Осень 2019

Лекция №3 — 27.09.19

Лектор: Елена Киршанова *Оформил Филипп Максимов*

Определение 1. Порядок точки $P \in E$, $\operatorname{ord} P, n \in \mathbb{N}$ — минимальное, такое что

$$n \cdot P = \mathcal{O}$$

1 Точки n-кручения

Определение 2. Для $n > 1$, E – эллиптической кривая над полем K точками n-кручения называется множество

$$E[n] = \left\{ P \in E(\bar{K}) \middle| \, nP = \mathcal{O} \right\}.$$

Рассмотрим $n = 2$

- $charK \neq 2 \Rightarrow E \cdot y^2 \pm f(x), \quad \deg f(x) = 3 \Rightarrow$

  $$y^2 = (x - e_1)(x - e_2)(x - e_3), \quad e_i - \text{ корни } f(x) \text{ в } \bar{K}$$

  Для $\forall P \in E$ справедливо: $2P = \mathcal{O} \Leftrightarrow$ касательная l в P — вертикальная $\Rightarrow y = 0$ $\Rightarrow$

  $$E[2] = \{\mathcal{O},\ (e_1, 0),\ (e_2, 0),\ (e_3, 0)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

  Вывод: для того, чтобы найти все точки r-кручения, в $charK \neq 2$, следует найти все корни $f(x)$.

- $charK = 2 : \exists$ 2 вида кривой A

  $$\underset{E : y^2 + xy + x^3 + a_2x^2 + a_6 = 0}{\underset{(a_6 \neq 0)}{\downarrow}} \qquad \underset{E : y^2 + a_3y + x^3 + a_4x + a_6}{\underset{(a_3 \neq 0)}{\downarrow}}$$

  В обоих случаях, если $P = (x, y)$ — точка порядка 2, то касательная к P — вертикаль $\Rightarrow \frac{dE}{dy} = 0$

  $$\underset{\begin{array}{c} 2y \neq x = 0 \\ x = 0 \\ \Rightarrow y^2 + a_6 = 0 \\ \Rightarrow P = \left(0, \sqrt{a_6}\right) \\ \Rightarrow E[2] = \left\{\mathcal{O},\ \left(0, \sqrt{a_6}\right)\right\} \simeq \mathbb{Z}_2 \end{array}}{\downarrow} \qquad \underset{\begin{array}{c} \frac{dE}{dy} = a_3 \\ a_3 \neq 0 \text{ (иначе } E \text{ — сингулярная)} \\ \Rightarrow E[2] = \{\mathcal{O}\}. \end{array}}{\downarrow}$$

Лемма 3. *Для E — эллиптической кривой над K, справедливо*

$$\begin{aligned} &E[2] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2, && \text{при } charK \neq 2 \\ &E[2] \cong 0 \text{ либо } E[2] \cong \mathbb{Z}_2 && \text{при } charK = 2. \end{aligned}$$

Можно показать, что [Was. § 3.1]

$$\begin{aligned} &E[3] \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3, && \text{при } charK \neq 3 \\ &E[3] \cong 0 \text{ либо } E[3] \cong \mathbb{Z}_3, && \text{при } charK = 3 \end{aligned}$$

В общем случае, справедлива теорема 4:

Теорема 4. *Пусть E — эллиптическая кривая над K, и $n \geqslant \mathbb{N}_+$. Тогда справедливо: [док-во в Was. § 32]*

- $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$, *если* $charK \nmid n$ *или* $charK \neq 0$,
- $E[n] \cong \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$ *или* $\cong \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$ *если* $char\ K = p > 0, \quad p|n$ *и* $n = p^r \cdot n', \quad p \nmid n'$.

Определение 5.

- E, заданная над K с $char\ K = p$, называется простой, если $E[p] \cong \mathbb{Z}_p$.
- E называется суперсингулярной, если $E[p] \cong 0$.
  ! Не путать с сингулярными кривыми.

2 Многочлены деления

Важность:

– описывают отображение $n : P \leftrightarrow n \cdot P$

– используются в алгоритме подсчета точек кривой

– используются в вычислениях изогений

Определение 6. A, B, x, y — переменные.

Многочлены деления $\psi_m \in \mathbb{Z}\ [x, y, A, B]$ определяются рекуррентными соотношениями:

$$\begin{aligned} \psi_0 &= 0 \\ \psi_1 &= 1 \\ \psi_2 &= 2y \\ \psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\ \psi_4 &= 4y^2\left(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - zB^2 - A^3\right) \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad m \geqslant 2 \\ \psi_{2m} &= (2y)^{-1} \cdot \psi_m \cdot \left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right), \quad m \geqslant 3 \end{aligned}$$

Могут быть получены с помощью формул сложения в так называемых координатах Якоби.

Свойства (док-во: Was. Lemma 3.3)

1. $\psi_n \in \mathbb{Z}[x, y^2, A, B]$ если n — нечетное
   $\psi_n \in 2y\mathbb{Z}[x, y^2, A, B]$, если n — четное.

2. Определим

$$\begin{aligned}
\varphi_m &= x \cdot \psi_m^2 - \psi_{m+1}\psi_{m-1} \\
\omega_m &= (4y)^{-1}\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right) \\
\varphi_n &\in \mathbb{Z}\left[x, y^2, A, B\right], \forall n \\
\omega_n &\in y\mathbb{Z}\ \left[x, y^2, A, B\right], n \text{ – нечетное} \\
\omega_n &\in \mathbb{Z}\left[x, y^2, A, B\right], n \text{ – четное}
\end{aligned}$$

3. Для эллиптической кривой $E : y^2 = x^3 + Ax + B$, в многочленах ψ_n, ϕ_n можно сделать замену $y^2 \mapsto x^3 + Ax + B$ и рассматривать их как многочлены от x (в $\mathbb{Z}[x, A, B]$). Тогда

$$\begin{aligned}
\varphi_n(x) &= X^{n^2} + \text{ мономы степени } < n^2 \\
\psi_n^2(x) &= n^2 x^{n^2-1} + \text{ мономы степени } < n^2 - 1
\end{aligned}$$

Теорема 7. *Пусть $E : y^2 = x^3 + Ax + B$ ($\Rightarrow charX \neq 2, 3$) $P = (x, y) \in E$, $n \in \mathbb{N}_+$. Тогда*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)},\ \frac{\omega_n(x)}{(\psi_n(x, y))^3}\right)$$

Таким образом, отображение (эндоморфизм) «умножение на n» $n \cdot P$ задается рациональными функциями.