Высоты и теорема Морделла–Вейля

Задача 1°. a) Пусть K — поле алгебраических чисел, M_K^0 (M_K^∞) — множество его неархимедовых (архимедовых) нормирований, E/K — эллиптическая кривая, $m \geq 2$ — целое число, Cl_K — группа классов идеалов K и $S = \{v \in M_K^0 \mid E$ имеет плохую редукцию в $v\} \cup \{v \in M_K^0 \mid v(m) \neq 0\} \cup M_K^\infty$. Предположим, что $E[m] \subset E(K)$. Докажите следующую количественную версию слабой теоремы Морделла–Вейля:

$$\mathrm{rk}_{\mathbb{Z}/m\mathbb{Z}}(E(K)/mE(K)) \leq 2|S| + 2\,\mathrm{rk}_{\mathbb{Z}/m\mathbb{Z}}(\mathrm{Cl}_K[m]).$$

b) Для каждого целого $d \geq 1$ рассмотрим эллиптическую кривую $E_d\colon y^2 = x^3 - d^2x$. Докажите, что $E_d(\mathbb{Q}) \cong E_d(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r$, где $r \leq 2\nu(2d)$ (здесь $\nu(N)$ обозначает число различных простых чисел, делящих N).

c) Найдите подгруппу кручения $E_d(\mathbb{Q})_{\mathrm{tors}}$ кривой E_d.

d^*) Покажите, что оценку на ранг E_d можно улучшить до $2\nu(2d) - 1$.

Задача 2. Пусть E/K — эллиптическая кривая и L/K — (бесконечное) алгебраическое расширение. Предположим, что ранг $E(M)$ ограничен, когда M пробегает все такие конечные расширения M/K, что M содержится в L.

a) Докажите, что $E(L) \otimes \mathbb{Q}$ — конечномерное векторное пространство над $\mathbb{Q}$.

b) Предположим, что L/K — расширение Галуа и $E_{tors}(L)$ конечна. Докажите, что $E(L)$ конечно порождена.

Задача 3. a) Покажите, что для любой эллиптической кривой $E/\mathbb{Q}_p$ и для любого $m \in \mathbb{Z}$ группа $E(\mathbb{Q}_p)/mE(\mathbb{Q}_p)$ конечна, но $E(\mathbb{Q}_p)$ не конечно порождена.

b) Докажите аналогичное утверждение для конечного расширения $K/\mathbb{Q}_p$.

Задача 4°. Пусть $x \in \bar{\mathbb{Q}}^\times$. Покажите, что $H(x) = 1$ тогда и только тогда, когда x — корень из единицы.

Задача 5. $a°$) Дайте явную оценку через N, C и d для числа точек в множестве

$$\left\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) \mid H(P) \leq C \text{ и } [\mathbb{Q}(P) : \mathbb{Q}] \leq d\right\}.$$

b) Пусть $\nu_K(N, C) = \#\left\{P \in \mathbb{P}^N(K) \mid H_K(P) \leq C\right\}$. Докажите, что $\lim\limits_{C\to\infty} \frac{\nu_{\mathbb{Q}}(N,C)}{C^{N+1}} = \frac{2^N}{\zeta(N+1)}$, где $\zeta(s)$ — дзета-функция Римана.

В общем случае асимптотика $\nu_K(N, C)$ даётся формулой Шануэла (см. С. Ленг “Основы диофантовой геометрии”)

Задача 6. Докажите следующие свойства функции высоты:

a) $H(x_1x_2 \ldots x_N) \leq H(x_1) \ldots H(x_N)$

b) $H(x_1 + x_2 + \ldots + x_N) \leq NH(x_1)H(x_2) \ldots H(x_N)$

c) Для $P = [x_0, \ldots x_N] \in \mathbb{P}^N(\bar{\mathbb{Q}})$ и $Q = [y_0, \ldots y_M] \in \mathbb{P}^M(\bar{\mathbb{Q}})$ определим

$$P * Q = [x_0y_0, x_0y_1, \ldots, x_iy_j, \ldots, x_Ny_M] \in \mathbb{P}^{MN+M+N}(\bar{\mathbb{Q}})$$

(вложение Сегре $\mathbb{P}^N \times \mathbb{P}^M$ в $\mathbb{P}^{MN+M+N}$). Докажите, что $H(P * Q) = H(P)H(Q)$.

d) Пусть $M = \binom{N+d}{N} - 1$ и пусть $f_0(X), \ldots f_M(X)$ — все различные мономы степени d от переменных $X_0, \ldots, X_N$. Для точки $P = [x_0, \ldots, x_N] \in \mathbb{P}^N(\bar{\mathbb{Q}})$ положим

$$P^{(d)} = [f_0(P), \ldots, f_M(P)] \in \mathbb{P}^M(\bar{\mathbb{Q}})$$

(отображение Веронезе из $\mathbb{P}^n$ в $\mathbb{P}^M$). Докажите, что $H(P^{(d)}) = H(P)^d = H([x_0^d, \ldots, x_N^d])$.

Задача 7. Пусть $x_0, \ldots, x_N \in K$ и $\mathfrak{b}$ — дробный идеал K, образованный $x_0, \ldots, x_N$. Докажите, что $H_K([x_0, \ldots, x_N]) = \left(N_{K/\mathbb{Q}}\mathfrak{b}\right)^{-1} \prod\limits_{v \in M_K^\infty} \max\limits_{0 \le i \le N} \{\|x_i\|_v\}$.

Задача 8°. Пусть F — рациональное отображение, $F\colon \mathbb{P}^2 \longrightarrow \mathbb{P}^2$, $[x, y, z] \longmapsto [x^2, xy, z^2]$ (F является морфизмом в каждой точке, кроме $[0, 1, 0]$, где оно не определено). Докажите, что существует бесконечно много таких точек $P \in \mathbb{P}^2(\mathbb{Q})$, что $H(F(P)) = H(P)$.

Задача 9 (вспомогательные утверждения о квадратичных формах). a) Пусть V — конечномерное вещественное векторное пространство и $L \subset V$ — решётка полного ранга. Пусть $q\colon V \longrightarrow \mathbb{R}$ — квадратичная форма и q обладает следующими свойствами:

(i) Если $P \in L$, то $q(P) = 0$ тогда и только тогда, когда $P = 0$.

(ii) Для любой константы C множество $\{P \in L \mid q(P) \le C\}$ конечно.

Докажите, что q положительно определена на V.
Подсказка: используйте теорему Минковского о выпуклом теле.

b) Покажите, что утверждение предыдущего пункта неверно, если отбросить требование (ii)

c) Пусть $f(x)$ — функция на группе A со значениями в поле характеристики $\neq 2$. Предположим, что $f(x + y) + f(x - y) = 2f(x) + 2f(y)$ для любых $x, y \in A$. Покажите, что $f(x) = B(x, x)$, где $B(x, y)$ — симметричная билинейная форма.
Подсказка: $B(x, y) = \frac{1}{2}(f(x + y) - f(x) - f(y))$, *достаточно проверить, что* $B(x + z, y) = B(x, y) + B(z, y)$.

Задача 10 (каноническая высота). Пусть K — поле алгебраических чисел, E/K — эллиптическая кривая.

a) Пусть $f \in K(E)$ — непостоянная чётная функция и $P \in E(\bar{K})$. Покажите, что предел $\hat{h}(P) = \frac{1}{\deg(f)} \lim\limits_{N \to \infty} 4^{-N} h_f\left([2^N]P\right)$ существует и не зависит от f. Этот предел называется *канонической высотой* на E.

b) Покажите, что для любых $P, Q \in E(\bar{K})$ имеем $\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q)$ (правило параллелограмма).

c) Выведите из предыдущего пункта, что $\hat{h}$ — квадратичная форма на $E(\bar{K})$. В частности, для всех $P \in E(\bar{K})$ и всех $m \in \mathbb{Z}$, выполнено $\hat{h}([m]P) = m^2\hat{h}(P)$.

d) Пусть $P \in E(\bar{K})$. Докажите, что $\hat{h}(P) \ge 0$ и $\hat{h}(P) = 0$ тогда и только тогда, когда P — точка кручения.

e) Пусть $f \in K(E)$ — чётная функция. Покажите, что $(\deg(f))\hat{h} = h_f + O(1)$, где $O(1)$ зависит от E и f.

f) Убедитесь, что, если $\hat{h}'\colon E(\bar{K}) \to \mathbb{R}$ — любая другая функция, удовлетворяющая (e) для какой-то непостоянной чётной функции f и при этом $\hat{h}'([m]P) = m^2\hat{h}'(P)$ для какого-то целого $m \ge 2$, то $\hat{h}' = \hat{h}$.

g) Покажите, что каноническая высота продолжается до положительно определённой квадратичной формы на вещественном векторном пространстве $E(K) \otimes \mathbb{R}$.

Таким образом, с любой эллиптической кривой связана решётка в $\mathbb{R}^{\mathrm{rk}E(K)}$. Её кообъём называется *регулятором* эллиптической кривой и является важным инвариантом группы K-рациональных точек.

Задача 11 (эффективные неравенства с высотами). Пусть E/K — эллиптическая кривая, задаваемая уравнением Вейерштрасса $y^2 = x^3 + Ax + B$.

a) Докажите, что существуют такие абсолютные константы c_1 и c_2, что для всех точек $P \in E(\bar{K})$ имеем $|h_x([2]P) - 4h_x(P)| \le c_1 h([A, B, 1]) + c_2$. Найдите явные значения c_1 и c_2.

b) Найдите такие абсолютные константы c_3 и c_4, что для всех точек $P \in E(\bar{K})$ имеем $\left|\frac{1}{2}h_x(P) - \hat{h}(P)\right| \leq c_3 h([A, B, 1]) + c_4$ ($\hat{h}$ — каноническая высота).

c) Докажите, что для любого целого $m \geq 1$ и любых точек $P, Q \in E(\bar{K})$ имеют место неравенства:

$$\left|h_x([m]P) - m^2 h_x(P)\right| \leq 2(m^2+1)(c_3 h([A, B, 1]) + c_4)$$

и

$$h_x(P+Q) \leq 2h_x(P) + 2h_x(Q) + 5(c_3 h\left([A, B, 1]\right) + c_4).$$

d) Пусть $Q_1, \ldots, Q_r \in E(K)$ — множество образующих $E(K)/2E(K)$. Найдите такие абсолютные константы c_5, c_6 и c_7, что множество точек $P \in E(K)$, удовлетворяющих

$$h_x(P) \leq c_5 \max_{1 \leq i \leq r} h_x(Q_i) + c_6 h\left([A, B, 1]\right) + c_7,$$

полностью содержит множество образующих $E(K)$.