Проблема десятого дискриминанта.
Конспект лекции 2 ноября 2022

Теория комплексного умножения

Введение

Обсудим сначала общую стратегию решения Хегнера для проблемы десятого дискриминанта. Пусть D — фундаментальный дискриминант. Мы уже установили, что если $D > -8$ и $h(D) = 1$, то $-D$ обязано быть нечётным простым числом. Оказывается, если $h(D) = 1$, то число $j\left(\frac{-1+\sqrt{D}}{2}\right)$ является кубом целого числа, а $j(\sqrt{D})$ — целая кубическая иррациональность. Позднее мы построим ещё несколько модулярных форм, значения которых будут связаны с этой кубической иррациональностью и получим соотношения на коэффициенты некоторого кубического многочлена. Данное соотношение сведёт проблему десятого дискриминанта к некоторому конкретному диофантову уравнению.
В предыдущей лекции обсуждались свойства функции $j(\tau)$. Было показано, что она инвариантна относительно действия $SL_2(\mathbb{Z})$ и что поле модулярных функций относительно $SL_2(\mathbb{Z})$ есть $\mathbb{C}(j(\tau))$. Также было показано, что для мнимоквадратичной иррациональности τ число $j(\tau)$ является алгебраическим целым числом. С другой стороны, метод доказательства позволял оценить степень $j(\tau)$ довольно неточным образом. Основная цель данной лекции — исправить это обстоятельство.

Теорема 1. *Пусть K — мнимоквадратичное поле, $\mathcal{O}_K$ — его кольцо целых, а I — дробный идеал $\mathcal{O}_K$. Тогда $j(I)$ имеет степень не выше $h(K)$, где $h(K)$ — число классов K.*

Эллиптические функции

Пусть $L \subset \mathbb{C}$ — решётка полного ранга. Функция $f(z)$ называется эллиптической относительно L, если $f(z)$ мероморфна и L-периодична, то есть $f(z + l) = f(z)$ для любого $l \in L$. Зададим $\wp$-функцию Вейерштрасса формулой

$$\wp(z; L) = \frac{1}{z^2} + \sum_{l \in L \setminus \{0\}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right).$$

Несложно показать, что

(i) $\wp(z; L)$ — чётная эллиптическая функция относительно L, все её полюсы находятся в точках L и имеют порядок 2

(ii) $\wp(z)$ удовлетворяет дифференциальному уравнению

$$\wp'(z; L)^2 = 4\wp(z; L)^3 - g_2(L)\wp(z; L) - g_3(L),$$

где

$$g_2(L) = 60 \sum_{l \in L \setminus \{0\}} l^{-4} \text{ и } g_3(L) = 140 \sum_{l \in L \setminus \{0\}} l^{-6}.$$

Чтобы доказать (i), заметим сначала, что при $R > 0$ для z с условием $|z| < R$, отделенных от элементов L, ряд, задающий $\wp(z; L)$ сходится абсолютно и равномерно (при больших $|l|$ каждое слагаемое есть $O(R|l|^{-3})$). С другой стороны, имеем

$$\wp'(z; L) = -2 \sum_{l \in L} \frac{1}{(z-l)^3},$$

так что $\wp'(z; L)$ — эллиптическая функция. Это означает, что для любого $l \in L$ функция $\wp(z + l; L) - \wp(z; L) = c(l)$ постоянна. Легко видеть, что $c : L \to \mathbb{C}$ — гомоморфизм. С другой стороны, если L порождена ω_1, ω_2, то $c(\omega_i) = 0$. Действительно, $\wp$ чётна и регулярна в точках $\pm\omega_i/2$, так что

$$c(\omega_i) = \wp(-\omega_i/2 + \omega_i; L) - \wp(-\omega_i/2; L) = \wp(\omega_i/2; L) - \wp(-\omega_i/2; L) = 0,$$

так что гомоморфизм c на самом деле тождественно равен нулю, что и требовалось доказать.
Для доказательства (ii) определим для всякого $r > 2$

$$G_r(L) = \sum_{l \in L \setminus \{0\}} l^{-r}.$$

Ясно, что $G_r(L) = 0$ для нечётных r. Кроме того, при $|x| < 1$

$$\frac{1}{(1-x)^2} = 1 + \sum_{n \geq 1} (n+1) x^n,$$

так что

$$\frac{1}{(z-l)^2} - \frac{1}{l^2} = \frac{1}{l^2} \left(\frac{1}{(1 - \frac{z}{l})^2} - 1 \right) = \sum_{n \geq 1} \frac{n+1}{l^{n+2}} z^n,$$

откуда

$$\wp(z) = \frac{1}{z^2} + \sum_{n \geq 1} (n+1) G_{n+2}(L) z^n = \frac{1}{z^2} + \sum_{n \geq 1} (2n+1) G_{2n+2}(L) z^{2n}.$$

В частности,

$$\wp(z) = \frac{1}{z^2} + O(z^2),$$

$$\wp(z)^3 = \frac{1}{z^6} + \frac{9G_4(L)}{z^2} + 15G_6(L) + O(z^2)$$

и

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24G_4(L)}{z^2} - 80G_6(L) + O(z^2).$$

Прямое вычисление показывает, что у функции $F(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4(L)\wp(z) + 140G_6(L)$ разложение в ряд Лорана в точке $z = 0$ начинается

с $O(z^2)$. Таким образом, $F(z)$ — эллиптическая функция без полюсов и с нулём в точке $z = 0$. Это означает, что $F(z) = 0$. В самом деле, для любого z найдется точка z_0 в фундаментальном параллелограмме решётки L с условием $F(z) = F(z_0)$. С другой стороны, в силу голоморфности, образ фундаментального параллелограмма ограничен, так что F постоянна по теореме Лиувилля. Это и завершает доказательство пункта (ii). Пункт (ii) и сюръективность функции $\wp$ показывают, что мероморфное отображение $\mathbb{C} \to \mathbb{C}^2 : z \mapsto (\wp(z), \wp'(z))$ задает структуру эллиптической кривой на факторе $\mathbb{C}/L$.

Упражнение 1. *Докажите, что*

$$\wp(z+w) = -\wp(z) - \wp(w) + \frac{1}{4}\left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\right)^2$$

Заметим, что функция $\wp$ — однородная степени -2 как функция решётки L в том смысле, что для $\lambda \in \mathbb{C}$ выполнено равенство

$$\wp(\lambda z; \lambda L) = \lambda^{-2}\wp(z; L).$$

В частности, коэффициент $\wp$ при z^{2n} является модулярной формой веса $2n+2$. Зададим число $\Delta(L)$ как дискриминант многочлена в правой части уравнения (ii), то есть

$$\Delta(L) = g_2(L)^3 - 27g_3(L)^2 = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2,$$

где e_i — корни многочлена $4x^3 - g_2x - g_3$.

Утверждение 1. *Для любой решетки L выполнено $\Delta(L) \neq 0$.*

Доказательство. Заметим сначала, что если $\wp(z) = \wp(w)$, то $z \equiv \pm w \mod L$. В самом деле, если w лежит в L, то это тривиально, а если $w \notin L$, то функция $\frac{\wp'(z)}{\wp(z)-\wp(w)}$ эллиптическая. Выберем фундаментальный параллелограмм Π решётки L, на границе которого нет полюсов этой функции. В силу эллиптичности получаем

$$\int_{\partial\Pi} \frac{\wp'(z)}{\wp(z) - \wp(w)} dz = 0,$$

так что у функции $\wp(z) - \wp(w)$ есть ровно два нуля внутри Π. Если $2w \in L$, то $z = w$ является двойным нулем в силу чётности, а если $2w \notin L$, то $\pm w$ дают два различных нуля. (Рассматривая вместо $\wp(z) - \wp(w)$ функцию $\wp(z) - a$ для произвольного комплексного a, получаем также, что $\wp(z)$ сюръективна.) Далее, если $u \notin L$, но $2u \in L$, то $\wp'(u) = 0$, поскольку $\wp'(2u - z) = (-\wp(2u - z))' = -\wp'(z)$. Значит если L порождено ω_1, ω_2, то $\wp'(\omega_1/2) = \wp'(\omega_2/2) = \wp'((\omega_1 + \omega_2)/2) = 0$. Согласно уравнению (ii) получаем, что $\wp(\omega_1/2), \wp(\omega_2/2)$ и $\wp((\omega_1+\omega_2)/2)$ — различные корни интересующего нас полинома, откуда $\Delta(L) \neq 0$. □

Замечание 1. *Если $y > 0$ — вещественное число и $L_y = \langle 1, iy\rangle$, то $\Delta(L_y) \to 0$ при $y \to \infty$. В самом деле,*

$$g_2(L_y) \to 120\zeta(4) = \frac{4\pi^4}{3}, g_3(L_y) \to 280\zeta(6) = \frac{8\pi^6}{27},$$

так что

$$\Delta(L_y) \to \left(\frac{4\pi^4}{3}\right)^3 - 27\left(\frac{8\pi^6}{27}\right)^2 = 0.$$

Замечание 2. *Существуют многочлены $P_n \in \mathbb{Q}[x, y]$ такие, что $G_{2n}(L) = P_n(g_2, g_3)$. В самом деле,*

$$\wp'' = 6\wp^2 - \frac{g_2}{2},$$

откуда получается полиномиальная формула для G_{2n} в терминах G_{2k} для $k < n$.

Утверждение 2. *Решётки L и L' подобны (т.е. $L' = \lambda L$ для некоторого $\lambda \in \mathbb{C}$) тогда и только тогда, когда $j(L) = j(L')$.*

Доказательство. Если решётки подобны, то $j(L) = j(L')$ в силу того, что $g_2(\lambda L) = \lambda^{-4} g_2(L)$ и $g_3(\lambda L) = \lambda^{-6} g_3(L)$. Чтобы доказать обратное, будем ради простоты считать, что $g_2(L'), g_3(L') \neq 0$. Найдется такое λ, что

$$\lambda^4 = \frac{g_2(L)}{g_2(L')}.$$

Так как $j(L) = j(L')$, то $g_2(L) = \lambda^4 g_2(L')$ и $g_3(L) = \lambda^6 g_3(L')$, так что $g_2(\lambda L) = g_2(L')$ и $g_3(\lambda L) = g_3(L')$. Согласно замечанию 2, отсюда получаем $G_{2n}(L') = G_{2n}(\lambda L)$, откуда $\wp(z; \lambda L) = \wp(z; L')$, так что их множества полюсов совпадают и $\lambda L = L'$, что и требовалось. □

Утверждение 3. *Всякая эллиптическая функция является рациональной функцией от $\wp$ и $\wp'$, а чётные рациональные функции — рациональные функции от $\wp$.*

Доказательство. Пусть $f(z)$ — эллиптическая функция, полюсы которой внутри какого-нибудь фундаментального параллелограмма равны $p_1, \ldots, p_m$, а порядок полюса в p_i равен d_i. Умножим $f(z)$ на все $(\wp(z) - \wp(p_i))^{d_i}$, где $p_i \notin L$. Получится эллиптическая функция $F(z)$, все полюсы которой лежат в L. Вычитая из $F(z)$ функции, пропорциональные $\wp'(z)^a \wp(z)^b$, можно уменьшать порядок полюса, пока он не станет ≤ 1. Четная часть такой функции обязана быть постоянной, а нечетная часть имеет по крайней мере три неэквивалентных нуля $\omega_1/2, \omega_2/2, (\omega_1 + \omega_2)/2$, так что порядок полюса не может быть равен 1. В случае чётной функции $f(z)$ можно на втором шаге обойтись функциями вида $\wp(z)^b$, что и завершает доказательство. □

Комплексное умножение

Если $\alpha \in \mathbb{C}$, а L — решётка, то будем говорить, что L допускает умножение на α, если $\alpha L \subset L$. Множество $\mathcal{O}$ всех α, на которые допускает умножение L, называется кольцом комплексного умножения L (и, действительно, является кольцом). Более того, несложно показать, что $\mathcal{O}$ всегда является порядком в мнимоквадратичном поле (Упражнение: сделайте это.)
Докажем следующий факт

Теорема 2. *Пусть L — решетка, $\wp(z)$ — соответствующая функция Вейерштрасса, $\alpha \in \mathbb{C}$. Следующие условия эквивалентны*

(i) $\wp(\alpha z) \in \mathbb{C}(\wp(z))$.

(ii) $\alpha L \subset L$.

(iii) *Существует порядок $\mathcal{O}$ в мнимоквадратичном K такой, что $\alpha \in \mathcal{O}$ и L подобно дробному идеалу $\mathcal{O}$.*

Более того, тогда

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))}$$

и

$$\deg A = \deg B + 1 = [L : \alpha L] = N(\alpha).$$

Доказательство. Из первого условия следует второе. В самом деле, если $\wp(\alpha z) \in \mathbb{C}(\wp(z))$, то $\wp(\alpha z)$ — эллиптическая функция относительно L. Поскольку она имеет полюс в точке $z = 0$, то она также имеет полюсы во всех точках L, так что $\wp(z)$ имеет полюсы во всех точках αL, поэтому $\alpha L \subset L$.
Из второго условия первое следует очевидно: если $\alpha L \subset L$, то $\wp(z)$ эллиптическая относительно αL, так что $\wp(\alpha z)$ эллиптическая относительно L.
Из второго условия следует третье: приведем L к виду $\langle 1, \tau \rangle$. Так как $\alpha L \subset L$, то $\alpha = a + b\tau$ и $\alpha\tau = c + d\tau$, откуда получается квадратичное уравнение для τ. Поле $K = \mathbb{Q}(\tau)$ мнимоквадратично, кольцо $\mathcal{O}$ комплексного умножения L лежит в нём, а L — его дробный идеал.
Наконец, пусть $\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))}$, где A и B — взаимно простые полиномы. Разность степеней A и B равна 1: для этого достаточно сравнить порядки полюса в $z = 0$. Выберем $z \in \mathbb{C}$ такое, что $2z \notin \frac{1}{\alpha}L$ и многочлен $A(x) - \wp(\alpha z)B(x) \in \mathbb{C}[x]$ не имеет кратных корней. Пусть w_i — представители $\frac{1}{\alpha}L/L$. Числа $\wp(z + w_i)$ различны, поскольку иначе либо $w_i \equiv w_j \mod L$ для некоторых $i \neq j$ или $z - w_i \equiv -(z - w_j) \mod L$, то есть $2z \equiv -w_i - w_j \in \frac{1}{\alpha}L$. Все эти числа являются корнями $A(x) - \wp(\alpha z)B(x)$, а никаких других корней нет: если $u = \wp(w)$ — корень, то $\wp(\alpha w) = \wp(\alpha z)$. Таким образом, степень $A(x)$ равна степени $A(x) - \wp(\alpha z)B(x)$ и количеству w_i, то есть $[\frac{1}{\alpha}L : L] = [L : \alpha L] = N(\alpha)$. □

Количество классов подобия идеалов $\mathcal{O}$ равно $h(\mathcal{O})$.

Упражнение 2. *Докажите, что $j(i) = 1728$ и $j(\omega) = 0$.*

Пример 1. *Пусть* $\kappa = \frac{1+\sqrt{-7}}{2}$. *Тогда* $N(\kappa) = 2$. *Положим* $L = \langle 1, \kappa \rangle$. *Согласно Теореме 2,*

$$\wp(\kappa z; L) = \frac{A(\wp(z; L))}{B(\wp(z; L))},$$

где A *квадратичный, а* B *— линейный, то есть*

$$\wp(\kappa z) = a\wp(z) + b + \frac{1}{c\wp(z) + d}.$$

Приведем подобием решетку L *к такой решетке* L', *что* $g_2(L')/20 = g_3(L')/28 = g$ *для некоторого комплексного* g. *Тогда*

$$\wp(z; L') = \frac{1}{z^2} + gz^2 + gz^4 + \frac{g^2}{3}z^6 + \dots$$

и

$$\wp(\kappa z; L') = \frac{\kappa^{-2}}{z^2} + \kappa^2 g z^2 + \kappa^4 g z^3 + \frac{g^2\kappa^6}{3}z^6 + \dots$$

Поскольку $\wp(\kappa z) - a\wp(z) - b$ *обращается в* 0 *в точке* $z = 0$, *получаем* $a = \kappa^{-2}$ *и* $b = 0$. *Итак,*

$$g(\kappa^2 - \kappa^{-2})z^2 + g(\kappa^4 - \kappa^{-2})z^4 + g^2\left(\frac{\kappa^6 - \kappa^{-2}}{3}z^6\right) + O(z^8) = \wp(\kappa z) - \frac{\wp(z)}{\kappa^2} =$$

$$= \frac{1}{c\wp(z) + d}$$

Сравнивая коэффициенты при z^2, *получаем* $c = \frac{1}{g(\kappa^2 - \kappa^{-2})}$.
Наконец, сравнивая следующие коэффициенты получим

$$cg = -\frac{1}{3}\frac{\kappa^6 - \kappa^{-2}}{(\kappa^2 - \kappa^{-2})} + \frac{1}{g(\kappa^2 - \kappa^{-2})}\left(\frac{\kappa^6 - 1}{\kappa^4 - 1}\right)^2.$$

Решая уравнение, находим $g = \frac{7}{4}$, *откуда* $g_2 = 20g = 35$ *и* $g_3 = 28g = 49$. *Отсюда*

$$j(\kappa) = -3375 = -15^3.$$

Докажем теперь Теорему 1.

Доказательство Теоремы 1. Пусть I — идеал в $\mathcal{O}_K = \mathcal{O}$. Вспомним, что

$$\wp(z; I) = \frac{1}{z^2} + \sum_{n \geq 1} a_n(g_2, g_3) z^{2n},$$

где a_n — многочлен с рациональными коэффициентами. Пусть $\alpha \in \mathcal{O}$. Согласно Теореме 2,

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))}.$$

Будем рассматривать наше $\wp$ как формальный степенной ряд с комплексными коэффициентами $\wp(z; g_2, g_3)$. Имеем

$$\wp(\alpha z; g_2, g_3) = \frac{1}{\alpha^2 z^2} + \sum_n a_n(g_2, g_3)\alpha^{2n} z^{2n}.$$

Пусть σ — автоморфизм поля $\mathbb{C}$. Применяя его к нашему соотношению между $\wp(\alpha z)$ и $\wp(z)$, получаем

$$\wp(\sigma(\alpha)z; \sigma(g_2), \sigma(g_3)) = \frac{A^\sigma(\wp(z; \sigma(g_2), \sigma(g_3)}{B^\sigma(\wp(z; \sigma(g_2), \sigma(g_3)}.$$

Здесь для многочлена $P(x) = p_m x^m + \ldots + p_0$ мы положили $P^\sigma(x) = \sigma(p_m)x^m + \ldots + \sigma(p_0)$. Поскольку $\sigma(g_2)^3 - 27\sigma(g_3)^2 = \sigma(\Delta(I)) \neq 0$, то (упражнение) существует решётка L такая, что $g_2(L) = \sigma(g_2)$ и $g_3(L) = \sigma(g_3)$. Из написанного тождества автоматически следует, что $\sigma(\alpha)L \subset L$. Таким образом, если $\mathcal{O}'$ — кольцо комплексного умножения L, то $\sigma(\mathcal{O}) \subset \mathcal{O}'$. С другой стороны, $\mathcal{O} = \sigma(\mathcal{O})$ для любого автоморфизма σ, так что $\mathcal{O} \subset \mathcal{O}'$. Если поменять местами I и L и использовать σ^{-1} вместо σ, то получим обратное включение, так что кольцо комлпексного умножения L совпадает с $\mathcal{O}$. Значит, L подобно одному из $h(\mathcal{O})$ дробных идеалов $\mathcal{O}$. Поскольку $j(L) = \sigma(j(I))$, то комплексное число $j(I)$ имеет не более чем $h(\mathcal{O})$ сопряженных, что и завершает доказательство. $\square$