Домашний экзамен за первый семестр

Задача 1. 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 2. Опишите все такие уравнения Вейерштрасса $E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, где $a_i \in \mathbb{Z}$ и $\Delta \neq 0$, что $E(\mathbb{Q})$ содержит точку кручения P с $x(P) \notin \mathbb{Z}$.

Задача 3. Посчитайте число классов изоморфизма эллиптических кривых над $\mathbb{F}_q$ при $\operatorname{char}\mathbb{F}_q \neq 2, 3$.

Задача 4. Пусть E/K — эллиптическая кривая с комплексным умножением над K, то есть такая, что $\operatorname{End}_K(E)$ строго больше, чем $\mathbb{Z}$. Докажите, что для всех простых $l \neq \operatorname{char} K$ действие $G_{\bar{K}/K}$ на модуле Тейта $T_l(E)$ абелево (т. е. образ $G_{\bar{K}/K}$ в $\mathrm{GL}_2(\mathbb{Q}_l)$ — коммутативная подгруппа).

Задача 5. Пусть $E = \mathbb{C}/\tau\mathbb{Z} + \mathbb{Z}$ — эллиптическая кривая, $P_1 = a + b\tau, P_2 = c + d\tau \in E[n]$ — две точки n-деления на E, $a, b, c, d \in \frac{1}{n}\mathbb{Z}$. Положим $e_n(P_1, P_2) = \exp(2\pi i(ad - bc)) \in \mu_n$. Докажите, что e_n с точностью до знака (т. е. e_n или e_n^{-1}) совпадает со спариванием Вейля.

Задача 6. a) Пусть $K/\mathbb{Q}$ — мнимое квадратичное поле, $\mathcal{O}$ — кольцо целых K и пусть $h_{\mathcal{O}}$ обозначает число классов идеалов $\mathcal{O}$. Докажите, что, если E — кривая с $\operatorname{End}(E) \cong \mathcal{O}$, то $j(E)$ алгебраично и степень расширения $[K(j(E))\colon K] \leq h_{\mathcal{O}}$.
b^*) Найдите $j(\mathbb{C}/\sqrt{-2}\mathbb{Z} + \mathbb{Z})$.