = nc^2 \tag{5}$$

разрешимо в натуральных числах. При этом числа a и b можно считать взаимно простыми числами разной четности.

Нас интересуют случаи $n = 2p_1$ и $n = 2p_5$. Тогда, поскольку все множители в левой части уравнения (5) взаимно просты, каждый из них является полным квадратом, возможно, домноженным на 2 или p. Таким образом вопрос сводится к исследованию разрешимости следующих восьми систем:

$$\begin{cases} 2px^2+y^2=z^2 \\ 2px^2-y^2=t^2 \end{cases}\ (\text{s1}) \qquad \begin{cases} px^2+2y^2=z^2 \\ px^2-2y^2=t^2 \end{cases}\ (\text{s2}) \qquad \begin{cases} 2x^2+py^2=z^2 \\ 2x^2-py^2=t^2 \end{cases}\ (\text{s3}) \qquad \begin{cases} x^2+2py^2=z^2 \\ x^2-2py^2=t^2 \end{cases}\ (\text{s4})$$

$$\begin{cases}2x^2+y^2=pz^2\\2x^2-y^2=t^2\end{cases}\quad(\text{s5})\qquad \begin{cases}x^2+2y^2=pz^2\\x^2-2y^2=t^2\end{cases}\quad(\text{s6})$$

$$\begin{cases}2x^2+y^2=z^2\\2x^2-y^2=pt^2\end{cases}\quad(\text{s7})\qquad \begin{cases}x^2+2y^2=z^2\\x^2-2y^2=pt^2\end{cases}\quad(\text{s8})$$

В правой части уравнений двойка не появляется, так как a и b разной четности.

Конгруэнтность n равносильна разрешимости хотя бы одной из вышеперечисленных систем. Основную трудность представляют системы (s2), (s6) и (s8), остальные по очевидным причинам никогда не имеют решений. Покажем это.

2.1. Нереализуемые случаи.

(s1):

$$\begin{cases}2px^2+y^2=z^2\\2px^2-y^2=t^2.\end{cases}$$

Так как $a=2px^2$ и $b=y^2$ разной четности, то и z^2, и t^2 нечетны, а тогда $z^2+t^2\equiv 2 \pmod 4$. Если же сложить равенства, то левая часть будет равна $4px^2$, что кратно 4. Противоречие.

(s3):

$$\begin{cases}2x^2+py^2=z^2\\2x^2-py^2=t^2.\end{cases}$$

аналогично (s1).

(s4):

$$\begin{cases}x^2+2py^2=z^2\\x^2-2py^2=t^2.\end{cases}$$

по теореме 2 из [1] допускает спуск.

(s5):

$$\begin{cases}2x^2+y^2=pz^2\\2x^2-y^2=t^2.\end{cases}$$

Так как $a=2x^2$ и $b=y^2$ разной четности, то y, z и t нечетны. Посмотрим теперь на систему по модулю 8. Из нижнего уравнения заключаем, что x тоже нечетно, а тогда из верхнего выходит, что $p\equiv 3 \pmod 8$.

(s7):

$$\begin{cases} 2x^2 + y^2 = z^2 \\ 2x^2 - y^2 = pt^2. \end{cases}$$

Из верхнего уравнения по модулю 8 получаем, что x четно, а тогда из нижнего следует, что $p \equiv 7 \pmod 8$.

Теперь перейдем к более сложным случаям.

2.2. Первая разрешимая система. Рассмотрим систему (s2):

$$\begin{cases} px^2 + 2y^2 = z^2 \\ px^2 - 2y^2 = t^2. \end{cases}$$

Вычтем из верхнего уравнения нижнее. Получим

$$z^2 = t^2 + (2y)^2.$$

Параметризуем эту пифагорову тройку:

$$z = u^2 + v^2, \quad t = u^2 - v^2, \quad y = uv,$$

где $(u, v) = 1$ и $u \not\equiv v \pmod 2$. Получаем, что

$$px^2 = u^4 + v^4.$$

Нам понадобится следующая

Лемма 2.3. *Пусть a и b – взаимно простые целые числа разной четности. Тогда если $d \mid N = a^4 + b^4$, то $d \equiv 1 \pmod 8$.*

Доказательство. Достаточно доказать лемму для простых делителей.

Легко видеть, что если $p \mid N$, то p имеет вид $4k + 1$. Действительно, если $p \equiv 3 \pmod 4$, то p является простым в $\mathbb{Z}[i]$ и делит там же либо $a^2 + b^2 i$, либо $a^2 - b^2 i$, в обоих случаях выходит, что и a, и b кратны p, что противоречит их взаимной простоте.

Теперь рассмотрим простой делитель $p = 4k + 1$. По малой теореме Ферма для целого A при $(A, p) = 1$ выполняется сравнение

$$A^{p-1} \equiv 1 \pmod p.$$

Тогда, если $A \overset{p}{\equiv} a^4$, очевидно, что $A^{\frac{p-1}{4}} \overset{p}{\equiv} 1$. Если теперь дополнительно обозначить $B = b^4$, то мы увидим, что условия приняли вид

$$\begin{cases} A \equiv -B \pmod p, \\ A^{\frac{p-1}{4}} \equiv 1 \pmod p, \\ B^{\frac{p-1}{4}} \equiv 1 \pmod p. \end{cases}$$

Пусть $p \equiv 5 \pmod 8$, т. е. $p = 8l + 5 = 4(2l + 1) + 1$, тогда

$$B^{\frac{p-1}{4}} \equiv (-A)^{\frac{p-1}{4}} \equiv (-A)^{2l+1} \equiv -(A^{2l+1}) \equiv -(A^{\frac{p-1}{4}}) \pmod p,$$

то есть два последних сравнения не могут выполняться одновременно. Отсюда получаем требуемое: $p \equiv 1 \pmod 8$. □

Теперь осталось отметить, что по лемме $x \equiv 1 \pmod 8$, поэтому $x^2 \equiv 1 \pmod{16}$, и $a^4 + b^4 \equiv 1 \pmod{16}$, так как a и b разной четности. Тогда получается, что и $p \equiv 1 \pmod{16}$.

2.3. Вторая разрешимая система. Перейдем к системе (s6):

$$\begin{cases} x^2 + 2y^2 = pz^2 \\ x^2 - 2y^2 = t^2. \end{cases}$$

Преобразуя второе уравнение, получаем $(x + t)(x - t) = 2y^2 = 8y_1^2$, поскольку y делится на 2. Таким образом, для некоторых натуральных u, v имеем

$$\begin{cases} x + t = 2u^2 \\ x - t = 4v^2 \end{cases}$$

(при необходимости поменяв знак t). То есть

$$\begin{cases} x = u^2 + 2v^2 \\ y = 2uv. \end{cases}$$

Подставляя в исходное уравнение $x^2+2y^2 = pz^2$, получаем $u^4+4v^4+12u^2v^2 = pz^2$. Пусть q – произвольный простой делитель pz^2. Можно считать, что u и v не делятся на q. Тогда имеем

$$X^4 + 4 + 12X^2 \equiv 0 \pmod q, \tag{6}$$

где $X = u/v \pmod q$. Выделяя полный квадрат, имеем

$$(X^2 + 6)^2 - 32 \equiv 0 \pmod q. \tag{7}$$

Следовательно, 2 является квадратичным вычетом по модулю q. А значит, p и все простые делители z имеют вид $\pm 1 \pmod 8$. Тогда $z^2 \equiv 1 \pmod{16}$. Поскольку можно считать, что u нечетно, легко видеть, что $u^4 + 4v^4 + 12u^2v^2 \equiv 1 \pmod{16}$. А значит, и $p \equiv 1 \pmod{16}$.

Таким образом, исходная система не имеет решений при $p = p_5$ и может иметь решения только при $p_1 \equiv 1 \pmod{16}$.

2.4. Третья разрешимая система. Рассмотрим систему (s8):

$$\begin{cases} x^2 + 2y^2 = z^2 \\ x^2 - 2y^2 = pt^2. \end{cases}$$

Действуя полностью аналогично предыдущему случаю, получаем:

$$\begin{cases} z + x = 2u^2 \\ z - x = 4v^2 \end{cases}$$

(при необходимости поменяв знак x). То есть

$$\begin{cases} x = u^2 - 2v^2 \\ y = 2uv. \end{cases}$$

Подставляя в исходное уравнение, получаем

$$u^4 + 4v^4 - 12u^2v^2 = pt^2. \tag{8}$$

Очевидно, можно считать, что u и v не делятся на p. Тогда имеем

$$X^4 + 4 - 12X^2 \equiv 0 \pmod p, \tag{9}$$

где $X \equiv u/v \pmod p$. Выделяя полный квадрат, имеем

$$(X^2 - 6)^2 - 32 \equiv 0 \pmod p. \tag{10}$$

Необходимо, чтобы 2 была вычетом по модулю p. Это неверно для p_5, что завершает доказательство теоремы в этом случае.

Продолжим рассмотрение в случае p_1. Аналогично случаю системы (s6) имеем $t^2 \equiv 1 \pmod{16}$ (помним, что u можно считать нечетным). Тогда при четных v левая часть (8) – это 1 по модулю 16 и снова выходит $p \equiv 1 \pmod{16}$.

При нечетных v получается $p \equiv 9 \pmod{16}$; рассмотрим разложение левой части (8) на множители:

$$u^4 + 4v^4 - 12u^2v^2 = (u^2 + 4uv + 2v^2)(u^2 - 4uv + 2v^2). \tag{11}$$

В силу (8) левая часть (11) положительна. Но сумма сомножителей в правой части также положительна. Поэтому сомножители в правой части (11) положительны. При нечетных u и v они взаимно просты, то есть имеют вид pA^2 и B^2. Но обе скобки сравнимы с 7 по модулю 8, поэтому никакая из них не соответствует B^2. Противоречие, то есть $p \not\equiv 9 \pmod{16}$, что завершает доказательство теоремы.

2.5. Заключительные замечания. Отметим, что найденное условие заведомо не является достаточным, так как число $n = 2 \cdot 241$ по теореме Туннела не является конгруэнтным.

Напомним, что конгруэнтность $2p$ равносильна существованию нетривиальной рациональной точки на эллиптической кривой $2pY^2 = X(X-1)(X+1)$. Поскольку все системы, кроме (s2), (s6) и (s8), никогда не имеют решений, получаем, что разрешимость соответствующих систем имеет место при делимости на p числителей X, $X+1$ и $X-1$, соответственно. Значит, как и в случае $n = p$, разрешимость любых двух из этих систем влечет разрешимость третьей, поскольку сумма точек, соответствующих решениям систем, будет соответствовать решению третьей системы. При этом неясно, влечет ли разрешимость одной системы разрешимость двух других.

Благодарности. Авторы благодарят Данилу Черкашина за помощь в верстке статьи и указание на препринты [6, 7].

Список литературы

1. Б. Б. Лурье, *О конгруэнтности простых чисел.* — Зап. научн. семин. ПОМИ, **455** (2017), 84–90.
2. Н. Коблиц, *Введение в эллиптические кривые и модулярные формы.* — Мир, (1988).
3. B. J. Birch, *Diophantine analysis and modular functions.* — Conf. Algebraic Geometry, Tata Institute, Bombay, (1968).
4. K. Heegner, *Diophantische Analysis und Modulfunktionen.* — Math. Zeitschrift, **56**, No. 3 (1952), 227–253.
5. P. Monsky, *Mock Heegner points and congruent numbers.* — Math. Zeitschrift, **204**, No. 1 (1990), 45–67.
6. Ye Tian, *Congruent numbers and Heegner points.* — `arXiv preprint arXiv:1210.8231` (2012).
7. Ye Tian, Yuan Xinyi, and Zhang Shouwu, *Genus periods, genus points and congruent number problem.* — `arXiv preprint arXiv:1411.4728` (2014).
8. Tunnell, B. Jerrold, *A classical Diophantine problem and modular forms of weight* 3/2. — Invent. Math., **72**, No. 2 (1983), 323–334.

Lurj'e B. B., Poretsky A. M. On the congruence for twice the primes.

The article proposes an elementary necessary condition for doubles prime integers to be congruent.

Поступило 16 апреля 2018 г.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
Фонтанка 27, 191023,
С.-Петербург, Россия
E-mail: lurje@pdmi.ras.ru

С.-Петербургский
государственный университет
Университетский пр. 28, Петродворец
198504, Санкт-Петербург, Россия
E-mail: pam-online@yandex.ru