Общероссийский математический портал

Э. Бомбьери, У. Заннье, О числе рациональных точек на некоторых эллиптических кривых, *Изв. РАН. Сер. матем.*, 2004, том 68, выпуск 3, 5–14

DOI: <https://doi.org/10.4213/im483>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 107.22.136.117

26 апреля 2023 г., 12:35:42

УДК 512.752

Э. Бомбьери, У. Заннье

О числе рациональных точек на некоторых эллиптических кривых

Пусть E – эллиптическая кривая, определенная над полем рациональных чисел с рациональным 2-кручением. Доказана равномерная оценка для числа рациональных чисел над E высоты не более B вида $\#\{P \in E(\mathbb{Q}) : H(P) \leq B\} \leq c(\varepsilon) (\max(H(E), B))^\varepsilon$, справедливая для любого фиксированного $\varepsilon > 0$ и некоторой эффективной константы $c(\varepsilon)$. Приведено приложение этого результата к подсчету четверок (p_1, p_2, p_3, p_4) различных простых чисел, не превосходящих X и связанных соотношениями $p_i^2 \Delta_{jk} - p_j^2 \Delta_{ik} + p_k^2 \Delta_{ij} = 0$ для всех $1 \leq i < j < k \leq 4$, где Δ_{ij} – заданные целые числа. Эти оценки прилагаются С. В. Конягиным (см. работу [3], опубликованную одновременно с настоящей статьей) к проблеме большого решета с квадратами.

Библиография: 7 наименований.

1. Введение и основные результаты. Пусть K – некоторое числовое поле и C – проективная кривая рода 1 над полем K в проективном пространстве $\mathbb{P}^N$. Часто в теории чисел возникает задача оценки числа рациональных точек над полем K на кривой C , высота которых как точек из $\mathbb{P}^N$ не превосходит заданной величины. С этой задачей связана и проблема получения хороших оценок сверху для числа целых точек из O_K на аффинной кривой C над полем K в некотором аффинном пространстве $\mathbb{A}^N$.

Как обычно, через $H(\cdot)$ обозначим абсолютную высоту Вейля точки P из стандартного проективного или аффинного пространства (в зависимости от рассматриваемого случая), а через $h(P) := \log H(P)$ – обычную логарифмическую¹ абсолютную высоту Вейля. *Высотой многочлена f* будем называть проективную высоту вектора его коэффициентов.

Пусть кривая C задается теоретико-множественным способом как множество решений системы $\mathcal{F}$ полиномиальных уравнений вида $f = 0$. Тогда *высотой кривой C* , соответствующей ее представлению $\mathcal{F}$, назовем величину

$$H(C; \mathcal{F}) := \max_{f \in \mathcal{F}} H(f).$$

В частном случае, когда аффинная кривая C в пространстве $\mathbb{A}^2$ задается единственным уравнением $f(x, y) = 0$, будем записывать $H(C)$ вместо $H(C; f)$. Аналогично будем записывать $H(C)$ вместо $H(C; F)$, если C – проективная

¹Прим. ред. В настоящей работе $\log a$ обозначает натуральный логарифм величины a .

кривая в пространстве $\mathbb{P}^2$, определенная единственным однородным уравнением $F(X, Y, Z) = 0$.

В настоящей статье рассмотрим эллиптические кривые лишь над полем рациональных чисел $\mathbb{Q}$, а в заключение будет сделано несколько дополнительных замечаний, касающихся эллиптических кривых над произвольным числовым полем.

Пусть $E/\mathbb{Q}$ – эллиптическая кривая в форме Вейерштрасса:

$$y^2 = x^3 + a_1x^2 + a_2x + a_3 = (x - e_1)(x - e_2)(x - e_3), \quad (1)$$

и, значит, $H(E)$ – аффинная высота вектора коэффициентов $(1, a_1, a_2, a_3)$. Тогда имеет место очевидное неравенство

$$H(E) \leq \max_i H^3(a_i). \quad (2)$$

Существует много примеров, когда необходимы оценки чисел лежащих на эллиптической кривой целых или рациональных точек высоты, не превосходящей заданного параметра B . Для большинства приложений достаточно знания оценок порядка $H^\varepsilon(E)$ или B^ε . Как предполагают многие специалисты, справедливы следующие две гипотезы.

ГИПОТЕЗА I. Пусть $\varepsilon > 0$ и $E/\mathbb{Q}$ – эллиптическая кривая в форме Вейерштрасса (1). Тогда для каждого числа $B \geq 1$ справедливо неравенство

$$\#\{P \in E(\mathbb{Q}) : H(P) \leq B\} \leq c(\varepsilon) (\max(H(E), B))^\varepsilon, \quad (3)$$

где положительная постоянная $c(\varepsilon)$ зависит только от ε .

ГИПОТЕЗА II. Пусть $E/\mathbb{Q}$ – эллиптическая кривая в форме Вейерштрасса (1). Тогда для каждого $\varepsilon > 0$ справедливо неравенство

$$\#\{P \in E(\mathbb{Z})\} \leq c'(\varepsilon) H^\varepsilon(E), \quad (4)$$

где положительная постоянная $c'(\varepsilon)$ зависит только от ε .

Далее, положим

$$h(E) = \log H(E), \quad r := \text{rank}_{\mathbb{Q}} E(\mathbb{Q}).$$

Покажем справедливость гипотезы I в частном случае, который используется в некоторых приложениях (см., например, [3]). Обозначим через $G[m]$ подгруппу m -крючения абелевой группы G .

ТЕОРЕМА 1. Пусть $E/\mathbb{Q}$ – эллиптическая кривая в форме Вейерштрасса (1), причем $E[2] \subset E(\mathbb{Q})$, т. е. $e_1, e_2, e_3 \in \mathbb{Q}$. Тогда имеет место гипотеза I.

Более точно, пусть $M := \max(3, h(E), \log B)$. Тогда справедливо неравенство

$$\#\{P \in E(\mathbb{Q}) : H(P) \leq B\} \leq \exp\left(C \frac{M}{\sqrt{\log M}}\right),$$

где C – вычислимая абсолютная положительная постоянная.

Для приложений, приведенных в [3], мы в явном виде получим

СЛЕДСТВИЕ. Для любых $X \geq 3$ и любых ненулевых целых чисел Δ_{ij} , $1 \leq i < j \leq 4$, количество четверок (p_1, p_2, p_3, p_4) простых чисел, удовлетворяющих условиям $p_1 < p_2 < p_3 < p_4 \leq X$ и $p_i^2 \Delta_{jk} - p_j^2 \Delta_{ik} + p_k^2 \Delta_{ij} = 0$ для всех $1 \leq i < j < k \leq 4$, не превосходит $\exp(C \log X / \sqrt{\log \log X})$, где $C > 0$ – эффективная абсолютная константа.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. В настоящей работе через $c_1, \dots, c_{14}$ будем обозначать вычислимые абсолютные положительные постоянные, а также для краткости будем обозначать $R := \sqrt{\log B}$.

Как мы увидим далее, будет удобно использовать высоту Нерона–Тейта, определяемую соотношением

$$\hat{h}(P) = \lim_{m \rightarrow \infty} 4^{-m} h(2^m P),$$

где $2^m P$ обозначает умножение P на 2^m в соответствии с групповым законом на кривой E . Х. Циммер [7] получил явные оценки разности двух весов для кривых в форме Вейерштрасса $Y^2 = 4X^3 - g_2X - g_3$. Несложное обобщение результата Циммера для кривых вида (1) позволяет для рассматриваемой кривой E и всякой точки $P \in E(\mathbb{Q})$ получить неравенство

$$|h(P) - \hat{h}(P)| \leq c_1 h(E) + c_1.$$

Из этой оценки следует, что для доказательства теоремы можно предполагать, что $B \geq H(E) \geq e^3$, и достаточно получить ту же самую оценку для величины

$$N(B) := \#\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq \log B\}.$$

Предположение $H(E) \geq e^3$ сделано лишь для удобства обозначений, чтобы обеспечить положительную оценку снизу $\log h(E) \geq \log 3 > 1$.

Как обычно, $\mathbb{R}^r = \mathbb{R} \otimes E(\mathbb{Q})$ – действительное векторное пространство с евклидовой нормой $|\mathbf{x}|$, определенной равенством $|\mathbf{x}| = \hat{h}^{1/2}(P)$, если $\mathbf{x}$ – класс точки $P \in E(\mathbb{Q})$ по модулю кручения, и продолженной по непрерывности и линейности на все пространство $\mathbb{R}^r$. Образом факторгруппы $E(\mathbb{Q})/\text{tors}$ в этом евклидовом пространстве является решетка Λ ранга r . Следовательно, число точек $P \in E(\mathbb{Q})$, для которых $\hat{h}(P) \leq \log B$, равно произведению количества узлов решетки Λ в шаре радиуса $R = \sqrt{\log B}$ с центром в начале координат пространства $\mathbb{R}^r$ на число точек конечного порядка из $E(\mathbb{Q})$, составляющих ядро гомоморфизма из группы $E(\mathbb{Q})$ в пространство $\mathbb{R} \otimes E(\mathbb{Q})$.

Сначала, следуя [6, гл. VIII, предложение 8.7], найдем квазимиимальную модель Вейерштрасса E' кривой E над $\mathbb{Z}$, а именно модель, являющуюся минимальной для всех простых чисел, за исключением, быть может, чисел 2 и 3. Искомая кривая задается уравнением Вейерштрасса $Y^2 = X^3 + a'_2X + a'_3$ с целыми коэффициентами a'_2, a'_3 , которое получается из уравнения (1) в результате подходящего рационального сдвига по X и последующей замены $X \mapsto u^2X$, $Y \mapsto u^3Y$,

где $u \in \mathbb{Q}^*$. Заметим, что переход к этой модели не изменяет ни ранг, ни высоту Нерона–Тейта в том смысле, что если $\varphi: E \rightarrow E'$ – соответствующий гомоморфизм над $\mathbb{Q}$, то $\hat{h}(P) = \hat{h}(\varphi(P))$. Более того, справедливо также неравенство $h(E') \leq c_2 h(E) + c_2$. Это означает, что при доказательстве теоремы можно далее предполагать квазимиимальность модели E .

Итак, пусть кривая E задана формулой

$$y^2 = x^3 + a_2x + a_3 = (x - e_1)(x - e_2)(x - e_3)$$

с целыми коэффициентами, целочисленными корнями e_i и дискриминантом

$$\Delta := -16(4a_2^3 + 27a_3^2) = 16(e_1 - e_2)^2(e_2 - e_3)^2(e_1 - e_3)^2.$$

Минимальный дискриминант $\mathcal{D}$ кривой E делит Δ и с точностью до множителя вида $2^a 3^b$ совпадает с Δ , так что

$$\omega(\mathcal{D}) \leq \omega(\Delta) \leq 2 + \omega(\mathcal{D}), \quad (5)$$

где $\omega(n)$ – количество различных простых делителей целого числа n .

Поскольку нам потребуется оценка ранга r группы $E(\mathbb{Q})$, докажем следующий результат.

ПРЕДЛОЖЕНИЕ 1. Пусть E/K – эллиптическая кривая над числовым полем K , $m \geq 2$ – целое число, Cl_K – группа классов поля K , и пусть $S = \{v \in M_K^0 : E \text{ имеет плотную редукцию по модулю } v\} \cup \{v \in M_K^0 : v(m) \neq 0\} \cup M_K^\infty$. Предположим, что кривая E имеет рациональное m -кручение такое, что $E[m] \subset E(K)$. Тогда справедливо неравенство

$$\text{rank}_{\mathbb{Z}/m\mathbb{Z}} E(K)/mE(K) \leq 2\#S + 2\text{rank}_{\mathbb{Z}/m\mathbb{Z}} \text{Cl}_K[m].$$

ДОКАЗАТЕЛЬСТВО. Это предложение содержится в качестве упражнения в книге [6, гл. VIII, упр. 8.1], поэтому мы лишь наметим схему доказательства. Как показал Э. Ландау в 1907 г., примарные идеалы в заданном классе идеалов имеют положительную плотность, одну и ту же для каждого класса, и, значит, каждый класс идеалов в Cl_K можно выразить через примарные идеалы бесконечно многими способами (см., например, [5, гл. VII, §2, утверждение 7.10, следствие 4]). Следовательно, можно избавиться от $\text{Cl}_K[m]$, увеличив S добавлением $\text{rank}_{\mathbb{Z}/m\mathbb{Z}} \text{Cl}_K[m]$ элементов, а затем применить теорему 1.1 из [6, гл. X]. Тогда группу $K(S, m)$ элементов из K^*/K^{*m} , локально являющихся m -ми степенями вне множества S , можно отождествить с группой U_S/U_S^m , где U_S – группа S -единиц поля K . Наконец, применение теоремы Дирихле о S -единицах для определения $\mathbb{Z}/m\mathbb{Z}$ -ранга группы U_S/U_S^m устанавливает справедливость предложения.

Продолжим доказательство теоремы 1. В нашем случае $K = \mathbb{Q}$, $\text{Cl}_K = \{1\}$, и нетрудно видеть, что

$$r = \text{rank}_{\mathbb{Q}} E(\mathbb{Q}) \leq 2 + 2\omega(\Delta), \quad (6)$$

где $\omega(n)$ – количество различных простых делителей числа n . Воспользуемся предложением 1, заметив, что кривая E имеет плохую редукцию по модулю простых чисел, делящих $\mathcal{D}$, и только их, в то время как $\mathcal{D}$ делит Δ , и что $\text{rank}_{\mathbb{Q}} E(\mathbb{Q}) = \text{rank}_{\mathbb{Z}/2\mathbb{Z}} E(\mathbb{Q}) - 2$, так как $E[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subseteq E(\mathbb{Q})$.

Поскольку

$$|\Delta| \leq 2^{10} H^6(E), \quad (7)$$

то согласно асимптотическому закону распределения простых чисел справедлива оценка

$$\omega(\Delta) \leq c_3 \frac{h(E)}{\log h(E)}, \quad (8)$$

и, кроме того, в силу неравенства (6) ясно, что

$$r \leq 2 + 2c_3 \frac{h(E)}{\log h(E)} \leq 2 + 2c_3 \frac{\log B}{\log \log B}. \quad (9)$$

В зависимости от того, насколько точна последняя оценка, возникают два случая. (Положительное число $\delta < 1$ будет выбрано в конце доказательства.)

СЛУЧАЙ А. Дискриминант Δ имеет не более $\delta \log B / \log \log B$ различных простых делителей.

Здесь можно воспользоваться результатом Массера [4], который при $k = K = \mathbb{Q}$ формулируется следующим образом.

ЛЕММА 1. *Существуют такие абсолютные постоянные c_4 и c_5 , что число точек из $E(\mathbb{Q})$, имеющих образ в шаре радиуса c_4 с центром в точке решетки Λ , не превосходит $c_5 h^{3/2}(E)$.*

Пусть $\rho > 0$. Всякое подмножество $\mathcal{X}$ шара радиуса R допускает покрытие, состоящее не более чем из $[(1 + 2R/\rho)^r]$ шаров радиуса ρ с центрами в элементах подмножества $\mathcal{X}$. (Достаточно взять наибольшее множество попарно не пересекающихся шаров радиуса $\rho/2$ с центрами в элементах подмножества $\mathcal{X}$: удвоив радиус этих шаров, получим покрытие, число элементов которого не превосходит отношения объемов шаров радиусов $R + \rho/2$ и $\rho/2$.) Таким образом, выбирая в качестве $\mathcal{X}$ множество точек решетки Λ в шаре радиуса R , полагая $\rho = c_4$ и учитывая лемму 1, получим неравенство

$$N(B) \leq c_5 h^{3/2}(E) \left(1 + 2 \frac{R}{c_4}\right)^r.$$

Учитывая то, что мы рассматриваем случай А, а также неравенство (6), имеем оценку

$$r \leq 2 + 2 \frac{\delta \log B}{\log \log B}.$$

Кроме того, $h(E) \leq R^2$. Следовательно,

$$\begin{aligned} N(B) &\leq c_5 R^3 \left(1 + 2 \frac{R}{c_4}\right)^{2+2\delta \log B / \log \log B} \\ &\leq c_6 R^5 (c_7 R)^{2\delta \log B / \log \log B} \\ &\leq c_6 (\log B)^{5/2} \exp\left(\delta \log B + c_8 \frac{\delta \log B}{\log \log B}\right). \end{aligned} \quad (10)$$

Теперь перейдем ко второму случаю.

СЛУЧАЙ В. *Дискриминант Δ имеет не менее $\delta \log B / \log \log B$ различных простых делителей.*

В этом случае вместо леммы 1 мы воспользуемся оценкой снизу высоты точек без кручения, полученной М. Хиндри и Дж. Сильверманом [2]. Эта оценка содержит отношение Шпиро $\sigma = \sigma_{E/\mathbb{Q}}$, определяемое равенством

$$\sigma = \frac{\log \mathcal{D}}{\log \mathcal{F}}, \quad (11)$$

где $\mathcal{F}$ – кондуктор кривой E над полем $\mathbb{Q}$ (см. [6, с. 361]). (Как указано в статье [2], если $\mathcal{F} = 1$, то $\mathcal{D} = 1$, что противоречит предположению случая В.) Перед тем как применить результат Хиндри–Сильвермана, оценим отношение Шпиро, учитывая условие случая В. Согласно таблице 15.1 приложения С книги [6] кондуктор кратен всем простым числам, делящим $\mathcal{D}$, за исключением, быть может, чисел 2 и 3, а поскольку мы рассматриваем квазимиимальную модель, кондуктор кратен также и всем простым числам, делящим Δ , за исключением, быть может, чисел 2 и 3. В частности, $6\mathcal{F}$ превосходит произведение первых $\delta \log B / \log \log B$ простых чисел. Снова применяя асимптотический закон распределения простых чисел, мы заключаем, что если, например, $\delta > 1/\sqrt{\log B}$, то

$$\log \mathcal{F} \geq c_9 \delta \log B.$$

С другой стороны, согласно неравенству (7) справедлива оценка

$$\log \mathcal{D} \leq 10 \log 2 + 4h(E).$$

Следовательно, поскольку $\log B \geq h(E)$ по предположению, в случае В для отношения Шпиро мы получаем неравенство $\sigma \leq c_{10}/\delta$.

Для удобства читателя приведем формулировку теоремы 0.3 работы [2].

ЛЕММА 2. *Пусть K – числовое поле. Тогда для всех эллиптических кривых E/K и всех точек $P \in E(K)$ без кручения выполнено неравенство*

$$\hat{h}_E(P) \geq (20\sigma_{E/K})^{-8[K:\mathbb{Q}]} 10^{-1.1-4\sigma_{E/K}} \log(N_{K/\mathbb{Q}} \mathcal{D}_{E/K}).$$

Здесь через $N_{K/\mathbb{Q}}$ обозначена норма, а через $\mathcal{D}_{E/K}$ – минимальный дискриминант кривой E как идеал в K .

Отсюда немедленно заключаем, что для всех точек $P \in E(\mathbb{Q})$ без кручения справедлива оценка

$$\hat{h}(P) \geq c_{11} \delta^8 10^{-4c_{10}/\delta} \log \mathcal{F}.$$

Таким образом, сочетая этот факт с полученной ранее нижней оценкой для $\log \mathcal{F}$, получим

$$\hat{h}(P) \geq e^{-c_{12}/\delta} \log B = e^{-c_{12}/\delta} R^2. \quad (12)$$

Снова перейдем к пространству $\mathbb{R}^r$. Используя нижнюю оценку (12), можно получить больше информации по сравнению с результатом Массера: *в любом шаре радиуса $\rho := e^{-c_{12}/(2\delta)} R$ с центром в узле решетки Λ находится не более одной точки множества $E(\mathbb{Q})/\text{tors}$.*

Проводя такое же рассуждение о покрытии, как и в случае А, получим

$$N(B) \leq \#E_{\text{tors}}(\mathbb{Q}) \left(1 + 2\delta \frac{R}{\rho}\right)^r = \#E_{\text{tors}}(\mathbb{Q}) (1 + 2\delta e^{c_{12}/(2\delta)})^r. \quad (13)$$

Простейший метод получения оценки для кручения описан в [6, гл. VIII, замечание 7.3.2]. Пусть p и q – два различных простых числа, по модулю которых кривая E имеет хорошую редукцию. Рациональное кручение порядка, взаимно простого с характеристикой, инъективно отображается в группу рациональных точек приведенной кривой (см. [6, гл. VII, предложение 3.1, (b)]), поэтому так как число рациональных точек $\bmod p$ на E тривиально оценивается числом $2p + 1$, то мы имеем

$$\#E_{\text{tors}}(\mathbb{Q}) \leq (2p + 1)(2q + 1).$$

Выбирая числа p и q наименьшими из возможных, получим неравенство

$$\#E_{\text{tors}}(\mathbb{Q}) \leq c_{13} \left(\frac{h(E)}{\log h(E)} \right)^2.$$

Кроме того, для ранга r вновь справедлива оценка (9).

Подставляя полученные оценки в формулу (13), при $\delta > 1/\sqrt{\log B}$ получим неравенство

$$N(B) \leq c_5 h^2(E) (1 + 2e^{c_{12}/(2\delta)})^{2+2c_3 \log B / \log \log B},$$

а поскольку $h(E) \leq \log B$, мы заключаем, что

$$N(B) \leq c_5 (\log B)^2 \exp \left(c_{14} \delta^{-1} \frac{\log B}{\log \log B} \right). \quad (14)$$

Наконец, положим $\delta = 1/\sqrt{\log \log B} > 1/\sqrt{\log B}$. Тогда результат доказываемой теоремы следует в случае А из оценки (10), а в случае В – из неравенства (14).

ДОКАЗАТЕЛЬСТВО СЛЕДСТВИЯ. Из условий следствия вытекают уравнения

$$p_3^2 \Delta_{12} = p_2^2 \Delta_{13} - p_1^2 \Delta_{23}, \quad (15)$$

$$p_4^2 \Delta_{12} = p_2^2 \Delta_{14} - p_1^2 \Delta_{24}. \quad (15^*)$$

Предположим вначале, что $\Delta_{13} \Delta_{24} = \Delta_{14} \Delta_{23}$. Тогда отношение p_3^2/p_4^2 однозначно определено (т.е. не зависит от p_i), и, значит, поскольку числа p_3 и p_4 простые и различные, то они также однозначно определены. Далее, из уравнений $p_i^2 \Delta_{34} - p_3^2 \Delta_{i4} + p_4^2 \Delta_{i3} = 0$, $i = 1, 2$, следует, что и числа p_1 , p_2 однозначно определены.

Таким образом, можно предполагать, что $\Delta_{13} \Delta_{24} \neq \Delta_{14} \Delta_{23}$.

Разделив равенства (15) и (15*) на наибольший общий делитель коэффициентов, можно переписать их в виде

$$p_3^2 A = p_2^2 A_2 - p_1^2 A_1, \quad (16)$$

$$p_4^2 B = p_2^2 B_2 - p_1^2 B_1, \quad (16^*)$$

где A , B , A_i , B_j — ненулевые целые числа такие, что $(A_1, A_2, A) = (B_1, B_2, B) = 1$ и $A_1 B_2 \neq A_2 B_1$.

Можно предположить, что имеются по крайней мере две различные четверки простых чисел (p_1, p_2, p_3, p_4) , (p'_1, p'_2, p'_3, p'_4) , удовлетворяющие уравнениям следствия. Векторы (p_1^2, p_2^2, p_3^2) и $(p_1'^2, p_2'^2, p_3'^2)$ неколлинеарны; в противном случае, будучи оба примитивными, они были бы равны, что повлекло бы $p_i = p'_i$ для $i = 1, 2, 3$. Тогда из (16*) следовало бы равенство $p_4 = p'_4$, что противоречит предположению о различности выбранных четверок.

Следовательно, вектор $(A_1, -A_2, A)$, ортогональный обоим векторам (p_1^2, p_2^2, p_3^2) и $(p_1'^2, p_2'^2, p_3'^2)$, пропорционален их векторному произведению, которое в силу сказанного выше отлично от нуля. Однако вектор $(A_1, -A_2, A)$ является примитивным, поэтому указанное векторное произведение равно целому кратному этого вектора. Учитывая границу для B_i , таким образом, можно считать, что

$$\max(|A_1|, |A_2|, |A|, |B_1|, |B_2|, |B|) \leq 2X^4. \quad (17)$$

Заметим, что соотношения (16), (16*), рассматриваемые как уравнения от неизвестных p_i , определяют эллиптическую кривую с рациональной точкой (p_1, p_2, p_3, p_4) . Чтобы применить теорему 1, мы используем классический трюк выделения уравнения Вейерштрасса. Перемножая (16) и (16*), умножая обе части получившегося равенства на $p_2^2(A_2 B_2)^2(AB)^3/p_1^6$ и полагая

$$u := \left(\frac{p_2}{p_1}\right)^2 A B A_2 B_2, \quad v := \frac{p_3 p_4 A B A_2 B_2}{p_1^3}, \quad (18)$$

получаем рациональную точку (u, v) на эллиптической кривой E , заданной уравнением

$$Y^2 = (X - e_1)(X - e_2)(X - e_3), \quad (19)$$

где $e_1 = 0$, $e_2 = A B A_1 B_2$, $e_3 = A B A_2 B_1$.

Заметим, что $A_1B_2 \neq A_2B_1$ и $A_1A_2B_1B_2AB \neq 0$, откуда следует, что e_i попарно различны и уравнение (19) действительно определяет эллиптическую кривую. Кроме того, числа e_1, e_2, e_3 целые, следовательно, E имеет рациональное 2-кручение, и можно применить теорему 1.

Определение (2) и оценка (17) влекут неравенство $H(E) \leq 2^{12}X^{48}$. Следовательно, полагая $M = \log(2^{12}X^{48})$, мы получаем из теоремы 1, что количество рациональных точек $P \in E$ таких, что $h(P) \leq M$, не превосходит

$$\exp\left(C \frac{M}{\sqrt{\log M}}\right) \leq \exp\left(C' \frac{\log X}{\sqrt{\log \log X}}\right), \quad (20)$$

где C, C' являются (эффективными) абсолютными константами.

Для завершения доказательства заметим, что в силу (18), (17) и оценки $p_i \leq X$ всякая четверка простых чисел указанного выше вида продуцирует рациональную точку P на E высоты $h(P) \leq \log(2^5X^{18}) \leq M$. Далее несложно проверить, что различные четверки продуцируют различные рациональные точки. Таким образом, мы получаем оценку (20) для числа соответствующих четверок, что доказывает следствие.

2. Несколько дополнительных замечаний. Теорема 1 справедлива для всякой эллиптической кривой $E/\mathbb{Q}$, для которой $E[2] \subset E(\mathbb{Q})$, с высотой, определенной произвольным положительным дивизором на кривой E (при этом постоянная C может зависеть от этого дивизора).

Подсчет точек решетки показывает, что $N(B) \sim c_\Lambda (\log B)^{r/2}$ при $B \rightarrow \infty$, где постоянная c_Λ равна отношению объема единичного шара в $\mathbb{R}^r$ к объему фундаментальной области решетки Λ . Важной особенностью теоремы 1 является равномерность ее результата по E и B , что позволяет использовать его в приложениях. Можно предположить, что оценка

$$\#\{P \in E(K) : H(P) \leq B\} \leq \left(\max\left(C, C \frac{\log B}{h(E)}\right)\right)^{r/2},$$

где $r := \text{rank}_{\mathbb{Q}} E(K) \leq Ch(E)/\log(h(E)+3)$, справедлива для квазимиимальной модели E/K , причем постоянная C зависит только от K или даже только от $[K:\mathbb{Q}]$.

Предположение того, что кривая E имеет рациональное 2-кручение, можно ослабить, потребовав, чтобы эта кривая содержала рациональную точку порядка 2, и применив метод спуска относительно изогении, имеющей ядро, равное подгруппе, порожденной этой точкой. Подробное рассмотрение этого вопроса можно найти в [6, гл. X, предложение 4.9 и замечание 4.9.2].

В случае, когда $E[2]$ не содержится в $E(\mathbb{Q})$, при оценке ранга мы сталкиваемся с серьезными трудностями. Если пытаться расширить исходное поле $\mathbb{Q}$ до нового поля K для того, чтобы получить включение $E[2] \subset E(K)$, то отсутствие контроля над $\text{Cl}_K[2]$ приводит к более слабым оценкам для $\text{rank}_{\mathbb{Q}} E(K)$. Но даже если бы имелась хорошая оценка этого ранга, мы все равно должны были построить последовательность инфляций и ограничений когомологии Галуа, нисходящую к $\text{rank}_{\mathbb{Q}} E(\mathbb{Q})$, что повлекло бы за собой новые сложности. Было бы интересно разобраться в этом вопросе.

Оценка леммы 2 была улучшена в работе [1, теорема 1.3], что, в принципе, должно привести к усилению результата теоремы 1. Однако в теореме 1.3 статьи [1] требуется, чтобы кривая E была полустабильной, и устранение этого условия посредством замены базы, по-видимому, приведет к описанным выше трудностям. Поэтому вместо того, чтобы изменять доказательство этой теоремы, мы применили более слабое утверждение работы [2], которое является предпочтительным для наших целей.

Список литературы

1. *David S.* Points de petite hauteur sur les courbes elliptiques // J. Number Theory. 1997. V. 64. P. 104–129.
2. *Hindry M., Silverman J. H.* The canonical height and integral points on elliptic curves // Invent. Math. 1988. V. 93. P. 419–450.
3. *Конягин С. В.* Задачи о множестве чисел, свободных от квадратов // Изв. РАН. Сер. матем. 2004. Т. 68. № 3. С. 63–90.
4. *Masser D.* Counting points of small height on elliptic curves // Bull. Soc. Math. France. 1989. V. 117. P. 247–265.
5. *Narkiewicz W.* Elementary and analytic theory of algebraic numbers, IInd // PWN – Polish Publishers. N. Y.: Springer-Verlag, 1990.
6. *Silverman J. H.* The Arithmetic of Elliptic Curves // GTM. V. 106. N. Y.: Springer-Verlag, 1986.
7. *Zimmer H. G.* On the difference of the Weil height and the Néron–Tate height // Math. Z. 1976. V. 147. P. 35–51.

Institute for Advanced Study Einstein Drive
Ist. Univ. Arch. DCA

Поступило в редакцию
15.08.2003

Перевод с английского
С. В. Конягина, А. В. Бегунца