Лекция 1. Уравнение Морделла, Теорема Морделла, Понятие кривых.

0.1 Уравнение Морделла.

Целые точки.

1. Примеры без решений

Чтобы доказать, что уравнение $y^2 = x^3 + k$ не имеет целых решений для некотрых k, используется сравнения и квадратичные вычеты. В частности, используем следующее когда -1, 2 и -2 могут быть сравнимы с квадратами по модулю p:

$$-1 \equiv \square mod p \Leftrightarrow p \equiv 1 mod 4,$$

$$2 \equiv \square mod p \Leftrightarrow p \equiv 1, 7 mod 8,$$

$$-2 \equiv \square mod p \Leftrightarrow p \equiv 1, 3 mod 8$$

Рассмотрим теперь пример уравнения Морделла.

Теорема 0.1 *The equation $y^2 = x^3 + 7$ has no integral solutions.*

Доказательство:

Предположим, что целое решение (x, y) есть. Если x чётный, то $y^2 \equiv 7 mod 8$. Но $7 mod 8$ не эквивалентно квадрату. Перепишем наше уравнение

$$y^2 = x^3 + 7 \Rightarrow y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4)$$

Второй сомножитель положителен как $(x - 1)^2 + 3$. Поскольку x нечётно, то $(x - 1)^2 + 3 \equiv 3 mod 4$. Значит в его разложении на простые есть хотя бы один сомножитель, который делится на нечётное простое вида $p \equiv 3 mod 4$. Поскольку $p | x^2 - 2x + 4$, то $p | y^2 + 1$. Значит, $-1 \equiv \square mod p$, что противоречит тому, что $p \equiv 3 mod 4$. Этот метод называется методом Лебега.

Есть и другой подход, рассмотрим первый сомножитель $x + 2$, так как x начётное, а y чётное, то, используя сравнение $x^3 \equiv x mod 4$, получаем, что $0 \equiv x + 3 mod 4$. Значит, $x \equiv 1 mod 4$, поэтому $x + 2 \equiv 3 mod 4$. Более того, $x + 2 > 0$, так как иначе $x^3 + 7 < -1$, что противоречит тому, что это полный квадрат. Если оно положительно и имеет остаток 3 по модулю 4, то в его разложении на простые есть простое с этим свойством, значит, опять $-1 \equiv \square mod p$. $\square$

Уравнение $y^2 = x^3 - 6$ использует сравнение $2 \equiv \square mod p \Leftrightarrow p \equiv 1, 7 mod 8$.

2. С конечным числом решений.

Посмотрим теперь на уравнение Морделла, у которого есть целочисленные решения. Основной инструмент это разложение на простые, однако, тут есть свои сложности, о которых мы тоже поговорим.

Теорема 0.2 *Уравнение $y^2 = x^3 + 16$ имеет два целых решения: (0, 4) и (0, -4).*

Для начала определим чётность целых решений. Запишем наше уравнение в следующем виде $x^3 = (y-4)(y+4)$. Если y нечётно, то $(y+4, y-4) = 1$, так как не может быть общих делителей. Значит, оба сомножителя являются кубами. Они отличаются на 8, но такого не бывает. Поэтому y чётно. Тогда и x чётно.

Правая часть $y^2 = x^3 + 16$ делится на 8, значит 4 делит y. Запишем $y = 4y'$, тогда $4|x$. Снова запишем $x = 4x'$, значит $y'^2 = x'^3 + 1$, поэтому y' нечётно. Запишем $y' = 2m + 1$ и получим $m^2 + m = x'^3$. Так как $m^2 + m = m(m+1)$ и $(m, m+1) = 1$, то и m, и $m+1$ являются кубами. А последовательными кубами являются только -1, 0, 1, поэтому одно из этих чисел ноль, тем самым x тоже ноль, а $y = \pm 4$.

Также часто используется факторизация в $Z[i]$ и $Z[\sqrt{-2}]$.

Теорема 0.3 *Единственные целые, удовлетворяющие уравнению $y^2 = x^3 - 1$ это пара (1,0).*

Опять же в начале выясним чётность решений. Пусть x чётно, тогда $y^2 + 1$ делится на 8, но квадрат целого не может иметь остаток -1 при делении на 8, следовательно, x нечётно, а y чётно.

Запишем

$$x^3 = y^2 + 1,$$

в $Z[i]$ есть разложение

$$x^3 = (y+i)(y-i).$$

Если два сомножителя справа взаимно просты в $Z[i]$, тогда они оба кубы с точностью до умножения на элемент единичной нормы. Более того, в $Z[i]$ все единицы являются кубами ($1 = 1^3$, $-1 = (-1)^3$, $i = (-i)^3$, $-i = i^3$), поэтому их можно занести в кубы. Тогда заметив, что $y+i$ и $y-i$ взаимно просты, получаем, что они сами кубы.

Упражнение: Покажите, что $y+i$ и $y-i$ взаимно просты. *Подсказка:* использовать норму

Запишем

$$y + i = (m + ni)^3$$

Раскроем куб и разделим на вещественную и мнимую часть:

$$y = m(m^2 - 3n^2), \quad 1 = n(3m^2 - n^2)$$

Значит, $n = \pm 1$.

Если $n = 1$, то $3m^2 = 2$. Нет целых. Если $n = -1$, то $m = 0$. Значит $y = 0$ и $x = 1$.

Теорема 0.4 *Единственные целые, удовлетворяющие уравнению* $y^2 = x^3 - 2$ *это пара (3,*$\pm$*5).*

Пусть у нас есть целое решение. Замечаем, что x нечётное, тогда и y тоже нечётное. Запишем уравнение как

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2})$$

Два сомножителя в правой части взаимно просты в кольце $Z[\sqrt{-2}]$. Действительно, пусть у них есть общий делитель, скажем ϵ, тогда ϵ делит их разность, т.е. $2\sqrt{-2}$. Поэтому $N(\epsilon)$ делит 8 с одной стороны, а с другой стороны, делит $y^2 + 2$, но оно нечётно. Значит, ϵ единица. Аналогично предыдущему, оба сомножителя кубы (с точностью до единиц). Единицы там ± 1. Снова запишем $y + \sqrt{-2} = (m + n\sqrt{-2})^3$. Получаем $n = \pm 1$. И рассматривая два случая, получаем искомое.

Замечание 0.5 *Не во всех кольцах есть однозначное разложение на множители. Напрмиер, его нет в* $Z[\sqrt{-3}]$.

Рассмотрим теперь уравнение $y^2 = x^3 + 1$, есть очевидные решения (-1,0), (0, $\pm$ 1), (2, $\pm$ 3).

Запишем, $x^3 = (y + 1)(y - 1)$. Легко видеть, что $(y - 1, y + 1) = 1$ или 2. Если y чётно, то тогда оба сомножителя кубы, отличающиеся на 2, получаем решение (-1, 0).

Если же y нечётно, то $(y-1, y+1) = 2$. Так как изменение знака y оставляет пару решением, то можно считать, что $y \equiv 1 mod 4$. Тогда $(\frac{x}{2})^3 = \frac{y+1}{2} \cdot \frac{y-1}{4}$. Аналогично предыдущему получаем, что оба сомножителя кубы

$$\frac{y+1}{2} = a^3, \quad \frac{y-1}{4} = b^3$$

и $a^3 - 2b^3 = 1$. Есть решения (1,0) и (-1,-1). Но непросто показать, что других решений нет. И вообще, что их конечно.

Замечание 0.6 *Уравнение вида* $a^3 - 2b^3 = 1$ *является частным случаем уравнения Туя, о котором речь пойдёт ниже (и в последней лекции). Для конкретного случая не так сложно, запишем*

$$x/y - \sqrt[3]{2} = 1/(y(x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2)$$

Но для больших $|y|$ *выражение справа доминируется кратным* $1/|y|^3$*, так что если у этого уравнения бесконечно много решений, то это противоречит неравенству Туе*

$$|p/q - \alpha| < c/|q|^\kappa$$

Сводная таблица ниже:

k	$\mathbf{Z}$-solutions of $y^2 = x^3 + k$
1	$(-1,0), (0,\pm 1), (2,\pm 3)$
-1	$(1,0)$
-2	$(3,\pm 5)$
-4	$(2,\pm 2), (5,\pm 11)$
-5	None
6	None
-6	None
7	None
16	$(0,4), (0,-4)$
-24	None
-26	$(3,\pm 1), (35,\pm 207)$
45	None
46	None

Рациональные точки.

k	$\mathbf{Q}$-solutions of $y^2 = x^3 + k$
1	$(-1,0), (0,\pm 1), (2,\pm 3)$
-1	$(1,0)$
-2	Infinitely many
-4	Infinitely many
-5	None
6	None
-6	None
7	None
16	$(0,4), (0,-4)$
-24	None
-26	Infinitely many
45	None
46	Infinitely many

Пример: Рассмотрим уравнение $y^2 = x^3 + 16$, целые решения мы изучили (0,± 4). Оказывается, больше рациональных нет, кроме тех, что являются целыми. Зато заметим, что если $a^3 + b^3 = c^3$ с ненулевыми целыми, то $x = 4bc/a^2$ и $y = 4(a^3 + 2b^3)/a^3$ удовлетворяют $y^2 = x^3 + 16$. Т.е. $x = 0$, тем самым следует теорема Ферма для показателя три.

0.2 Теорема Морделла и уравнение Туе

Теорема 0.7 *(Mordell, 1922) Для заданного $d \neq 0$ уравнение $y^2 + d = x^3$ имеет конечное число целых решений.*

Теорема 0.8 *Для заданного $d \neq 0$ уравнение $y^2 + d = x^3$ сводится к решению конечного числа уравнений вида $f(x, y) = 1$, где f- бинарная кубическая форма с целыми коэффициентами. Более того, набор таких форм может быть задан явно.*

Бинарные формы

Бинарная форма — многочлен от двух переменных, общий вид такой формы степени n

$$a_n X^n + a_{n-1} X^{n-1} Y + ... + a_0 Y^n$$

Эквивалентность: две бинарные формы называются эквивалентными, если существуют такие p, q, r, s с $ps - qr = 1$, что $g(X, Y) = f(pX + qY, rX + sY)$.

Важным инвариантом форм являются такие многочлены, зависящие от коэффициентов форм, которые сохраняются под действием преобразований эквивалентности.

Наиболее распространённый пример, дискриминант формы, заданный как

$$D = a_n^{2n-2} \prod_{i>j} (\alpha_i - \alpha_j)^2,$$

где α_i — корни многочлена $f(x, 1)$. Можно показать, что у этого многочлена целые коэффициенты.

У бинарной квадратичной формы $aX^2 + 2bXY + cY^2$ дискриминант $D = 4(b^2 - ac)$. У бинарной кубической формы $aX^3 + 3bX^2Y + 3cXY^2 + dY^3$ дискриминант $D = 27(-a^2d^2 + 6abcd + 3b^2c^2 - 4ac^3 - 4db^3)$. Это единственные инварианты для квадратичной и кубической форм. Для тетрарной формы их уже два

$$I_2 = a_0 a_4 - 4a_1 a3 + 3a_2^2$$

$$I_3 = a_0 a_2 a_4 - a_0 a_3^2 - a_1^2 a_4 + 2a_1 a_2 a_3 - a_2^3$$

и дискриминант $D = 27(I_2^2 - 27I_3^3)$.

Теорема 0.9 *Число классов эквивалентности бинарных целых форм заданной степени и дискриминанта конечно.*

Перейдём к рассмотрению кубических форм
$f(X, Y) = aX^3 + 3bX^2Y + 3cXY^2 + dY^3$. Построим форму, которая называется, гессиан

$$H(X, Y) = -\frac{1}{36}(f_{xx} f_{yy} - f_{xy} f_{yx}) = (b^2 - ac)x^2 + (bc - ad)xy + (c^2 - bd)y^2$$

Определим также кубическую форму $G(x, y) = \frac{1}{3}(f_x H_y - f_y H_x)$.

Эти формы называются ковариантами
второй и третьей степени. Дискриминант $D = 27D_1$, где $D_1 = -a^2d^2 + 6abcd + 3b^2c^2 - 4ac^3 - 4db^3$. Заметим, что дискриминант H равен $-D_1$.

Предложение 0.10

$$G^2 + D_1 f^2 = 4H^3$$

Заметим теперь, что если f бинарная кубическая форма с $D_1 = 4k$, такая что $f(x_0, y_0) = 1$, то уравнение Морделла $y^2 + k = x^3$ имеет решение $y = G(x_0, y_0)/2, x = H(x_0, y_0)$. Обратное тоже верно.

Предложение 0.11 *Рассмотрим уравнение $y^2 + k = x^3$ и пусть оно имеет решение p, q. Тогда кубическая форма $f(x, y) = x^3 - 3pxy^2 + 2qy^3$ имеет $D_1 = 4k$ и $p = H(1, 0), q = G(1, 0)/2$. Более того, $H(X, Y) = pX^2 - 2qXY + p^2Y^2$, т.е. H чётная форма. Также, $G(X, Y) = 2(-qX^3 + 3p^2X^2Y - 3pqXY^2 + (-p^3 + 2q^2)Y^3)$, т.е. $G(X, Y)/2$ целая форма.*

Доказательство является прямой проверкой. Тем самым, чтобы решить уравнение Морделла достаточно найти элемент в каждом классе эквивалентности кубических форм с дискриминантом $108k$. Для каждой из них надо решить $f(x, y) = 1$. Это кубическое уравнение Туе. Теорема Туе утверждает, что у него конечное число решение, а, значит, их число конечно и у уравнения Морделла.

Уравнение Туе

Пусть F целая бинарная форма и m ненулевое целое. Уравнение

$$F(x, y) = m,$$

где $x, y \in Z$ называется уравнение Туе.

Теорема 0.12 *(Thue, 1909) Пусть F целая бинарная форма, такая что $F(x, 1)$ имеет не менее трёх различных нулей. Тогда уравнение $F(x, y) = m$ имеет конечное число решений.*

Обычно рассматривают однородные многочлены.

Доказательство этой теоремы основано на диофантовых приближениях и мы обсудим его уже в конце курса. Сейчас же мы рассмотрим более простой случай.

Рассмотрим уравнение вида $x^3 - by^3 = c$, где $b, c \in Z^*$ и b не является кубом целого. Можно считать, что коэффициенты положительны. Пусть $\beta = \sqrt[3]{b}$.

Запишем $(x - y\beta)(x^2 + xy\beta + y^2\beta^2) = c$.

Также заметим, $x^2 + xy\beta + y^2\beta^2 \geq \frac{3}{4}\beta^2 y^2$. Заметим, что мы имеем не более одного решения при $y = 0$.

Если $y \neq 0$, то

$$(x - y\beta) = \frac{c}{x^2 + xy\beta + y^2\beta^2} \leq \frac{c}{\frac{3}{4}\beta^2 y^2} = \frac{4c}{3\beta^2 y^2}$$

Используя положительность обеих частей, получаем

$$|\frac{x}{y} - \beta| \leq \frac{4c}{3\beta^2}|\frac{1}{y^3}|$$

Нам достаточно доказать, что число пар (x, y), удовлетворяющих неравенству выше конечно. Это следует из диофантовой аппроксимации. Мы вернёмся к нему позже.

Теорема Фуета

Теорема 0.13 *Рассмотрим уравнение Морделла $y^2 = x^3 + k$, если k не имеет шестых степеней в разложении на простые, не равно 1 или -432, а уравнение имеет рациональное решение (r, s), такое что $rs \neq 0$, то имеется бесконечно много рациональных решений.*

Идея как можно действовать:
Рассмотрим пару

$$x = r + z, \quad y = s + 3r^2 z/2s$$

Предположим, что (x, y) решение, тогда $z = 9r^4/4s^2 - 3r$.

Если $x = 0$, то получаем, что $k = t^6$, чего быть не может. Рассматривая редукцию по модулю 2^n также получаем, что $y \neq 0$. И так далее, если $k \neq 1$ или -432.