Д. К. Фаддеев, Об одной работе А. Бейкера, *Зап. научн. сем. ЛОМИ*, 1966, том 1, 128–139

Д.К.Фаддеев

ОБ ОДНОЙ РАБОТЕ А.БЕЙКЕРА

В работе [1] А.Бейкер производит подсчет констант в оценках приближения радикальных иррациональностей при помощи метода Туэ-Зигеля, с применением явных формул для полиномов Туэ. В качестве применения полученных результатов приводятся примеры диофантовых уравнений вида $ax^3+by^3=c$, эффективно разрешимых при любой правой части c. К числу таких уравнений, оказывается, можно причислить уравнение $x^3-2y^3=c$.

Цель настоящей заметки - довести подсчет констант до предельной точности и распространить результат на некоторые уравнения из более обширного класса бинарных кубических диофантовых уравнений.

1°. Пусть $f(x,y)$ - неприводимая в поле Q рациональных чисел кубическая форма, имеющая корень ρ в поле $K=Q(\rho)$ (под корнем формы понимается корень уравнения $f(x,1)=0$). Ясно, что если мы умеем эффективно решить уравнение $f(x,y)=c$ при любой правой части c, то эффективно разрешимым окажется всякое уравнение $F(x,y)=c$, где F любая кубическая форма с корнем в поле K, ибо, как легко видеть, существует такое целое число A и такая целочисленная невырожденная (не обязательно унимодулярная) матрица $\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}$, что

$AF(x,y)=f(\alpha x+\beta y,\ \gamma x+\delta y)$ так что решение уравнения $F(x,y)=C$ приводится к решению уравнения $f(x,y)=AC$. Поэтому, при отыскании уравнений, допускающих эффективное решение методом Туэ-Зигеля, достаточно ограничиться одной формой f для каждого кубического поля, содержащего корень формы, например, индекс-формы ([2] , § 15) кольца всех целых чисел поля K. Технически удобнее привлечь к рассмотрению индекс-форму некоторого кольца Λ, не обязательно максимального (то есть кольца всех целых), но тесно с ним связанного.

2°. Как показано в монографии [2], §§ 44, 45, с каждым кубическим полем K с дискриминантом $\mathfrak{D}$ естественным образом связывается некоторая плоская решетка L точек - решетка целых резольвент Лагранжа чисел поля K. Напомним, как устроена эта решетка. Допустим сначала, что K не чисто-кубическое поле, то есть $\mathfrak{D}\neq-3\delta^2$ при рациональном δ. Тогда

$$L=\sqrt[3]{\ell\mu}\cdot\mathfrak{a}.$$

Здесь $\mathfrak{a}$ - некоторый идеал поля $k=Q(\sqrt{-3\mathfrak{D}})$, $\ell=N(\mathfrak{r})$, $\mathfrak{r}$ - идеал, норма ℓ которого свободна от квадратов и взаимно проста с дискриминантом d поля k, причем $\mathfrak{r}$ эквивалентен идеалу $\mathfrak{a}^3$; наконец μ - множитель, в равенстве $\mathfrak{r}=\mu\mathfrak{a}^3$. Идеал $\mathfrak{a}$ определен с точностью до эквивалентности, множители μ с точностью до кубов единиц поля k. Наконец, требуется, чтобы число $\ell\mu$ не было кубом числа из k (обратное возможно только, если $\mathfrak{a}$ главный идеал и $\ell=1$).

Наряду с решеткой L нужно ввести в рассмотрение сопряженную решетку $\overline{L}=\sqrt[3]{\ell\bar{\mu}}\ \bar{\mathfrak{a}}$. Здесь черточкой обозначен переход к сопряженным числам в поле k. Значение для $\sqrt[3]{\ell\bar{\mu}}$ выбирается так, чтобы произведение $\sqrt[3]{\ell\mu}\cdot\sqrt[3]{\ell\bar{\mu}}$ оказалось рациональным числом, что всегда можно сделать, ибо

$$(\ell\mu)(\ell\bar{\mu})=\ell^2\gamma\bar{\gamma}\,(\alpha\bar{\alpha})^{-3}=(\ell N\alpha^{-1})^3.$$

Оказывается, что между кубическими (не чисто-кубическими) полями K и парами сопряженных решеток $L, \bar{L}$ существует взаимно-однозначное соответствие, причем сопряженным полям K отвечают решетки L, разлагающиеся на кубические корни из 1.

Для чисто-кубических полей вместо поля k нужно рассмотреть прямую сумму двух полей рациональных чисел с покоординатным умножением, в качестве α решетку с целыми координатами, $\mu=(a,b)$, где a и b взаимно простые, свободные от квадратов числа, $\ell=ab$, так что решетка L образована парами $\left(u\sqrt[3]{a^2b},\ v\sqrt[3]{ab^2}\right)$ с целыми u, v; переход к решетке $\bar{L}$ осуществляется перестановкой координат.

Множество чисел вида $s+\lambda+\bar{\lambda}$, где s целое рациональное, $\lambda\in L$, образует кольцо Λ в поле K, причем оно имеет индекс 1, 3 или 9 в кольце всех целых чисел поля K. Индекс-форма кольца Λ находится по формуле

$$f(x,y)=\frac{\theta^3-\bar{\theta}^3}{\ell\sqrt{d}}=\frac{\mu(\alpha_1x+\alpha_2y)^3-\bar{\mu}(\bar{\alpha}_1x+\bar{\alpha}_2y)}{\sqrt{d}}\ .$$

Здесь α_1, α_2 - какой-либо базис идеала α, θ - "общее" число решетки L, $\theta=\sqrt[3]{\ell\mu}\ (\alpha_1x+\alpha_2y)$. Диофантово уравнение $f(x,y)=c$ равносильно уравнению

$\theta^3 - \bar{\theta}^3 = \ell c \sqrt{d}$, причем решение требуется искать среди чисел, составляющих решетку L .

Решетка L обладает еще следующими, почти очевидными свойствами. Произведение двух чисел из решетки L есть число из решетки $\bar{L}$, точнее, из ее подрешетки $\gamma \bar{L}$. Произведение числа из L на число из $\bar{L}$ есть целое число поля k , делящееся на ℓ . Куб числа из решетки L есть целое число поля k , принадлежащее идеалу $\ell\gamma$, не являющееся кубом числа из поля k и имеющее норму, равную кубу целого рационального числа.

Для последующих оценок нам полезно ввести норму $\|\theta\|$ для точек решетки L , $\bar{L}$ и поля k, положив $\|\theta\| = \max(|\theta|, |\bar{\theta}|)$. Если $\mathcal{D} > 0$, то числа поля k , решеток L и $\bar{L}$ суть комплексные числа и $\bar{\theta}$ комплексно сопряжено с θ . Поэтому, в этом случае $\|\theta\| = |\theta|$. Если же $\mathcal{D} < 0$, то можно считать числа поля k и решеток L и $\bar{L}$ вещественными и интерпретировать каждое такое число точкой на плоскости с координатами $\theta, \bar{\theta}$.

Ясно, что $\|\theta_1 + \theta_2\| \leqslant \|\theta_1\| + \|\theta_2\|$ и $\|\theta_1\theta_2\| \leqslant \leqslant \|\theta_1\| \cdot \|\theta_2\|$.

Для точек решетки L, отличных от точки $(0, 0)$, имеет место неравенство $\|\theta\| \geq 1$. Для $\mathcal{D} \neq -3s^2$ это следует из того, что $|\theta\bar{\theta}|$ есть натуральное число; для $\mathcal{D} = -3s^2$ неравенство непосредственно следует из формул для координат точки $(\theta, \bar{\theta})$. Оценка может быть уточнена еще следующим образом. Пусть δ – наибольший общий делитель чисел θ и $\bar{\theta}$ в кольце всех целых алгебраических чисел. Тогда δ^3 есть наибольший делитель сопряженных чисел θ^3 и $\bar{\theta}^3$ поля k, и, следовательно, его квадрат δ^6 ассоциирован с некоторым натуральным числом τ, так что можно принять $\delta = \tau^{1/6}$. Тогда $|\theta\bar{\theta}| \geq \tau^{1/3}$ и, следовательно, $\|\theta\| \geq \tau^{1/6}$.

3^0. Если уравнение $\theta^3 - \bar{\theta}^3 = \ell c\sqrt{d}$ удовлетворяется некоторым числом $\theta \in L$ и наименьшим по модулю из трех чисел $\theta - \bar{\theta}$, $\theta - \bar{\theta}\zeta$, $\theta - \bar{\theta}\zeta^2$ $\left(\zeta = -\frac{1}{2} + i\,\frac{\sqrt{3}}{2}\right)$, оказывается $\theta - \bar{\theta}$, то как легко видеть, будет выполнено неравенство

$$\left|\bar{\theta} - \theta\right| < \frac{\ell |c| \sqrt{|d|}}{\|\theta\|^2}.$$

Поэтому, если нам удается ограничить норму $\|\theta\|$ для всех точек решетки L, удовлетворяющих неравенству

$$\left|\bar{\theta} - \theta\right| < \frac{1}{\|\theta\|^{2-\varepsilon}}$$

при некотором $\varepsilon > 0$, то, тем самым, будет ограничена норма для решений уравнения $\theta^3 - \bar{\theta}^3 = \ell c\sqrt{d}$ при любом фиксированном целом числе c.

4^0. Введем теперь в рассмотрение полиномы Туэ в форме, описанной в § 70 монографии [2], причем нам нужны только полиномы с четными номерами.

$$A_{2n}(z) = \sum_{k=0}^{n} \binom{n - \frac{2}{3}}{k} \binom{n - \frac{1}{3}}{n-k} z^k$$

$$B_{2n}(z)=\sum_{k=0}^{n-1}\binom{n-\frac{1}{3}}{k}\binom{n-\frac{2}{3}}{n-1-k}z^{k}.$$

В дальнейшем с каждым полиномом $F(z)$ степени m мы будем связывать бинарную форму

$$F(u,v)=v^{m}F\left(\frac{u}{v}\right).$$

Полиномы A_{2n}, B_{2n} обладают следующими свойствами.

1. $A_{2n}(x^{3})-x\,B_{2n}(x^{3})=(1-x)^{2n}\,V_{2n}(x).$

Здесь $V_{2n}(x)$ некоторый полином степени n.

2. Коэффициенты полиномов A_{2n}, B_{2n} и V_{2n} положительны и становятся целыми рациональными числами после умножения на $3^{[\frac{3}{2}n]}$

3. $A_{2n}(1)=\dfrac{(2n-1)!}{n!\,(n-1)!}<\dfrac{1}{2}\,2^{2n}$,

$$V_{2n}(1)=\frac{(3n)!}{3^{n}n!\,(2n)!}<\frac{1}{2}\left(\frac{3}{2}\right)^{2n}.$$

Заметим, что основания степени в этих оценках не могут быть уменьшены, что легко видеть, например, из формулы Стирлинга.

4. $A_{2n}(x^3,y^3)A_{2n}(y^3,x^3)-x^3y^3B_{2n}(x^3,y^3)B_{2n}(y^3,x^3)=$

$=(x^3-y^3)^{2n}A_{2n}(1,0)A_{2n}(0,1).$

5. $A_{2n}(z)=\sum_{k=0}^{n}(-1)^k\frac{(2n-k-1)!}{(n-1)!\,(n-k)!}\cdot\binom{n-\frac{2}{3}}{k}\cdot(1-z)^k,$

$$B_{2n}(z)=\sum_{k=0}^{n-1}(-1)^k\frac{(2n-k-1)!}{n!\,(n-k-1)!}\binom{n-\frac{1}{3}}{k}(1-z)^k.$$

Доказательства свойств I - 4 имеется в [2] , § 70. Свойство 5 имеется в [I] .

6. $3^{\frac{3-\sigma}{2}}A_{2n}(1-3^{\sigma/2}v)$ имеет целые коэффициенты (в поле $Q(\sqrt{3})$, $0\leqslant\sigma\leqslant 3$).

Это свойство непосредственно следует из свойств 5.

5°. Пусть θ точка решетки L , причем $|\theta-\bar\theta|$ достаточно близко к нулю. Пусть, кроме того, θ_1 -другая точка решетки L , такая, что

$$|\bar\theta_1-\theta_1|<\frac{1}{\|\theta_1\|^{2-\varepsilon}},$$

при некотором $\varepsilon>0$.

Рассмотрим число

$$U_n=3^{[\frac{3}{2}n]}\left[\bar\theta_1A_{2n}(\bar\theta^3,\theta^3)-\theta_1\bar\theta\,\theta^2B_{2n}(\bar\theta^3,\theta^3)\right].$$

Оно изображается точкой решетки L, причем обе координаты $\mathcal{U}_n, \bar{\mathcal{U}}_n$ этой точки не могут одновременно обратиться в 0, в силу свойства 4 полиномов A_{2n}, B_{2n}. Поэтому $\|\mathcal{U}_n\|$ легко ограничить снизу. Обозначив через h наибольший общий делитель чисел θ^3, $\bar{\theta}^3$ (который можно принять равным некоторому натуральному числу или квадратному корню из натурального числа), мы получим

$$\|\mathcal{U}_n\| \geq h^n.$$

Свойство 6 позволяет еще немного усилить это неравенство. Именно, верно

$$\|\mathcal{U}_n\| \geq h^n 3^{\frac{n\sigma}{2}},$$

где $3^{\frac{\sigma}{2}}$, $0 \leq \sigma \leq 3$, есть наибольший общий делитель чисел $3^{3/2}$ и $\dfrac{\theta^3 - \bar{\theta}^3}{h}$.

С другой стороны,

$$\mathcal{U}_n = 3^{\left[\frac{3}{2}n\right]}\left[(\bar{\theta}_1 - \theta_1)A_{2n}(\bar{\theta}^3, \theta^3) + \theta_1(\bar{\theta} - \theta)^{2n} V_n(\bar{\theta}, \theta)\right],$$

откуда следует

$$\|\mathcal{U}_n\| \leq 3^{3/2 n}\left[|\bar{\theta}_1 - \theta_1| \cdot \|A_{2n}(\bar{\theta}^3, \theta^3)\| + |\bar{\theta} - \theta|^{2n} \|\theta_1\| \cdot \|V_{2n}(\bar{\theta}, \theta)\|\right].$$

В силу положительности коэффициентов A_{2n} и V_{2n} ясно, что $\| A_{2n}(\bar{\theta}^3, \theta^3) \| \leq \|\theta\|^{3n} A_{2n}(1) < \frac{1}{2} \|\theta\|^{3n} 2^{2n}$

и $\| V_{2n}(\bar{\theta}, \theta) \| \leq \|\theta\|^{n} V_{2n}(1) < \frac{1}{2} \|\theta\|^{n} (3/2)^{2n}$.

Итак, имеет место неравенство :

$$3^{3/2 n} \cdot \frac{1}{\|\theta_1\|^{2-\varepsilon}} \cdot \frac{1}{2} \cdot \|\theta\|^{3n} \cdot 2^{2n} + 3^{3/2 n} |\bar{\theta}-\theta|^{2n} \cdot \|\theta_1\| \cdot \frac{1}{2} \cdot \|\theta\|^{n} \cdot$$

$$\cdot (3/2)^{2n} \geq h^n 3^{\frac{n\sigma}{2}}.$$

Оно, очевидно, невозможно, если

$$3^{3/2 n} \cdot \frac{1}{\|\theta_1\|^{2-\varepsilon}} \cdot \|\theta\|^{3n} 2^{2n} < h^n 3^{\frac{n\sigma}{2}}$$

и

$$3^{\frac{3}{2} n} \|\theta\|^{n} \cdot |\bar{\theta}-\theta|^{2n} \cdot \left(\frac{3}{2}\right)^{2n} \cdot \|\theta_1\| < h^n 3^{\frac{n\sigma}{2}},$$

то есть, если

$$\left[3^{\frac{3-\sigma}{2(2-\varepsilon)}}\cdot 2^{\frac{2}{2-\varepsilon}}\|\theta\|^{\frac{3}{2-\varepsilon}} h^{-\frac{1}{2-\varepsilon}}\right]^n < \|\theta_1\| <$$

$$< \left[h\, 3^{-\frac{3-\sigma}{2}}\cdot\frac{4}{9}\cdot\|\theta\|^{-1}\, |\bar\theta-\theta|^{-2}\right]^n .$$

Если только

$$3^{\frac{3-\sigma}{4}}\, 2\cdot\|\theta\|^{\frac{3}{2}}\cdot h^{-1/2} < h\, 3^{-\frac{3-\sigma}{2}}\cdot\frac{4}{9}\,\|\theta\|^{-1}\,|\bar\theta-\theta|^{-2}, \qquad (*)$$

то, при некотором $\varepsilon > 0$, мы получим бесконечную последовательность интервалов, которым не может принадлежать $\|\theta_1\|$, причем, при достаточно большом n, эти интервалы будут перекрываться и закроют все достаточно большие числа действительной оси. Тем самым, мы получим ограничение сверху для $\|\theta_1\|$.

Для построения ограничения $\|\theta_1\|$ этим методом нужно существование точки θ решетки L, удовлетворяющей неравенству $(*)$, то есть такой, что

$$3^{\frac{3}{4}(3-\sigma)}\cdot\frac{9}{2}\cdot\|\theta\|^{5/2}\cdot|\bar\theta-\theta|^{2} < h^{3/2} \qquad (**)$$

Заметим, что если некоторая точка θ решетки L удовлетворяет неравенству $(**)$, то ему удовлетворяет и любая точка $K\theta$ (при целом K) и обратно, ибо при переходе от $K\theta$ к θ

обе части (**) умножаются на $|\kappa|^{9/2}$. Поэтому, при поиске нужных точек достаточно ограничиться примитивными точками решетки L. Пусть $\theta = \sqrt[3]{\ell_{\mathfrak{m}}} \cdot \alpha$, $(\alpha) = \mathfrak{a}\mathfrak{b}$ – примитивная точка решетки L. Для этого необходимо и достаточно, чтобы идеал $\mathfrak{b}$ не делился на натуральное число, то есть чтобы $\mathfrak{b}$ состоял лишь из простых идеалов первой степени, взятых по одному (но с любым показателем) из некритических простых чисел $\mathfrak{u}$ с показателем, не превосходящим 1, из критических. Ввиду того, что $(\theta^3) = \ell \mathfrak{r} \mathfrak{b}^3$, $(\bar{\theta}^3) = \ell \bar{\mathfrak{r}} \bar{\mathfrak{b}}^3$, имеем $h = \ell m \Delta^{3/2}$, где m – делитель ℓ, равный норме идеала $(\bar{\mathfrak{r}}, \mathfrak{b})$ и Δ – делитель d, равный норме произведения критических простых идеалов, входящих в идеал $\mathfrak{b}$.

Разумеется, точки решетки L, удовлетворяющие неравенству (* *) конструируются из достаточно хороших рациональных приближений какого-либо числа поля k.

Для полей с отрицательным дискриминантом достаточно хорошие приближения существуют при $\mathfrak{D} = -23$, $\mathfrak{D} = -44$, так что, в частности, диофантовы уравнения $x^3 + x^2y - y^3 = c$ и $x^3 + x^2y + xy^2 - y^3 = c$ эффективно разрешимы при любых целых c.

Среди полей с положительным дискриминантом оказывается эффективно разрешимым, в частности, уравнение $x^3 + x^2 y - 2xy^2 - y^3 = c$, с дискриминантом 49.

Литература

[I]. A. Baker. Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers. Quat. Journ. of Math. I964, I5, n 60, 327-336.

[2]. Делоне Б.Н. и Фаддеев Д.К. Теория иррациональностей третьей степени. Тр.Матем.инст.АН СССР, I940, 11, I-340.