M. I. Bashmakov, A. S. Kurochkin, Rational points of some modular curve over 2-cyclotomic field, *Zap. Nauchn. Sem. LOMI*, 1976, Volume 57, 5–7

М.И.Башмаков, А.С.Курочкин

РАЦИОНАЛЬНЫЕ ТОЧКИ НА ОДНОЙ МОДУЛЯРНОЙ КРИВОЙ В КРУГОВОМ 2-РАСШИРЕНИИ

Модулярная кривая $X_0(32)$ может быть задана уравнением $y^2 = x^3+4x$. Нас интересует поведение этой кривой в бесконечном расширении поля рациональных чисел, получающемся при присоединении всей корней степеней 2^n из единицы.Этот вопрос представляет большой интерес в связи с гипотезой Мазура о конечной порожденности группы рациональных точек эллиптической кривой в круговом Γ-расширении. Решению этой проблемы в разных частных случаях посвящены работы [I, 2] .

Выбранная нами кривая интересна в нескольких отношениях. Во-первых, ее редукция по делителю двойки вырождена, но становится невырожденной и суперсингулярной в конечном расширении основного поля. Как выяснено в работе [2] этот случай является существенно более трудным, чем те, которые разбирались Б.Мазуром и Ю.И. Маниным. Во-вторых, фиксируется простое число $p = 2$. Методы, развитые в работе [2] не переносятся так прямо на этот случай.$p = 2$ всегда вызывает дополнительные трудности.

Разумеется, подход, развитый в настоящей статье,является довольно общим и применим к более широкому классу ривых. В то же время мы ограничиваемся конкретным примером, так как в нем удается все вычисления довести до конца, а полученный числовой материал может послужить в дальнейшем несколько более широким целям, чем подтверждение гипотезы Мазура.

I^0. Обозначения и формулировка результата. Основное поле: $K_0 = \mathbb{Q}(i)$, $i^2=-1$. Исходная кривая E : $y^2=x^3+x$ (она очевидно изоморфна $X_0(32)$ над полем корней восьмой степени из единицы). Рассматривается круговое 2-расширение K_0 : $K_n = K_{n-1}(\varepsilon_n)$, где $\varepsilon_n^2 = \varepsilon_{n-1}$, $\varepsilon_0 = i$; $K_\infty = \bigcup K_n$ Очевидно, что поле K_n является полем деления круга на 2^{n+2} частей, его степень над $\mathbb{Q}$ равна 2^{n+1}

Для любого поля L через $E(L)$ будем обозначать группу точек E с координатами в поле L .

ТЕОРЕМА I. Группа $E(K_\infty)$ конечна и изоморфна $\mathbb{Z}/4\mathbb{Z} + \mathbb{Z}/4\mathbb{Z}$. Этот результат описывает все решения диофантова уравнения $y^2 = x^3+ x$ в бесконечном расширении $K_\infty/\mathbb{Q}$.

СЛЕДСТВИЕ. Уравнение $x^4+y^4=z^4$ не имеет решений в K_∞, кроме „тривиальных", соответствующих точкам периода 2^n на якобиевом многообразии.

ЗАМЕЧАНИЕ. Точки конечного порядка на якобиевом многообразии кривой $x^4+y^4=z^4$ в поле K_∞ были найдены Д.К.Фаддеевым и В.Е.Лапицким. Число их оказалось равным 2^9.

Группа $\mathrm{Ш}^n$ определяется как 2-компонента группы локально тривиальных главных однородных пространств над E в поле K_n, а группа S^n как группа соответствующих накрытий [3]. Имеется точная последовательность

$$0 \to E(K_n) \otimes \mathbb{Q}_2/\mathbb{Z}_2 \to S^n \to Ш^n \to 0.$$

ТЕОРЕМА 2. Группа $Ш^n$ конечна и изоморфна

$$(\mathbb{Z}/2^{n-2}\mathbb{Z})^4 + (\mathbb{Z}/2^{n-3}\mathbb{Z})^8 + \ldots + (\mathbb{Z}/2\mathbb{Z})^{2^{n-1}}; \quad |Ш^n| = 2^{n+1} - 4n, \quad n \geq 1.$$

2°. <u>Группы Зельмера</u>. Группы Зельмера S^n_k определяются из точной последовательности

$$0 \to E(K_n)/\nu^k E(K_n) \to S^n_k \to Ш^n_k \to 0,$$

где через ν обозначено комплексное умножение кривой E на $1+i$, а $Ш^n_k$ - ядро умножения $Ш^n$ на ν^k. Информация о группах S^n_k при $k =$ I, 2, 3 была получена в работе [4].

Сформулируем результаты:

ПРЕДЛОЖЕНИЕ I. $\nu S^n_2 = S^n_1$.

ПРЕДЛОЖЕНИЕ 2. $2S^n_3 \overset{2}{=} iS^{n-1}_1$, где i - вложение S^{n-1}_1 в S^n_1, $(n \geq 3)$.

Обозначим через K^+_n вещественное подполе K_n, а через τ нетривиальный автоморфизм K_n/K^+_n. Группы Зельмера можно рассматривать как $\mathbb{Z}[\tau, i]$ - модули $(\tau i = -i\tau)$. Для $\mathbb{Z}[\tau, i]$-модуля A через A^+ будет обозначаться ядро $\tau - 1$, а через A^x ядро $\tau + i$.

ПРЕДЛОЖЕНИЕ 3. а) $S^n_1 = (S^n_1)^+ = (S^n_1)^x$,

б) $S^n_2 = (S^n_2)^x$; $S^n_2 = j S^n_1$, где j - вложение S^n_1 в S^n_2.

ПРЕДЛОЖЕНИЕ 4. $S^n_k = (S^n_k)^+ + (S^n_k)^x$.

Доказывается по индукции.

ПРЕДЛОЖЕНИЕ 5. $S^{n-1}_k = 2S^n_{k+2}$ (мы считаем S^{n-1}_k вложенной в S^n_{k+2}).

Базой индукции является предложение 2. Индукционнй переход проводится несложно.

3°. <u>Доказательство основных теорем</u>. Из предложения 5 получается точная последовательность

$$0 \to S^n_2 \to S^n_k \xrightarrow{2} S^{n-1}_{k-2} \to 0 \quad (k > 2).$$

Если $f \in S^n_1$ и бесконечно делим в S^n, то очевидно, что $f \in S^1_1$. Однако мы знаем, что группа S^1_1 состоит только из накрытия, соответствующего точке конечного порядка. Отсюда вытекает теорема I, а также конечность группы $Ш^n$. Из приведенной выше точной последовательности следует, что $|Ш^n| = \sum |Ш^k_2| + 1 = 2^{n+1} - 4n$, $n \geq 1$. Отсюда же следует и структура группы $Ш^n$.

Литература

I. Манин Ю.И. Круговые поля и модулярные кривые. - Успехи мат. наук, 1971, 26, № 6, 7-71.

2. Башмаков М.И., Аль-Надер Н.Ж. Поведение кривой $x^3+y^3=1$ в круговом Г-расширении. - Мат.сб., 1973, 90, № I, 117-130.

3. Башмаков М.И. Когомологии абелевых многообразий над числовым полем. - Успехи мат.наук, 1972, 27, № 6, 25-66.

4. Башмаков М.И., Курочкин А.С. Группы Зельмера эллиптической кривой $X_0(32)$. - В сб. Современная алгебра, вып.IУ. Л., 1975, 3-12.