# Эллиптические кривые

1. Обобщённая форма Вейерштрасса.

Вычисления в этом пункте основаны на теореме Римана-Роха. Пусть $X$ - гладкая кривая над полем $k$ рода $g$, $D$ - дивизор на $X$, определённый над $k$. Обозначим $L(D)$ линейное подпространство в $k(X)$, состоящее из рациональных функций $f$ таких, что $\mathrm{div}\,(f)+(D) \geq 0$, а через $|D|$ его проективизацию, находящуюся во взаимнооднозначном соответствии с множеством всех эффективных дивизоров, линейно эквивалентных $D$. $L(D)$ конечномерно, его размерность обозначим $l(D)$, она зависит только от класса линейной эквивалентности дивизора $D$. Пусть $K$ - канонический класс дивизоров (т.е. класс эквивалентности дивизора любого дифференциала на $X$ - последние образуют одномерное пространство над $k(X)$). Тогда
$l(D) - l(K - D) = 1 - g + \deg D$.

Лемма. 1) Если $\deg D \geq 2g - 1$, то $\dim |D| = \deg D - g$
2) Если $\deg D \geq 2g$, то $|D|$ не имеет базисных точек
3) Если $\deg D \geq 2g + 1$, то $|D|$ определяет регулярное вложение.

Действительно, из условия 1) следует, что $\deg(K-D) < 0$, а значит, в классе $(K-D)$ нет эффективных дивизоров (в этом случае дивизор $D$ называется неспециальным),. Если выполнено условие 2) и существует базисная точка $P$ (то есть все дивизоры из $|D|$ её содержат), то $L(D) = L(D - P)$, а это противоречит 1). Наконец, если выполнено 3), то $\forall P \in X$ никакая точка $Q$ не является базисной для линейной системы $|D - P|$, а следовательно, в $L(D)$ содержится функция, равная нулю в $P$, но не равная ему в $Q$, в частности, при $Q = P$ имеющая в $P$ нуль ровно первого порядка. Это означает, что степень морфизма, задаваемого линейной системой $|D|$, равна 1 и все точки образа простые.

Теорема - определение. Эллиптическая кривая $E$ задается одним из эквивалентных определений:
1) Неособая кривая степени 3 в $\mathbf{P}^2(k)$ вместе с точкой $O \in E(k)$.
2) То же, но при этом $O$ - точка перегиба.
3) Кривая $E$ в $\mathbf{P}^2(k)$ (при условии, что она неособа), заданная уравнением
$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$.
4) Неособая проективная кривая $E$ рода 1 вместе с точкой $O \in E(k)$.

Доказательство. 1) $\Rightarrow$ 4 следует из формулы присоединения для рода плоской кривой степени $d$: $g = \frac{(d-1)(d-2)}{2}$.
3) $\Rightarrow$ 2 очевидно (точка $0:1:0$ является точкой перегиба. На самом деле, если $\mathrm{char}\,(k) \neq 2$, то точки перегиба на кривой любой степени можно вычислить и непосредственно, добавляя к уравнению кривой $F(X,Y,Z) = 0$ условие равенства нулю гессиана - определителя, составленного из вторых частных производных $F$ по координатам. Для кривой степени 3 это условие также имеет степень 3, поэтому на ней есть 9 точек перегиба (можно проверить, что при $\mathrm{char}\,(k) \neq 3$ все они однократны), но при $k \neq \overline{k}$ они не обязательно определены над $k$.
4) $\Rightarrow$ 3. При $g = 1$ по теореме Римана-Роха $l(D) = \deg D$ для любого дивизора $D$. Поэтому $L(O)$ состоит из констант, $L(2(O)) = \langle 1, x\rangle$, $L(3(O)) = \langle 1, x, y\rangle$, при этом функции $x$ и $y$ имеют в $O$ полюса порядка, соответственно, 2 и 3. Поскольку $x^2$ имеет там полюс порядка 4, $x^2$ не может линейно выражаться через $1, x$ и $y$, поэтому $L(4(O)) = \langle 1, x, y, x^2\rangle$. Аналогично $L(5(O)) = \langle 1, x, y, x^2, xy\rangle$. Функции $1, x, y, x^2, xy, x^3, y^2$ все лежат в пространстве $L(6(O))$, размерность которого равна 6, поэтому они должны быть линейно зависимы, причем коэффициенты при $x^3$ и $y^2$ должны быть ненулевыми, так как только эти две функции имеют в $(O)$ полюс шестого порядка. Домножая при необходимости $x$ или $y$ на константу, мы получим (в неоднородной форме) уравнение из 3). По п.3 предыдущей леммы линейная система $|3(O)|$ определяет регулярное вложение $E \to \mathbf{P}^2(k)$, которое в координатах при $P \neq O$ задается формулой $P \to x(P) : y(P) : 1$, а точка $O$ переходит в $xt^3(O) : yt^3(O) : t(O)^3 = 0 : 1 : 0$, где $t$ - локальный параметр в $O$.

2. Групповой закон.

Мы будем пользоваться вариантом 4) определения. Пусть $P$ и $Q$ - не обязательно различные точки на $E$. Степень дивизора $D = (P) + (Q) - (O)$ равна 1, поэтому по п.1) леммы из предыдущего пункта $\dim |D| = 0$, а это означает, что существует единственный эффективный дивизор, линейно эквивалентный $D$. Поскольку $\deg D = 1$, этот дивизор имеет вид $(R)$, где $R$ - точка. Будем считать эту точку суммой точек $P$ и $Q$. Аналогично, точка $-P$ соответствует единственному эффективному дивизору в классе $2(O) - (P)$.

Отображение $P \to cl((P)-(O))$, которое ставит в соответствие точке $P$ класс линейной эквивалентности дивизора $(P)-(O)$, является биекцией множества точек на множество классов дивизоров степени 0. Действительно, дивизоры $(P)$ и $(Q)$ не могут лежать в одном классе эквивалентности по указанной лемме, а если $\deg D = 0$, то точка

$P$ такая, что $(P) \sim D + (O)$ однозначно восстанавливается по той же причине. Из определения в предыдущем абзаце сразу следует, что это отображение переводит сумму точек в сумму классов дивизоров, и поэтому операция суммирования определяет структуру абелевой группы на точках кривой $E$.

Теперь нужно доказать, что так определенный групповой закон является "алгебраическим". Для этого понадобится

Лемма. Пусть $P$ и $Q$ - точки на $E$ (возможно, совпадающие). Тогда существует алгебраическая инволюция $\sigma : E \to E$ такая, что $\sigma(P) = Q$ и при этом $\forall R \in E \;\; (R) + (\sigma(R)) \sim (P) + (Q)$.

Дейчтвительно, $\deg((P) + (Q)) = 2$, поэтому по п.2 леммы из предыдущего пункта линейная система $|(P)+(Q)|$ не имеет базисных точек и определяет морфизм $E \to \mathbf{P}^1$, который имеет степень 2 и сепарабелен, поскольку чисто несепарабельный морфизм не меняет род кривой. Сепарабельный морфизм степени 2 является накрытием Галуа, и в качестве $\sigma$ можно взять единственный элемент группы Галуа.

Теорема. Отображения $P, Q \to P + Q : E \times E \to E$ и $R \to -R : E \to E$ являются морфизмами.

Доказательство. По лемме, примененной к точкам $P = Q = O$, $(\sigma(R)) + (R) \sim 2(O)$, откуда $-R = \sigma(R)$. Далее нетрудно видеть, что при вложении $E \to \mathbf{P}^2$, определяемом линейной системой $|3(O)|$, точку $-P-Q$ можно вычислить, как третью точку пересечения кривой $E$ с прямой, проходящей через $P$ и $Q$. Действительно, дивизоры, получающиеся как пересечения различных прямых в $\mathbf{P}^2$ с кривой $E$, очевидно, линейно эквивалентны, а бесконечноудаленная прямая трехкратно пересекается с $E$ в точке $O$, поэтому если $R$ - искомая третья точка пересечения, то $(P) + (Q) + (R) \sim 3(O)$, а из этого следует, что $R = -P - Q$. Ясно, что координаты $R$ задаются рациональными функциями от координат $P$ и $Q$ и что рациональное отображение $(P, Q) \mapsto R$ всюду определено ■

Пример. Точки порядка 2. Точка $P$ имеет порядок $2 \Leftrightarrow 2(P) \sim 2(O)$. Следовательно, все точки порядка 2 являются точками ветвления сепарабельного морфизма $E \to \mathbf{P}^1$ степени 2, заданного линейной системой $|2(O)|$, который уже упоминался в лемме. По формуле Гурвица $2g(E) - 2 = 2(2g(\mathbf{P}^1) - 2) + \sum\limits_P \mathrm{v}_P(\mathcal{D}_P)$, где $P$ пробегает точки ветвления, а $\mathcal{D}_P$ - локальная дифферента. Если $\mathrm{char}\,(k) \neq 2$, то ветвление может быть только слабым, и в любой точке ветвления $\mathrm{v}_P(\mathcal{D}_P) = e_P - 1 = 1$, поэтому точек ветвления ровно 4, а значит, группа точек второго порядка $E_2(\overline{k})$ изоморфна $\mathbf{Z}/(2) \oplus \mathbf{Z}/(2)$ (координаты точек второго порядка не обязаны лежать в $k$).

Точки третьего порядка также просто описываются - это точки перегиба. При $\mathrm{char}\,(k) \neq 3$ их ровно 9, и $E_3(\overline{k}) \simeq \mathbf{Z}/(3) \oplus \mathbf{Z}/(3)$. Позже мы увидим, что аналогичное утверждение верно для группы точек любого порядка, не делящегося на $\mathrm{char}\,(k)$.

Справедливо также утверждение, отчасти обратное к доказанной выше теореме: если $f : (E, O) \to (E', O')$ - морфизм эллиптических кривых, переводящий $O$ в $O'$, то он является гомоморфизмом групп. Действительно, $P + Q = R \Rightarrow (P) + (Q) \sim (R) + (O) \Rightarrow (f(P)) + (f(Q)) \sim (f(R)) + (f(O)) \Rightarrow f(P) + f(Q) = f(R)$ (на самом деле тот факт, что морфизм переводит линейно эквивалентные дивизоры в линейно эквивалентные, не вполне очевиден, но мы опустим доказательство).

3. Эллиптические кривые над $\mathbf{C}$.

Пусть $L$ - решётка в $\mathbf{C}$. Определим $\wp$-функцию Вейрштрасса формулой
$\wp_L(z) = \sum\limits_{w \in L,\, w \neq 0} (\frac{1}{(z-w)^2} - \frac{1}{w^2}) + \frac{1}{z^2}$.
Элементарно проверяется, что ряд сходится абсолютно и равномерно на компактах, не содержащих точек решетки, и определяет инвариантную относительно сдвигов на векторы решётки мероморфную функцию, голоморфную вне точек решетки $L$. Её производная
$\wp'_L(z) = -2 \sum\limits_{w \in L} \frac{1}{(z-w)^3}$.
Разложение Лорана функции $\wp_L(z)$ в нуле имеет вид
$\wp_L(z) = \frac{1}{z^2} + \sum\limits_{k=1}^{\infty} (2k+1)\gamma_{2k+2}(L) z^{2k}$,
где $\gamma_n(L) \stackrel{\text{def}}{=} \sum\limits_{w \in L,\, w \neq 0} \frac{1}{w^n}$ (ряд сходится абсолютно при четных $n \geq 4$ и равен нулю при нечетных $n$; ср. с определением ряда Эйзенштейна). Соответственно,
$\wp'_L(z) = -\frac{2}{z^3} + \sum\limits_{k=1}^{\infty} 2k(2k+1)\gamma_{2k+2}(L) z^{2k-1}$
Функция $\wp_L(z)$ является четной, а $\wp'_L(z)$ нечетной.

С точностью до прибавления функций, обращающихся в 0 в $z = 0$, $\wp_L(z) = \frac{1}{z^2}$, $\wp_L(z)^3 = \frac{1}{z^6} + 9\gamma_4(L)\frac{1}{z^2} + 15\gamma_6(L)$, $\wp_L(z)'^2 = \frac{4}{z^6} - 24\gamma_4(L)\frac{1}{z^2} - 80\gamma_6(L)$.
Следовательно, функция $\wp'^2_L - 4\wp^3_L + 60\gamma_4(L)\wp_L + 140\gamma_6(L)$ инвариантна относительно сдвигов на векторы $L$, обращается в нуль при $z = 0$, а значит, и во всех точках $L$, и тем самым всюду голоморфна. Следовательно, она тождественно равна нулю, и мы видим, что функции $\wp_L$ и $\wp'_L$ связаны уравнением (оно называется уравнением

Вейерштрасса), которое является практически частным случаем уравнения из п.1 (в аффинной форме). Чтобы убедиться в том, что кривая, задаваемая этим уравнением, эллиптическая, достаточно проверить её невырожденность.

Пусть $g_2 = 60\gamma_4(L)$, а $g_3 = 140\gamma_6(L)$ (это традиционные обозначения). Кривая, в аффинной форме задаваемая уравнением $y^2 = 4x^3 - g_2x - g_3$, в бесконечной точке всегда невырождена, а на $\mathbf{C}^2$ не имеет особых точек тогда и только тогда, когда $\Delta \neq 0$, где $\Delta$ - дискриминант кубического полинома в правой части. $\Delta = g_2^3 - 27g_3^2 = 16\prod_{i\neq j}(e_i - e_j)^2$, а $e_i$ - корни полинома. Из предыдущего раздела мы знаем, что модулярная форма $\Delta(z)$ нигде не обращается в нуль. Решетка $L$ подобна решетке $\langle z, 1\rangle$ при некотором $z$, и наш дискриминант отличается от $\Delta(z)$ умножением на ненулевую константу.

Невырожденность кривой можно проверить и непосредственно.

Пусть $f$- эллиптическая функция (по определению, это означает, что $f$ - мероморфная функция на $\mathbf{C}$, инвариантная относительно сдвигов на векторы решетки $L$). Если $\Pi$ - фундаментальный параллелограмм $L$, граница которого не содержит нулей и полюсов $f$, то справедливы равенства:
1) $\sum_{P\in\Pi} ord_P f = 0$; 2) $\sum_{P\in\Pi} (ord_P f)P \equiv 0 \mod L$; 3) $\sum_{P\in\Pi} res_P f = 0$.
Доказательство сразу получается интегрированием по границе $\Pi$, соответственно, $d\log f$, $zd\log f$ и $df$.

Функция $\wp'_L$ имеет тройные полюса в точках $L$ и больше полюсов не имеет. Она $L$- инвариантна и нечетна и поэтому обращается в нуль в точках $w_1/2, w_2/2$ и $w_3/2 = (w_1 + w_2)/2)$, где $(w_1, w_2)$- какой-нибудь базис $L$. Из свойства 1) предыдущего абзаца следует, что все эти нули простые и больше нулей (по модулю $L$) у $\wp'_L$ нет. Далее, по определению $\wp_L(w_i/2) = e_i$, следовательно, функция $\wp_L(z) - e_i$ обращается в точке $z = w_i/2$ в нуль, причем этот нуль двойной (ибо $\wp'_L(w_i/2) = 0$), а значит, других нулей у этой функции нет (она мероморфна с двойными полюсами только в точках $L$). Это показывает, что все $e_i$ различны и ещё раз подтверждает невырожденность кривой.

Проведенные вычисления позволяют легко проверить, что поле эллиптических функций для решетки $L$ алгебраически порождается функциями $\wp_L$ и $\wp'_L$. Пусть $f$ - такая функция. Её можно представить в виде суммы чётной и нечетной, так что можно

считать, что $f$- четна, и достаточно проверить, что она есть рациональная дробь от $\wp_L$. Рассмотрим функцию $g(z) \stackrel{\text{def}}{=} \prod(\wp_L(z)_- \wp_L(u_i))^{m_i}$. Здесь точки $u_i$ пробегают полный набор представителей $\mod L$ нулей и полюсов функции $f$, но из каждой пары противоположных по знаку представителей выбирается только один, а если представитель лежит в $L$, то он вообще не учитывается. Показатели $m_i$ суть порядки $f$ в $u_i$, но при этом если $2u_i \in L$, то порядок считается с кратностью $1/2$. Легко видеть, что дивизоры функций $f$ и $g$ совпадают вне $L$, а значит, и с учетом точек $L$ тоже (поскольку дивизор функции должен иметь нулевую степень). Это означает, что поделив $f$ на $g$, мы получим эллиптическую функцию с нулевым дивизором, то есть константу.

Естественная проекция $\pi : \mathbf{C} \to E(\mathbf{C})$, где $E$ - эллиптическая кривая, построенная выше по решетке $L$, является сюръективным гомоморфизмом групп с ядром $L$. Действительно, при любом $c \in \mathbf{C}$ функция $\wp_L(z) - c$ имеет по модулю $L$ один или два нуля, в последнем случае нули имеют вид $z = u$ и $z = -u$, и они простые, так что нечетная функция $\wp'_L(z)$ принимает в них разные значения. Это доказывает, что отображение $\mathbf{C}/L \to E(\mathbf{C})$ взаимнооднозначно (0 при этом переходит в бесконечноудаленную точку $O$). Условие $P + Q = R$ на $E(\mathbf{C})$ эквивалентно условию $(P) + (Q) \sim (R) + (O)$, которое, в свою очередь, эквивалентно существованию эллиптической функции $f$ такой, что $\operatorname{div}(f) = (\pi^{-1}(P)) + (\pi^{-1}(Q)) - (\pi^{-1}(R) - (0)) \mod L$, и утверждение о гомоморфности теперь следует из свойства 2) тремя абзацами выше.

В заключение отметим, что на кривой $E$, заданной уравнением $y^2 = 4x^3 - g_2x - g_3$, $x$-координата суммы $P_3$ точек $P_1$ и $P_2$ задается уравнением $x_3 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_1-y_2}{x_1-x_2}\right)^2$ при $P_1 \neq P_2$ и уравнением $x_3 = -2x_1 + \frac{1}{4}\left(\frac{6x_1^2-g_3/2}{y_1}\right)^2$ при $P_1 = P_2$, а точка $-P$ получается из точки $P$ изменением знака $y$-координаты.

4. Изогении.

Пусть теперь $k$ - произвольное алгебраически замкнутое поле. Непостоянный морфизм эллиптических кривых $(E_1, O_1) \to (E_2, O_2)$ называется изогенией. Поскольку $E_1$ проективна, изогения является конечным накрытием, и согласно замечанию в конце п.2 она является гомоморфизмом групп.
Теорема. 1) Морфизм $[m]$ умножения на $m$ - изогения (т.е. $[m] \neq 0$).
2) $\operatorname{Hom}(E_1, E_2)$ - $\mathbf{Z}$-модуль без кручения.
3) $\operatorname{End} E$ - целостное кольцо характеристики 0.

Доказательство. 1) [2] сюръективно, так как точки второго порядка являются точками ветвления сепарабельного накрытия $E \to \mathbf{P}^1$, уже рассматривавшегося выше, а следовательно, их конечное число. Согласно примеру из п.2 при $\mathrm{char}\,(k) \neq 2$ существует нетривиальная точка второго порядка, поэтому $[m] \neq 0$ при нечетных $m$, а следовательно, и при любых. Если $\mathrm{char}\,(k) = 2$, то можно аналогичным образом использовать описание точек третьего порядка как точек перегиба.
2) Гомоморфизмы $E_1 \to E_2$ можно складывать, используя сложение на $E_2$. $m$-кратнвя сумма гомоморфизма $\phi$ с собой есть $[m] \circ \phi$, и она не равна 0, так как $[m]$ сюръективно. 3) аналогично; дополнительно можно заметить, что $\deg(\phi \circ \psi) = \deg \phi \deg \psi$ ■

Элементы $\mathrm{End}\, E$, отличные от $[m]$, называются комплексными умножениями. Терминология связана с кривыми $\mathbf{C}/L$, для которых комплексные умножения отвечают числам $c \in \mathbf{C}$ таким, что $cL \subset L$. Например, отвечающая решетке Гаусса $\langle i, 1\rangle$ кривая изоморфна кривой $y^2 = x^3 - x$, и умножение решетки на $i$ соответствует автоморфизму кривой, переводящему точку $(x, y)$ в $(-x, iy)$. Если кривая $E$ определена над полем $\mathbf{F}_q$, то $\mathrm{End}\, E$ всегда содержит комплексные умножения: позже мы проверим, что эндоморфизм Фробениуса $Fr_q$, возводящий координаты точек в $q$-ю степень, не совпадает ни с каким $[m]$.

Теперь мы установим связь между изогениями и их ядрами.
Теорема. 1) Пусть $\phi : E_1 \to E_2$ - изогения. Тогда $\forall Q \in E_2\ \#(\phi^{-1}(Q)) = \#(\ker \phi) = \deg_{sep}(\phi), \forall P \in E_1 e_P(\phi) = \deg_{insep}(\phi)$ и естественный гомоморфизм $\ker \phi \to \mathrm{Aut}\,(k(E_1)/k(E_2)$, соответствующий действию сдвигов на элементы ядра на рациональные функции на $E_1$, является изоморфизмом.
2) Если $\phi : E_1 \to E_2$ - сепарабельная изогения, $\psi : E_1 \to E_3$ - любая изогения, и $\ker \phi \subset \ker \psi$, то существует изогения $\lambda : E_2 \to E_3$ такая, что $\psi = \lambda \circ \phi$.
3) Пусть $\Phi \in E_1$ - конечная подгруппа. Тогда $\exists! E_2 \simeq E_1/\Phi$ и сепарабельная изогения $E_1 \to E_2$.
Доказательство. 1) В общей точке $Q \in E_2$ число прообразов равно $deg_{sep}(\phi)$, сдвиг показывает, что число прообразов постоянно. Сдвиги на элементы $\ker \phi$ являются изоморфизмами $E_1 \to E_1$ и действуют вдоль слоев $\phi$, поэтому все индексы ветвления одинаковы. Если сдвиг на элемент $t \in \ker \phi$ тождественно действует на функциях из $k(E_1)$, то $t = 0$, поэтому гомоморфизм из 1) - вложение. Но $\#(\mathrm{Aut}\,(k(E_1)/k(E_2)) = [k(E_1) : k(E_2)]_{sep} = \deg_{sep} \phi = \#(\ker \phi)$, значит, это изоморфизм.
2) Вложение $k(E_3) \to k(E_2)$ строится по теории Галуа, а изогения $\lambda$ восстанавливается по нему.
3) Как и в 2), по общей теории кривых однозначно строится конечный морфизм

$\phi : E \to C$, где кривая $C$ имеет поле функций $k(E)^{\Phi}$. Если $P \in E$, а $f \in k(C)$, то $\forall T \in E \ f(\phi(P+T) = f(\phi(T)$, а это означает, что $\phi(P+T) = \phi(T)$. Следовательно, любая точка кривой $C$ имеет не менее $\#(\Phi) = \deg \phi$ прообразов, и $\phi$ неразветвлен, после чего из формулы Гурвица следует, что $C$ - тоже эллиптическая кривая ■

По теореме Римана-Роха $k$-пространство $\Omega(E)$ регулярных дифференциалов на $E$ одномерно; пусть $\omega$ - его образующая. Например, для кривой в обобщенной форме Вейерштрасса $F(x,y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0$ можно положить $\omega = \frac{dx}{2y+a_1x+a_3} = \frac{dx}{F'_x} = -\frac{dy}{F'_y}$. Очевидно, что $\omega$ регулярен вне бесконечной точки $O$ (иначе кривая была бы особой), и без труда проверяется, что в $O$ он тоже регулярен.
Теорема. 1) $\omega$ инвариантен относительно сдвигов.
2) Группа $\mathrm{Hom}(E_1, E_2)$ линейно действует на $\Omega(E_2)$ при его отображении посредством $\omega \mapsto \phi^*\omega$ в $\Omega(E_1)$.
Доказательство. 1) В силу одномерности $\Omega(E)$ $t_P^*\omega = c(P)\omega$. Тогда $P \mapsto c(P)$ - рациональная функция на $E$, не имеющая нулей и полюсов, значит, это константа (равная 1, поскольку $c(O) = 1$).
2) Пусть $\phi_1$ и $\phi_2$ - две изогении $E_1 \to E_2$. Если $\phi_1 + \phi_2 = 0$, то достаточно проверить, что $[-1]^*_{E_2}\omega = -\omega$. Это проверяется непосредственно по форме Вейрештрасса, ибо $[-1](x,y) = (x, -y - a_1x - a_3)$. Так что, можно считать, что $\phi_1 + \phi_2$ - изогения. Пусть $\oplus$ - операция сложения на $E_2 \times E_2 \to E_2$, её действие на дифференциалах задается в общем виде формулой $\oplus^*\omega = f(P,Q)\omega' + g(P,Q)\omega''$, где $\omega'$ и $\omega''$ - 1-формы на $E_2 \times E_2$ вдоль координат. Если зафиксировать точку $Q = Q_0$, то ограничение $f(P,Q)\omega'$ формы $\oplus^*\omega$ на проходящую через эту точку первую координатную кривую будет равно $t_{Q_0}\omega' = \omega'$ (благодаря инвариантности дифференциала относительно сдвигов), а следовательно, $f(P,Q_0) = 1$. Поскольку это верно при любом выборе $Q_0$, функция $f(P,Q)$ тождественно равна 1 (и $g(P,Q) = 1$ аналогично), а значит, $\oplus^*\omega = \omega' + \omega''$ ■

Следствие. $[m]^*\omega = m\omega$. В частности, если $\mathrm{char}\,(k) \nmid m$, то $[m]$ - сепарабельный эндоморфизм.

Двойственная изогения.

Теорема. Пусть $\phi : E_1 \to E_2$ - изогения степени $m$. Тогда
1) $\exists!\ \hat{\phi} : E_2 \to E_1$ такая, что $\hat{\phi} \circ \phi = [m]_{E_1}$.
2) Как отображение групп $\hat{\phi}$ есть $E_2 \to \mathrm{Div}^{\,0}(E_2) \xrightarrow{\phi^*} \mathrm{Div}^{\,0}(E_1) \xrightarrow{\Sigma} E_1$
3) $\phi \circ \hat{\phi} = [m]_{E_2}$
4) Если $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\lambda} E_3$, то $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$

5) $\widehat{\phi+\psi} = \hat{\phi} + \hat{\psi}$
6) $\widehat{[m]} = [m]$, в частности, $\deg[m] = m^2$
7) $\deg\hat{\phi} = \deg\phi$
8) $\hat{\hat{\phi}} = \phi$
Доказательство. 1) Если $(\hat{\phi} - \hat{\phi}'))\circ\phi = 0$, то $\phi$ не может быть сюръективна, поэтому $\hat{\phi}$ единственна. По теореме о структуре несепарабельных расширений, примененной к полям функций, любая изогения есть композиция сепарабельной изогении и некоторой степени абсолютного Фробениуса $Fr_p$ (аналогичное утверждение верно для любого накрытия кривых). Если $\phi$ сепарабельна, то, поскольку $ker\phi \subset \ker[m]$, где $m = \deg\phi$, изогения $\hat{\phi}$ строится по п.2 теоремы о ядрах изогений, доказанной выше. Если $\mathrm{char}\,(k) = p$, то $[p] = \phi\circ Fr_p^e$, где $\phi$ сепарабельна, а $e \geq 1$ (так как $[p]$ несепарабельна), и можно положить $\widehat{Fr_p} \stackrel{\mathrm{def}}{=} \phi\circ Fr_p^{e-1}$.
2) Пусть $\phi(P) = Q \in E_2$ и $\psi$ - отображение из формулировки. Тогда
$\psi(Q) = (\deg_{insep}\phi)(\sum\limits_{T\in\phi^{-1}(Q)} T - \sum\limits_{T\in\phi^{-1}(O_2)} T = (\deg_{insep}\phi)\#(\phi^{-1}(Q))P = (\deg\phi)P$
3) $\phi\circ\hat{\phi}\circ\phi = \phi\circ[m] = [m]\circ\phi$ (будучи гомоморфизмом, $\phi$ коммутирует с $[m]$). Поскольку $\phi$ сюръективно, отсюда следует, что $\phi\circ\hat{\phi} = [m]$.
4) Очевидно из определения.
5) Двойственная изогения переводит точку на $E_2$ в сумму (с кратностями) её прообразов на $E_1$. Следовательно, необходимо доказать, что $\forall Q \in E_2 \sum\limits_{\phi(P)=Q} P + \sum\limits_{\psi(P)=Q} P = \sum\limits_{\phi(P)+\psi(P)=Q} P$ или, что то же самое, доказать, что дивизор $\sum\limits_{\phi(P)=Q}(P) + \sum\limits_{\psi(P)=Q}(P) - \sum\limits_{\phi(P)+\psi(P)=Q}(P) - (\deg\phi + \deg\psi - \deg(\phi+\psi))(O_{E_1})$ является дивизором рациональной функции на $E_1$. Для этого рассмотрим рациональную функцию $f$ на $E_1\times E_2$ такую, что $\forall P \in E_1\ \mathrm{div}\,(f_P) = (\phi(P)) + (\psi(P)) - (\phi(P)+\psi(P)) - (O_{E_2})$. Её дивизор нулей на $E_1\times E_2$ будет объединением графиков $\phi$ и $\psi$, а дивизор полюсов - объединением графика $\phi+\psi$ и графика константы $O_{E_2}$. Поэтому функция ${}_Qf$ на $E_1$ будет иметь дивизор, указанный выше.
6) $\widehat{[m]} = [m]$ по индукции из предыдущего пункта $\Rightarrow$ по определению $[m^2] = [\deg[m]] \Rightarrow m^2 = \deg[m]$ (так как $\mathbf{Z}$- модуль $\mathrm{End}\,E$ не имеет кручения).
7) - 8) Простое упражнение на тему предыдущих пунктов ■

5. Точки конечного порядка.

Будем считать, что $k$ алгебраически замкнуто. Обозначим $E_m \stackrel{\mathrm{def}}{=} \ker[m]$ множество

(и подгруппу) точек конечного порядка, делящего $m$, в $E(k)$. Если $\mathrm{char}\,(k) \nmid m$, то изогения $[m]$ сепарабельна, а значит, $\#(E_m) = \deg[m] = m^2$ и для любого простого $l|m$ $\#(E_l) = l^2$, поэтому $E_l \simeq \mathbf{Z}/(l) \times \mathbf{Z}/(l)$. Следовательно $E_m \simeq \mathbf{Z}/(m) \times \mathbf{Z}/(m)$ по теореме о структуре кончных абелевых групп.

Если же $p = \mathrm{char}\,(k)$, то $[p]$ несепарабельна, поэтому $\deg_{sep}[p] = p$ или $\deg_{sep}[p] = 1$. Поскольку $[p] = Fr_p \circ \widehat{Fr_p}$, а $Fr_p$ - чисто несепарабельнный морфизм степени $p$, всё зависит от того, сепарабелен ли $\widehat{Fr_p}$. Если да, то имеет место первый случай (кривая $E$ называется обыкновенной) и $\forall r \;\; E_{p^r} \simeq \mathbf{Z}/(p^r)$. Если нет, то кривая по историческим причинам называется суперсингулярной (будучи эллиптической, она, разумеется, невырождена), изогения $[p]$ чисто несепарабельна и $\forall r \;\; E_{p^r} = 0$.

Суперсингулярных кривых в данной характеристике $p$ с точностью до изоморфизма конечное число. Действительно, нетрудно проверить, что эллиптическая кривая с точностью до изоморфизма определяется своим $j$-инвариантом. Это рациональное выражение от коэффициентов $a_i$ её уравнения (для кривой $E$ над $\mathbf{C}$, задаваемой решеткой $L$, с точностью до умножения на не зависящую от $L$ константу, $j_E = \frac{g_2^3}{\Delta}$). Если изогения $\widehat{Fr_p} : E^{(p)} \to E$, которая имеет степень $p$, чисто несепарабельна, то она, как было отмечено в предыдущем разделе, представляется в виде композиции $E^{(p)} \stackrel{Fr_p}{\to} E^{(p^2)} \stackrel{\lambda}{\to} E$, где $\lambda$ - сепарабельная изогения. Последняя имеет степень 1, и следовательно, является изоморфизмом. Это означает, что $E \simeq E^{(p^2)}$, а значит $j_E^{p^2} = j_E \Rightarrow j_E \in \mathbf{F}_{p^2}$.

Пусть $l$ - простое число. Определим модуль Тэйта кривой $E$ формулой $T_l(E) = \lim\limits_{\leftarrow} E_{l^n}$. Из сказанного выше следует, что $T_l(E) \simeq \mathbf{Z}_l \oplus \mathbf{Z}_l$ при $l \neq \mathrm{char}\,(k)$, и $T_l(E) = \mathbf{Z}_l$ или 0 при $l = \mathrm{char}\,(k)$. Далее мы считаем, что $l \neq \mathrm{char}\,(k)$.

Теорема. Естественный гомоморфизм $\mathrm{Hom}(E_1, E_2) \otimes \mathbf{Z}_l \to \mathrm{Hom}(T_l(E_1), T_l(E_2))$ - вложение.
Доказательство. Прежде всего заметим, что deg - положительно определённая квадратичная форма на группе $\mathrm{Hom}(E_1, E_2)$. Действительно, $[\deg(\phi + \psi)] - [\deg\phi] - [\deg\psi] = \hat{\phi}\circ\psi + \hat{\psi}\circ\phi$ билинейна. Пусть теперь $\Phi = \sum \alpha_i\phi_i$ ($\alpha_i \in \mathbf{Z}_l$, $\phi_i \in \mathrm{Hom}(E_1, E_2)$) переходит в 0. Подгруппа $H \subset \mathrm{Hom}(E_1, E_2)$, состоящая из всех таких $\psi$, что $[m] \circ \psi \in \langle\phi_i\rangle$ при каком-нибудь $m$, конечно порождена (в противном случае степень каких-то её элементов оказалась бы не целой в силу замечания в начале доказательства), а значит, благодаря отсутствию кручения, свободна. Заменим набор $\phi_i$ на её базис. То,

что $\Psi$ переходит в 0, означает, что $\forall n \forall \{a_i \in \mathbf{Z}, a_i \equiv \alpha_i \mod l^n\}$ изогения $\psi = \sum [a_i] \circ \phi_i$ аннулирует $(E_1)_{l^n}$, и тем самым $\psi = [l^n] \circ \lambda$. Из определения $H$ следует, что $\lambda \in H$, то есть $\lambda = \sum [b_i] \circ \phi_i$. Сравнивая $\psi$ и $\lambda$, получаем, что $a_i = l^n b_i$, откуда $l^n | \alpha_i$. Поскольку это верно при любом $n$, все $\alpha_i = 0$ ■

Из теоремы сразу следует, что $\mathrm{Hom}(E_1, E_2)$ - свободный $\mathbf{Z}$-модуль ранга, не превосходящего 4. Если $E_1 = E_2 = E$, то несложно проверить, что при $\mathrm{char}\,(k) = 0$ $\mathrm{End}\, E$ это $\mathbf{Z}$ или порядок в кольце $\mathcal{O}_K$, где $K$ - мнимое квадратичное поле. В случае конечной характеристики кроме этих двух случаев (реализующихся, соответственно, когда $E$ не определена над конечным полем и когда определена и обыкновенна) $\mathrm{End}\, E$ может также быть порядком в кватернионной алгебре (это происходит, когда $E$ суперсингулярна).

Несложный анализ показывает, что группа единиц $(\mathrm{End}\, E)^* = \mathrm{Aut}\, E$ конечна, а её порядок делит 24.

Предположим временно, что поле $k$ совершенно, но $k \neq \overline{k}$. Тогда на точках конечного порядка кривой $E$ и на её модуле Тэйта действует группа Галуа, и несложно проверить, что отображение $\rho_l : \mathrm{Gal}\,(\overline{k}/k) \to \mathrm{Aut}\,(T_l(E))$ непрерывно. Насколько велик его образ, зависит от природы поля $k$ и от того, обладает ли кривая $E$ комплексным умножением. Например, если $k$ - числовое поле, а у $E$ нет комплексного умножения, то по теореме Серра образ является подгруппой конечного мндекса для всех $l$, а для всех $l$, кроме конечного числа, совпадает с полной группой автоморфизмов $T_l(E)$.

Спаривание Вейля.

Пусть $k = \overline{k}$ и $\mathrm{char}\,(k) \nmid m$. Если $T \in E_m$, то $\exists f \in k(E)$ такая, что $\mathrm{div}\, f = m(T) - m(O_E)$. Выберем $T'$ так, чтобы $mT' = T$, тогда $\exists g \in k(E)$ такая, что $\mathrm{div}\, g = [m]^*(T) - [m]^*(O_E) = \sum\limits_{R \in E_m} ((T' + R) - (R))$.
Диизоры функций $f \circ [m]$ и $g^m$ совпадают, так что, домножив $f$ на константу, можно считать, что $f \circ [m] = g^m$.
Пусть теперь $S \in E_m$ ($S$ и $T$ могут совпадать). Поскольку дивизоры функций $g$ и $g \circ t_S$ совпадают, то эти функции пропорциональны, иначе говоря $e_m(S,T) \stackrel{\mathrm{def}}{=} g(P+S)/g(P)$ не зависит от выбора точки $P \in E$. При этом $g(P+S)^m = f([m]P + [m]S) = f([m]P) = g(P)^m$, поэтому $e_m(S,T) \in \mu_m$.

Свойства $e_m$.
1) $e_m(S_1+S_2,T)=e_m(S_1,T)e_m(S_2,T)$ и аналогично для суммы справа
2) $e_m(S,T)e_m(T,S)=1$
3) Если $\forall S\ \ e_m(S,T)=1$, то $T=O_E$.
4) Если предположить, что $k$ совершенно, но $k\neq\overline{k}$, то $\forall\sigma\in\mathrm{Gal}\,(\overline{k}/k)$
$\sigma(e_m(S,T))=e_m(\sigma(S),\sigma(T))$
5) Если $S\in E_{mm'}$ и $T\in E_m$, то $e_{mm'}(S,T)=e_m([m']S,T)$
6) Если $\phi:E_1\to E_2$ - изогения, то $e_m(S,\hat{\phi}(T)=e_m(\phi(S),T)$.
Доказательство: рутинная проверка ■

$e_m$ очевидным образом продолжается до Галуа-инвариантного спаривания
$T_l(E)\times T_l(E)\to T_l(\mu)$.

6. Эллиптические кривые над конечными полями, локальными полями и полями алгебраических чисел.

Каждому из случаев следовало бы посвятить отдельный подраздел, но у нас нет на это времени. Поэтому ограничимся кратким обзором.

Конечное поле. $k=\mathbf{F}_q$.

Для начала отметим, что при любом $n$ $\#(E(\mathbf{F}_{q^n}))=\deg(1-Fr_{q^n})$, поскольку степень сепарабельной изогении равна порядку её ядра.

Теорема. $|\#(E(k))-q-1|\leq 2\sqrt{q}$
Доказательство. Сумма под знаком модуля равна $\deg(1-Fr_q)-\deg Fr_q-\deg 1_E$. Согласно замечанию в начале доказательства теоремы из предыдущего пункта, deg - положительно определённая квадратичная форма, поэтому по неравенству Коши абсолютная величина этой суммы не превосходит $2\sqrt{\deg Fr_q\deg 1_E}=2\sqrt{q}$ ■.

Это простейший частный случай "гипотезы Римана", обсуждавшейся в разделе "Дзета-функции".

Из замечания перед теоремой сразу следует, что $Z(E/k,T)=\frac{1-aT+qT^2}{(1-T)(1-qT)}$, где $a=1-q-\deg(1-Fr_q)=Tr(Fr_q|T_l(E))$. Переходя к переменной $s$, получаем $\zeta(E/k,s)=Z(E/k,q^{-s})=\frac{1-aq^{-s}+q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}$.

Локальное поле.

Пусть $k$ - поле частных полного дискретно нормированного кольца $\mathcal{O}_k$ с максимальным идеалом $\mathfrak{p}$ и конечным полем вычетов $k_\mathfrak{p}$. Зададим эллиптическую кривую $E$ над $k$ уравнением в обобщенной форме Вейерштрасса $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Дискриминант $\Delta$ (аналог $g_2^3 - 27g_3^2$ для обычного уравнения Вейерштрасса) задается полиномом от коэффициентов $a_i$, который мы здесь не станем выписывать, и не обращается в 0. Уравнение называется минимальным, если все $a_i \in \mathcal{O}_k$ и $\mathrm{v}_\mathfrak{p}(\Delta)$ принимает минимальное значение.

Общий вид замены переменных в обобщенном уравнении Вейерштрасса, переводящей кривую $E$ в изоморфную, имеет вид $x = u^2x' + r;\ \ y = u^3y' + u^2sx' + t$, где $u \neq 0, s, t, r \in k$ - произвольные параметры, при этом $\Delta = u^{12}\Delta'$. Ясно, что заменой переменных можно добиться, чтобы все $a_i \in \mathcal{O}_k$, поэтому минимальное уравнение существует. Для того, чтобы замена переменных оставляла минимальное уравнение минимальным, достаточно (и, как несложно проверить, необходимо) чтобы $u \in \mathcal{O}_k^*, s, t, r \in \mathcal{O}_k$. Инвариантный дифференциал $\omega = \frac{dx}{2y+a_1x+a_3}$ при замене переменных умножается на $u$ ($\omega' = u\omega$), следовательно, инвариантный дифференциал, ассоциированный с минимальным уравнением, определен однозначно с точностью до умножения на элемент $\mathcal{O}_k^*$.

Кривая $\tilde{E}/k_\mathfrak{p}$, полученная путем замены коэффициентов минимального уравнения кривой $E$ на их вычеты $\bmod \mathfrak{p}$, называется редукцией кривой $E$. Она является гладкой (и следовательно, эллиптической кривой над $k_\mathfrak{p}$) тогда и только тогда, когда $\mathrm{v}_\mathfrak{p}(\Delta) = 0$. В этом случае говорят, что кривая $E$ имеет хорошую редукцию. В противном случае редукция называется плохой. Плохая редукция бывает двух видов: кривая $\tilde{E}$ может иметь точку самопересечения или точку возврата.

Вырожденная плоская кубическая кривая рациональна; если удалить из неё особую точку, то оставшаяся часть $\tilde{E}^{ns}$ будет изоморфна $\mathbf{P}^1$ без точки в случае, если особая точка была точкой возврата, и $\mathbf{P}^1$ без двух точек, если это была точка самопересечения. В обоих случаях на $\tilde{E}^{ns}$ сохраняется структура группы ($-P - Q$ это третья точка пересечения прямой, проходящей через $P$ и $Q$, с кубической кривой $\tilde{E}$; она не может быть особой, иначе пересечение было бы четырехкратным). В случае точки возврата группа $\tilde{E}^{ns}(k_\mathfrak{p})$ изоморфна $k_\mathfrak{p}^+$, поэтому плохая редукция называется аддитивной. В случае точки самопересечения $\tilde{E}^{ns}(k_\mathfrak{p})$ изоморфна либо $k_\mathfrak{p}^*$, либо подгруппе элементов единичной нормы в мультипликативной группе квадратичного расширения $k_\mathfrak{p}$, в

зависимости от того, определены ли над $k_\mathfrak{p}$ касательные к кривой $\tilde{E}$ в особой точке, поэтому редукция называется мультипликативной (соответственно, обычной либо скрученной)

В случае хорошей редукции сопоставление точке $E(k)$ её редукции даёт точную последовательность групп $0 \to E_1 \to E(k) \to \tilde{E}(k_\mathfrak{p}) \to 0$. Подгруппа $E_1$ состоит из точек, редуцирующихся в бесконечноудаленную, т.е. тех, чьи координаты имеют $\mathfrak{p}$ в знаменателе. Если редукция плохая, то эта последовательность заменяется на последовательность $0 \to E_1 \to E_0 \to \tilde{E}^{ns}(k_\mathfrak{p}) \to 0$, где $E_1$ та же, что и раньше, а $E_0$ состоит из точек $E(k)$, чья редукция не попадает в особую точку.

Хотелось бы и в случае плохой редукции написать точную последовательность со средним членом $E(k)$. Спектр кольца $\mathcal{O}_k$ состоит из двух точек - общей $\operatorname{Spec} k$ и замкнутой $\operatorname{Spec} k_\mathfrak{p}$. Минимальное уравнение $E$ задает двумерную схему $E_{min}$ над $\operatorname{Spec} \mathcal{O}_k$ (подсхему трехмерной схемы $\mathbf{P}^2(\mathcal{O}_k)$) с общим слоем $E$ и замкнутым слоем $\tilde{E}$. Разрешая особенности $E_{min}$, мы получим схему $\mathfrak{E}$ над $\operatorname{Spec} \mathcal{O}_k$, которая уже не обязана быть подсхемой $\mathbf{P}^2$, и замкнутый слой которой является в общем случае приводимой кривой над $k_\mathfrak{p}$. Если выкинуть из $\mathfrak{E}$ особые точки замкнутого слоя (сама она регулярна, но морфизм $\mathfrak{E} \to \operatorname{Spec} \mathcal{O}_k$ продолжает оставаться негладким), то получится групповая схема $\mathcal{E}$ над $\operatorname{Spec} \mathcal{O}_k$ - так называемая модель Нерона кривой $E$. Можно доказать, что имеет место изоморфизм $E(k) \simeq \mathcal{E}(\mathcal{O}_k)$. Иначе говоря, если часть точек $E(k)$ при редукции попадали в особые точки замкнутого слоя $E_{min}$, то при замене $E_{min}$ на $\mathfrak{E}$ в особые точки замкнутого слоя уже ничего не попадает. Таким образом, мы получили то, что хотели: точную последовательность $0 \to E_1 \to E(k) \to \tilde{\mathcal{E}}(k_\mathfrak{p}) \to 0$.

Иногда может случиться, что $E_{min}$ сама регулярна. Тогда $\mathfrak{E} = E_{min}$ и $\tilde{\mathcal{E}}(k_\mathfrak{p}) = \tilde{E}^{ns}(k_\mathfrak{p})$. Но, как мы уже отметили, в общем случае замкнутый слой $\mathfrak{E}$ (если заменить $k$ на его максимальное неразветвленное расширение, соответственно, $k_\mathfrak{p}$ на $\overline{k_\mathfrak{p}}$; это не влияет на предыдущие построения) приводим и состоит из нескольких компонент, изоморфных $\mathbf{P}^1$. Тэйт разработал несложный алгоритм, позволяющий установить структуру замкнутого слоя $\mathfrak{E}$ по минимальному уравнению кривой $E$. Если редукция мультипликативна, то этот слой представляет собой "колесо" из нескольких проективных прямых (каждая пересекается с предыдущей и с последующей), и имеет место точная последовательность $0 \to \tilde{E}^{ns}(k_\mathfrak{p}) \to \tilde{\mathcal{E}}(k_\mathfrak{p}) \to \mathbf{Z}/(n) \to 0$, где $n$ - число компонент в обычном случае и $n = 1$ или 2 в скрученном случае (если $\mathfrak{E} = E_{min}$, то $n = 1$ и вместо "колеса" имеется единственная самопересекающаяся проективная прямая). Если редукция аддитивна, то некоторые из компонент замкнутого слоя $\mathfrak{E}$ могут быть

кратными (при переходе к модели Нерона от них ничего не остается), а $\tilde{\mathcal{E}}(k_\mathfrak{p})/\tilde{E}^{ns}(k_\mathfrak{p})$ - группа порядка не более 4.

В заключение упомянем полезное свойство группы $E_1$: в ней нет элементов конечного порядка, не делящегося на $\mathrm{char}\,(k_\mathfrak{p})$. Проще всего доказать это, представив $E_1$, как группу точек формальной группы, связанной с $E$, но мы опустим подробности.

Поле алгебраических чисел.

Теорема Морделла. Пусть $E$ - эллиптическая кривая над полем $k$ - конечным расширением $\mathbf{Q}$. Тогда $E(k)$ - группа с конечным числом образующих.

Скажем пару слов о доказательстве. Оно состоит из двух частей.
Первая часть - так называемая "слабая теорема Морделла" - утверждает, что группа $E(k)/nE(k)$ конечна при любом $n$. В нынешние времена это доказывается в одну строчку при помощи точной последовательности когомологий $\mathrm{Spec}\,\mathcal{O}_k$ в подходящей топологии Гротендика для точной последовательности пучков $0 \to E_n \to \mathcal{E} \stackrel{n}{\to} \mathcal{E} \to 0$. Впрочем, при $n = 2$ можно доказать то же самое вручную, применяя классический метод спуска.
Вторая часть состоит в построении на группе E(k) квадратичной формы $\hat{h}$ (так называемой высоты Нерона-Тейта), положительно определённой на $E(k)/E_{tors}(k)$ и такой, что разность $\hat{h}(P) - \log H(P)$ ограничена на $E(k)$. Здесь $H(P)$ - высота Вейля точки $P$, которая задается формулой $H(P) = \prod_v \max(||X(P)||_v, ||Y(P)||_v, ||Z(P)||_v)$, где $v$ пробегает все нормирования поля $k$, а $X, Y, Z$ - однородные координаты точки $P$. Почти очевидно, что количество точек ограниченной высоты Вейля в $\mathbf{P}^2(k)$ конечно. Отсюда и из второго свойства формы $\hat{h}$ следует, что и количество точек $P \in E(k)$, таких, что $\hat{h}(P)$ ограничена, конечно. Вместе со слабой теоремой Морделла это чисто формально приводит к выводу, что группа $E(k)/E_{tors}(k)$ имеет конечный ранг. Поскольку $E_{tors}(k)$ - легко вычисляемая конечная группа (это сразу следует из замечания в конце параграфа про локальные поля), отсюда следует теорема Морделла.
Форма $\hat{h}$ может быть построена как сумма локальных компонент, отвечающих различным нормированиям поля $k$ (именно так действовал Нерон). Компоненты, отвечающие неархимедовым нормированиям, строятся с помощью теории пересечений на модели Нерона, а для архимедовых нормирований используется сигма-функция Вейерштрасса.

Вычисление ранга группы $E(k)/E_{tors}(k)$ - до сих пор не решенная задача. Неизвестно

даже, существует ли последовательность эллиптических кривых над $\mathbf{Q}$, для которых этот ранг стремится к бесконечности. Гипотеза Бёрча - Суиннертона-Дайера предполагает, что ранг равен порядку нуля канонической $L$- функции $L(E/k,s)$ в точке $s=0$. В случае, когда $k=\mathbf{Q}$, а порядок нуля равен 0 или 1, гипотеза доказана, но это почти всё.

Остается напомнить, что представляет собой ряд $L(E/k,s)$. Обозначим $\zeta(E/k,s)$ дзета-функцию схемы $\mathfrak{E}$ над $\operatorname{Spec}\mathcal{O}_k$. Тогда $\zeta(E/k,s)=\prod\limits_{\mathfrak{p}\subset\mathcal{O}_k}\zeta(\tilde{E}\mod\mathfrak{p},s)$. Пусть $q=\#(\mathcal{O}_k/\mathfrak{p})$. Если редукция хорошая, то $\zeta(\tilde{E}\mod\mathfrak{p},s)=\frac{1-aq^{-s}+q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}$. Если редукция аддитивная, то $\tilde{E}\mod\mathfrak{p}$ - проективная прямая, и $\zeta(\tilde{E}\mod\mathfrak{p},s)=\frac{1}{(1-q^{-s})(1-q^{1-s})}$. Если редукция обычная мультипликативная, то $\tilde{E}\mod\mathfrak{p}$ - проективная прямая с одной точкой самопересечения, т.е с точки зрения количества точек - аффинная прямая, поэтому $\zeta(\tilde{E}\mod\mathfrak{p},s)=\frac{1}{(1-q^{1-s})}$. Наконец, если редукция скрученная мультипликативная, то вычисление оставляется в качестве задачи.

В итоге имеем $\zeta(E_k,s)=\frac{\zeta_k(s)\zeta_k(s-1)}{L(E/k,s)}$, где $L(E/k,s)=\prod\limits_{\mathfrak{p}\subset\mathcal{O}_k}L_{\mathfrak{p}}(E,s)$ как раз и есть искомая каноническая $L$-функция. Сомножители имеют вид $L_{\mathfrak{p}}(E,s)=(1-a_{\mathfrak{p}}q(\mathfrak{p})^{-s}+q(\mathfrak{p})^{1-2s})^{-1}$ в случае хорошей редукции, $L_{\mathfrak{p}}(E,s)=1$ в случае аддитивной редукции, $L_{\mathfrak{p}}(E,s)=(1-q(\mathfrak{p})^{-s})^{-1}$ в случае обычной мультипликативной редукции и (посчитайте самостоятельно) в случае скрученной мультипликативной редукции.

Гипотеза Хассе-Вейля предполагает, что $L(E/k,s)$ продолжается до мероморфной функции на $\mathbf{C}$ и удовлетворяет функциональному уравнению. Для случая эллиптических кривых над $\mathbf{Q}$ Уайлз и его последователи доказали, что $L(E/\mathbf{Q},s)$ является преобразованием Меллина некоторой параболической модулярной формы для группы $\Gamma_0(N)$, собственной для полной алгебры Гекке, где $N$ -так называемый кондуктор кривой $E$, легко вычисляемый по её модели Нерона. Из этого очевидно следует, что $L(E/Q,s)$ удовлетворяет функциональному уравнению и всюду голоморфна.