Формальные группы и эллиптические кривые над локальными полями

Задача 1°. Пусть $F(X,Y) \in R[[X,Y]]$ — такой степенной ряд, что $F(X,Y) = X + Y + \cdots$ (точками обозначены члены старшей степени по X или Y) и $F(X,F(Y,Z)) = F(F(X,Y),Z)$.

a) Покажите, что имеется единственный ряд $i(T) \in R[[T]]$ такой, что $F(T,i(T)) = 0$. Докажите, что $i(T)$ также удовлетворяет $F(i(T),T) = 0$.

b) Докажите, что $F(X,0) = X$ и $F(0,Y) = Y$.

Задача 2. a) Пусть $R = \mathbb{F}_p[\epsilon]/(\epsilon^2)$. Докажите, что $F(X,Y) = X + Y + \epsilon XY^p$ определяет некоммутативную формальную группу, т.е. F удовлетворяет всем свойствам формального группового закона, но $F(X,Y) \neq F(Y,X)$.

b^*) Пусть R — кольцо. Докажите, что некоммутативная формальная группа, определённая над R, существует тогда и только тогда, когда существует ненулевой элемент $\epsilon \in R$ и положительные целые числа m и n такие, что $m\epsilon = \epsilon^n = 0$.

Задача 3. Пусть R — кольцо целых в конечном расширении $\mathbb{Q}_p$, $\mathfrak{m}$ — максимальный идеал в R и пусть $\mathcal{F}/R$ — формальная группа.

a) Докажите, что для любого $x \in \mathcal{F}(\mathfrak{m})$ выполняется $\lim\limits_{n\to\infty} [p^n](x) = 0$.

b) Докажите, что для любого $\alpha \in \mathbb{Z}_p$ существует единственный гомоморфизм $[\alpha] : \mathcal{F} \longrightarrow \mathcal{F}$ такой, что $[\alpha](T) = \alpha T + \cdots \in R[[T]]$.

Задача 4. Пусть E — эллиптическая кривая $y^2 = x^3 + Ax$.

a°) Пусть $w(z) = \sum A_n z^n$ — разложение координаты w в ряд по координате z (см. лекции). Докажите, что $A_n = 0$ для всех $n \not\equiv 3 \mod 4$.

b°) Пусть $F(X,Y) = \sum F_n(X,Y)$ — формальный групповой закон для E, где $F_n(X,Y)$ — однородный многочлен степени n. Докажите, что $F_n = 0$ для всех $n \not\equiv 1 \mod 4$.

c) Докажите аналогичные результаты для кривой $y^2 = x^3 + B$.

Задача 5. Пусть R — кольцо характеристики p, $\mathcal{F}/R$ и $\mathcal{G}/R$ — формальные группы и пусть $f\colon \mathcal{F} \longrightarrow \mathcal{G}$ — гомоморфизм над R. Назовём высотой $\mathrm{ht}(f)$ такое наибольшее целое число h, что $f(T) = g(T^{p^h})$ для какого-то степенного ряда $g(T) \in R[[T]]$ (если $f = 0$, полагаем $\mathrm{ht}(f) = \infty$). Высотой формальной группы $\mathrm{ht}(\mathcal{F})$ называется высота отображения $[p]\colon \mathcal{F} \longrightarrow \mathcal{F}$ умножения на p.

a) Докажите, что, если $f'(0) = 0$, то $f(T) = f_1(T^p)$ для какого-то $f_1 \in R[[T]]$.

Подсказка: посмотрите на инвариантные дифференциалы.

b) Запишем $f(T) = g(T^{p^h})$ с $h = \mathrm{ht}(f)$. Тогда $g'(0) \neq 0$.

c) Пусть $\mathcal{F}/R, \mathcal{G}/R$ и $\mathcal{H}/R$ — формальные группы и пусть $\mathcal{F} \xrightarrow{f} \mathcal{G} \xrightarrow{g} \mathcal{H}$ — цепочка гомоморфизмов над R. Докажите, что $\mathrm{ht}(g \circ f) = \mathrm{ht}(f) + \mathrm{ht}(g)$.

d) Пусть K — поле характеристики $p > 0$, E_1/K и E_2/K — эллиптические кривые и $\phi\colon E_1 \longrightarrow E_2$ — ненулевая изогения, определённая над K. Далее, пусть $f\colon \hat{E}_1 \longrightarrow \hat{E}_2$ — гомоморфизм формальных групп, индуцированный ϕ. Докажите, что $\deg_i(\phi) = p^{\mathrm{ht}(f)}$.

e) Пусть E/K — эллиптическая кривая, определённая над полем положительной характеристики. Докажите, что $\mathrm{ht}(\hat{E}) = 1$ или 2. Когда $\mathrm{ht}(\hat{E}) = 2$ для кривой над конечным полем?

f) Пусть $k = R/\mathfrak{m}$ и h — высота формальной группы $\tilde{\mathcal{F}}/k$, полученной редукцией коэффициентов формального группового закона $F(X,Y)$ по модулю $\mathfrak{m}$. Предположим, что $x \in \mathcal{F}(\mathfrak{m})$ имеет порядок в точности p^{n+1}. Докажите, что $v(x) \leq \left\lceil \frac{v(p)}{p^{hn}(p^h-1)} \right\rceil$.

В следующих задачах K — поле дискретного нормирования, R — кольцо нормирования, $\mathfrak{m}$ — его максимальный идеал, $k = R/\mathfrak{m}$ — поле вычетов, v — дискретное нормирование.

Задача 6°. Предположим, что $\mathrm{char}\,(k) \neq 2, 3$.

a) Пусть E/K — эллиптическая кривая, заданная уравнением Вейерштрасса с коэффициентами $a_i \in R$. Докажите, что уравнение минимально тогда и только тогда, когда или $v(\Delta) < 12$, или $v(c_4) < 4$.

b) Пусть E/K задана минимальным уравнением Вейерштрасса вида $y^2 = x^3 + Ax + B$. Докажите, что E имеет

(i) хорошую редукцию $\Longleftrightarrow 4A^3 + 27B^2 \in R^\times$,

(ii) мультипликативную редукцию $\Longleftrightarrow 4A^3 + 27B^2 \in \mathfrak{m}$ и $AB \in R^\times$,

(iii) аддитивную редукцию $\Longleftrightarrow A \in \mathfrak{m}$ и $B \in \mathfrak{m}$.

Задача 7°. Пусть E/K — эллиптическая кривая с $j-$инвариантом $j(E) \in R$. Докажите, что для минимального дискриминанта E справедливо $v(\Delta) < 12 + 12v(2) + 6v(3)$.

Задача 8°. Опишите все 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 $\Delta \neq 0$, такие, что $E(\mathbb{Q})$ содержит точку кручения P с $x(P) \notin \mathbb{Z}$.

Задача 9. Пусть E/K — эллиптическая кривая, заданная минимальным уравнением Вейерштрасса. Для каждого $n \geq 1$ определим подмножество в $E(K)$ следующим образом: $E_n(K) = \{P \in E(K)\colon v(x(P)) \leq -2n\} \cup \{O\}$.

a) Докажите, что $E_n(K)$ — подгруппа в $E(K)$.

b) Докажите, что $E_n(K)/E_{n+1}(K) \cong k^+$.

Задача 10. Написав минимальное уравнение, покажите, что следующие эллиптические кривые имеют хорошие редукции над полями

a) $E\colon y^2 = x^3 + x$, $\quad \mathbb{Q}_2(\eta, i), \eta^8 = 2, i^2 = -1$.

b) $E\colon y^2 + y = x^3$, $\quad \mathbb{Q}_3(\pi, \eta), \pi^2 = \sqrt{-3}, \eta^3 = 2$.

c) $E\colon y^2 = x^3 + x^2 - 3x - 2$, $\quad \mathbb{Q}_5(\pi), \pi^4 = 5$.

Задача 11. Предположим, что K локально компактно в топологии, индуцированной дискретным нормированием v (это эквивалентно предположению, что поле вычетов k конечно). Цель этого упражнения — доказать, что $E(K)/E_0(K)$ в этом случае конечная группа (к сожалению, иногда требуется более сильное утверждение о том, что $E(K)/E_0(K)$ конечна, когда поле вычетов k алгебраически замкнуто).

a) Покажите, что $\mathbb{P}^N(K)$ компактно в топологии, заданной v.

b) Пусть E/K — эллиптическая кривая, $E(K) \subset \mathbb{P}^2(K)$. Снабдим $E(K)$ топологией, индуцированной с $\mathbb{P}^2(K)$. Докажите, что $E(K)$ — компакт и для любого $P \in E(K)$ отображение $\tau_P\colon E(K) \longrightarrow E(K)$ сдвига на P непрерывно.

c) Докажите, что $E_0(K)$ — открытое и замкнутое подмножество в $E(K)$.

d) Докажите, что $E(K)/E_0(K)$ конечно.

Задача 12. Пусть E/K — эллиптическая кривая, $E\colon y^2 = x^3 + Ax + B$.

a) Если $v(A) \geq 1$ и $v(B) = 1$, докажите, что $E(K) = E_0(K)$.

b) Если $v(A) = 1$ и $v(B) \geq 2$, докажите, что $E(K)/E_0(K) \cong \mathbb{Z}/2\mathbb{Z}$.

Подсказка: предположите, что $P, Q \notin E_0(K)$. Используя формулу сложения, покажите, что $P + Q \in E_0(K)$.

c) Если $v(A) \geq 2$ и $v(B) = 2$, докажите, что $E(K)/E_0(K)$ либо 0, либо $\mathbb{Z}/3\mathbb{Z}$.

Задача 13. Пусть $[K\colon \mathbb{Q}_p] = 2$ и E/K — эллиптическая кривая, заданная уравнением Вейерштрасса с коэффициентами из R. Пусть, далее, $P \in E(K)$ — такая точка порядка в точности $m \geq 2$, что $x(P) \notin R$, т.е. $v(x(P)) < 0$.

a) Докажите, что $p = 2$ или 3 и что $m = 2, 3$ или 4. Приведите примеры, чтобы показать, что каждое значение m принимается.

b) Предположим, что редуцированная кривая $\tilde{E}/k$ суперсингулярна. Докажите, что тогда $p = m = 2$.