# Эллиптические кривые над конечным полем

**Задача 1 (эллиптические кривые над маленькими полями).**
$a^\circ$) Опишите все неизоморфные эллиптические кривые над полем $\mathbb{F}_2$.
*Подсказка: чтобы показать, что кривые не изоморфны, можно посмотреть на $j$-инвариант и посчитать количество точек на них.*
b) Какие из полученных в предыдущем пункте кривых становятся изоморфными над $\mathbb{F}_4$? Над $\mathbb{F}_{16}$? А над $\mathbb{F}_{256}$?
c) Посчитайте группы автоморфизмов кривых из предыдущего пункта над полями $\mathbb{F}_{2^k}$, $k \in \mathbb{N}$.
d) Опишите все различные (т. е. неизоморфные) кривые над $\mathbb{F}_4$. Какие у них $j$-инварианты? Какие из них становятся изоморфными над $\mathbb{F}_{16}$?
e) Ответьте на аналогичные вопросы про кривые над $\mathbb{F}_3$ и $\mathbb{F}_5$. Опишите группы точек получившихся кривых.

**Задача 2°.** Пусть $E/\mathbb{F}_q$ — эллиптическая кривая, для $n \geq 1$ положим $a_n = q^n + 1 - \#E(\mathbb{F}_{q^n})$, а также $a_0 = 2$. Докажите, что $a_{n+2} = a_1 a_{n+1} - q a_n$ для всех $n \geq 0$.

**Задача 3°.** Докажите, что для эллиптической кривой $E\colon y^2 = x^3 + x$ над полем $\mathbb{F}_p$ имеет место $\#E(\mathbb{F}_p) \equiv 0 \mod 4$ для всех $p > 2$.

**Задача 4.** Пусть $E/\mathbb{F}_q$ — эллиптическая кривая и пусть $m \geq 1$ — такое целое число, что $q-1$ и $m$ взаимно просты. Пусть, далее, $P \in E(\mathbb{F}_q)$ — точка в точности порядка $m$ и $d$ — такое целое число, что $q^d \equiv 1 \mod m$. Докажите, что $E[m] \subset E(\mathbb{F}_{q^d})$.
*Подсказка: заметьте, что $\mu_m \subset \mathbb{F}_{q^d}$ и используйте спаривание Вейля для изучения действия отображения Фробениуса на базис $E[m]$.*

**Задача 5.** Пусть $E/\mathbb{F}_q$ — эллиптическая кривая.
a) Докажите, что найдутся такие натуральные числа $n$ и $m$, $(m, q) = 1$, что $E(\mathbb{F}_q) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/nm\mathbb{Z}$.
b) Покажите, что $q \equiv 1 \mod m$.
c) Пусть $p \geq 5$ и $E$ суперсингулярна. Проверьте, что либо $m = 1$, либо $m = 2$ и, если $p \equiv 1 \mod 4$, то $m = 1$.

**Задача 6 (суперсингулярные эллиптические кривые).** Пусть $E/\mathbb{F}_q$ — эллиптическая кривая, $\phi\colon E \longrightarrow E$ — эндоморфизм Фробениуса возведения в степень $q$, $p = \operatorname{char} \mathbb{F}_q$.
a) Докажите, что $E$ суперсингулярна тогда и только тогда, когда $\operatorname{tr}(\phi) \equiv 0 \mod p$ (след $\phi$ вычисляется в $\operatorname{End}(T_l(E))$ для любого простого $l \neq p$).
b) Предположим, что $q = p \geq 5$ — простое. Докажите, что $E$ суперсингулярна тогда и только тогда, когда $\#E(\mathbb{F}_p) = p + 1$.
c) Выпишите все эллиптические кривые $E$ над $\mathbb{F}_2$ и $\mathbb{F}_3$ и убедитесь, что утверждение пункта (b) не верно при $p = 2, 3$.
d) Пусть опять $q = p \geq 5$ — простое, а $n \geq 1$ — целое число. Докажите, что

$$\#E(\mathbb{F}_{p^n}) = \begin{cases} p^n + 1, & \text{если } n \text{ нечётно}, \\ (p^{n/2} - (-1)^{n/2})^2, & \text{если } n \text{ чётно}. \end{cases}$$

e) Пусть $p^i$ — наибольшая степень $p$ такая, что $p^{2i} \mid q$. Докажите, что $\operatorname{tr}(\phi) \equiv 0 \mod p$ тогда и только тогда, когда $\operatorname{tr}(\phi) \equiv 0 \mod p^i$.
f) Докажите, что не существует таких эллиптических кривых $E/\mathbb{F}_8$, что $\#E(\mathbb{F}_8) = 7$ или $\#E(\mathbb{F}_8) = 11$.
*Подсказка: воспользуйтесь предыдущим пунктом.*

g) Пусть $E/K$ — эллиптическая кривая над полем характеристики 2. Докажите, что $E$ суперсингулярна тогда и только тогда, когда $j(E) = 0$.

**Задача 7.** Пусть $E/\mathbb{Q}$ — эллиптическая кривая. Зафиксируем уравнение Вейерштрасса для $E$ с коэффициентами в $\mathbb{Z}$. Докажите, что существует бесконечно много простых $p \in \mathbb{Z}$, для которых редуцированная кривая $E/\mathbb{F}_p$ не суперсингулярна.

*Подсказка: Зафиксируйте простое $l$ и рассмотрите те простые $p$, которые полностью распадаются в поле $\mathbb{Q}(E[l])$, полученном присоединением к $\mathbb{Q}$ координат всех точек $l$-кручения $E$. Далее воспользуйтесь предыдущей задачей.*

**Задача 8.** Пусть $E/\mathbb{F}_{p^2}$ — суперсингулярная эллиптическая кривая.

a) Докажите, что отображение умножения на $p$ может быть записано как

$$[p](x,y) = \Big(g(x^{p^2}, y^{p^2}), h(x^{p^2}, y^{p^2})\Big)$$

с рациональными функциями $g, h \in \mathbb{F}_{p^2}(X, Y)$.

b) Докажите, что $g$ и $h$ — полиномы, т.е. $g, h \in \mathbb{F}_{p^2}[X, Y]$.

c) Предположим, что $p \geq 3$ и возьмём уравнение Вейерштрасса для $E$ с $a_1 = a_3 = 0$. Докажите, что $g = X$ и $h = \pm Y$.

d) Предположим, что $p \geq 5$ и что $E$ определена над $\mathbb{F}_p$. Докажите, что $h = -Y$. Пусть $\phi\colon E \longrightarrow E$ — отображение Фробениуса возведения в степень $p$ на $E$. Докажите, что $\phi^2 = [-p]$ и $\hat{\phi} = -\phi$.

**Задача 9 (масс-формулы).** a) Покажите, что над конечным полем существует в точности две неизоморфных эллиптических кривых с заданным $j$-инвариантом $\neq 0, 1728$.

*Подсказка: можно для простоты считать, что характеристика поля $\neq 2, 3$.*

b) Пусть $p \neq 2, 3, q = p^r$ Докажите, что $\sum_{E/\mathbb{F}_q} \frac{1}{\#\mathrm{Aut}(E)} = q$.

*Подсказка: посмотрите на множество орбит при действии $\mathbb{F}_q^\times$ на $\mathcal{E}_q = \mathbb{F}_q^2 \setminus \{(a,b) \mid a^3 - 27b^2 = 0\}$, определённом формулой $(a,b) \mapsto (u^4 a, u^6 b)$.*

c) Посчитайте число классов изоморфизма эллиптических кривых над $\mathbb{F}_q$ при $p \neq 2, 3$.

d) Докажите формулу Эйхлера–Дойринга:

$$\sum_{\substack{E/\overline{\mathbb{F}}_p \\ \text{суперсингулярные}}} \frac{1}{\#\mathrm{Aut}(E)} = \frac{p-1}{24}.$$

**Задача 10*.** Пусть $\operatorname{char} K = p > 0$ и $E/K$ — эллиптическая кривая с $j(E) \notin \overline{\mathbb{F}}_p$. Докажите, что $\mathrm{End}(E) = \mathbb{Z}$.

*Подсказка: достаточно показать (кстати, почему?), что $End(E)$ не является порядком в мнимом квадратичном поле.*