Семинар 12. Вокруг эллиптических кривых

Введение в теорию чисел, весенний семестр 2024 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Задача 1 (Последняя запись в дневнике Гаусса[1])**.** Пусть $a+bi$ — простое целое гауссово число, причём $a-1+bi$ делится на $2+2i$.

(а) Докажите, что $p := a^2+b^2$ — нечётное простое целое число.

(б) Найдите количество элементов в поле вычетов $\mathbb{Z}[i]/(a+bi)$.

(в) Покажите, что число a нечётно, и выразите его знак через $|a|$ и символ Лежандра $\left(\frac{2}{p}\right)$ с помощью явной формулы.

Задача 2 (Лемниската Бернулли)**.** На евклидовой плоскости даны точки F_1 и F_2. Определим кривую Λ как геометрическое множество точек P, таких что

$$PF_1 \cdot PF_2 = c^2,$$

где c — это половина расстояния между F_1 и F_2.

(а) Предъявите такую систему координат (в ортонормальном базисе), что Λ задаётся уравнением

$$(x^2+y^2)^2 = 2c^2(x^2-y^2).$$

(б) Пусть $2c^2 = 1$. Покажите, что длина дуги лемнискаты от начала координат O до точки на расстоянии r от O задаётся *эллиптическим интегралом*

$$\int_{t=0}^{r} R(t, \sqrt{f(t)})dt$$

для некоторой рациональной функции R от двух переменных и многочлена f степени не выше 4 от одной переменной.

(в) Проверьте, что плоская кривая, заданная уравнением $u^2 = f(t)$ имеет род один.

Задача 3. Покажите, что кривые $E_1 : u^2 = 1-t^4$ и $E_2 : y^2 = x^3+x$ бирационально эквивалентны над $\mathbb{C}$.

Задача 4. Эллиптическая кривая E над $\mathbb{Q}$ задана уравнением

$$y^2 = x^3 - 2.$$

В качестве нейтрального элемента $O \in E$ выбрана точка на бесконечности.

(а) Найдите дискриминант многочлена x^3-2.

(б) Для каких простых чисел p кривая $E(\mathbb{F}_p)$ имеет особенность? Какого типа эта особенность (самопересечение или касп)?

(в) Найдите количество точек на $E(\mathbb{F}_p)$ для $p=5$ и $p=7$.

(г) Найдите группу кручения $E_{tors}(\mathbb{Q})$ в группе всех рациональных точек $E(\mathbb{Q})$.

---

[1] Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta, si $a+bi$ est numerus primus, $a-1+bi$ per $2+2i$ divisibilis, multitudo omnium solutionum congruentiae $1 = xx+yy+xxyy \pmod{a+bi}$ inclusis $x=\infty, y=\pm i$, $x=\pm i, y=\infty$ fit $=(a-1)^2+bb$.