Криптосистеми на еліптичних кривих

Lecture 8: Divisors' magic

Грубіян Євген Олександрович

Еквівалентні дівізори

Приклад

Покажемо що дівізори D_1, D_2 з прикладу нижче є еквівалентними:

$$P = (57, 24), Q = (25, 37), R = (17, 32), S = (42, 35) \in E/F_{61} \cap f$$
$$E/F_{61} : y^2 = x^3 + 8x + 1, f : y = 33x^2 + 10x + 24$$
$$D_1 = (P) + (Q) + (R) \in \mathrm{Div}(E), D_2 = 4(\mathcal{O}) - (S) \in \mathrm{Div}(E)$$
$$(f) = (P) + (Q) + (R) + (S) - 4(\mathcal{O})$$
$$f \in F_{61}(E) \implies (f) \in \mathrm{Prin}(E) \implies D_1 - D_2 = (f) \implies D_1 \sim D_2.$$

Зазначимо що оскільки $(f) \in \mathrm{Prin}(E)$ то $\deg((f)) = 0$, а також
$P + Q + R + S = \mathcal{O}$
Як бачимо дівізори D_1, D_2 відрізняються на деякий головний дівізор, тому вони еквівалентні

Еквівалентні дівізори

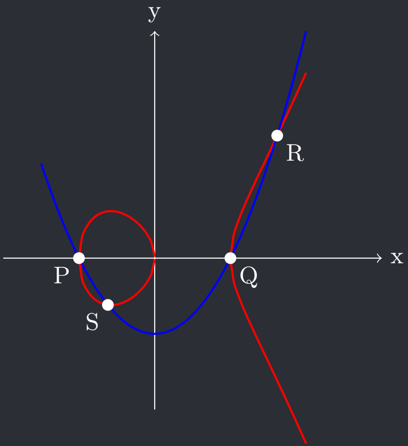


Рис.: $(f) = (P) + (Q) + (R) + (S) - 4(\mathcal{O})$

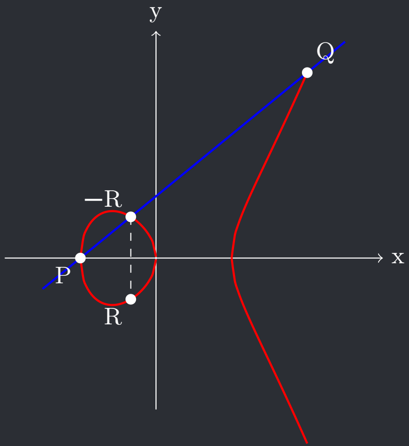
Еквівалентні дівізори

Приклад

Розглянемо еліптичну криву E/K
Нехай маємо знайомий нам дівізор прямої що проходить через точки P, Q: $(l) = (P) + (Q) + (-R) - 3(\mathcal{O})$, де $R = P + Q$. А також дівізор вертикалі $v : x = x_R$: $(v) = (R) + (-R) - 2(\mathcal{O})$
Обчислимо дівізор частки функцій
$(l/v) = (l) - (v) = (P) + (Q) - (R) - (\mathcal{O})$, зазначимо що $(l/v) \in Prin(E)$.
Із рівності точок на кривій $R = P + Q$ отримуємо рівність дівізорів $(R) - (\mathcal{O}) = (P) - (\mathcal{O}) + (Q) - (\mathcal{O}) - (l/v)$ що добре ілюструє згаданий ізоморфізм групи точок $E(\overline{K})$ та групи Пікарда $Pic^0(E)$: $P \to (P) - (\mathcal{O})$
Зазначимо що при цьому $(R) - (\mathcal{O}) \sim (P) + (Q) - 2(\mathcal{O})$

Інтуїтивно ми можемо для будь якого «великого» дівізора знайти менший для деякої точки R, що буде еквівалентний йому.

Еквівалентні дівізори



Теорема Рімана Роха

Ефективний дівізор

Це дівізор $\sum_{P \in E} n_P(P)$ для якого $\forall P \in E : n_P \geq 0$

Ефективна частина дівізора D

$\epsilon(D) = \sum_{P \in E} n_P(P)$, де $n_P \geq 0$

Розмір дівізора D

$L(D) = \deg(\epsilon(D))$

Теорема Рімана-Роха (дуже інтуїтивно)

Для алгебраїчної кривої C роду(кількість «дірок» як топологічної поверхні) g, кожен дівізор $D \in \mathrm{Pic}^0(C)$ еквівалентний деякому дівізору D' розміру, який не перевищує g: $L(D') \leq g$

Гіпереліптичні криві

Гіпереліптична крива

Алгебраїчна крива роду $g > 1$ над полем K, що задається рівнянням
$y^2 + h(x)y = f(x),\ \deg(f) = 2g + 1$

Теорема Рімана-Роха каже що для алгебраїчної кривої роду g кожен дівізор можна «скоротити» до еквівалентного йому дівізора розміру не більше g

Приклад

Візьмемо алгебраїчну криву 2-го роду:

$$C/K : y^2 = x^5 + a_4x^4 + \cdots + a_0$$
$$\forall D \in \mathrm{Div}^0(C) \exists D' \in \mathrm{Pic}^0(C) : D \sim D' \ \ \&\ \ D' = (P) + (Q) - 2(\mathcal{O})$$

Таким чином ми можемо ефективно працювати в групі(якобіані кривої) $\mathrm{Pic}^0(C)$, попри те що точки кривої для $g > 1$ ($g = 1$ - класичний еліптичний випадок) не утворюють групу.

Наслідок з теореми Рімана-Роха

Для будь якої еліптичної кривої (алгебраїчної кривої роду 1) кожен дівізор можна «скоротити» до еквівалентного, що має розмір 1:
$\forall D \in \mathrm{Pic}^0(E) : D \sim (R) - (\mathcal{O})$

1. Нехай на вході маємо дівізор $D = (P_1) + \cdots + (P_{n+1}) - (n+1)(\mathcal{O}) \in \mathrm{Pic}^0(E)$, де P_i не обов'язково різні точки
2. За теоремою про інтерполяцію існує поліном ℓ_n степеня n, якому задовольняють всі P_i. Цей поліном перетне криву у 2n точках (враховуючи кратності): $P_1, \ldots, P_{n+1}$ та $P'_1, \ldots, P'_{n-1}$
3. Будуємо дівізор $(\ell_n) = \sum_{i=1}^{n+1}(P_i) + \sum_{i=1}^{n-1}(P'_i) - 2n(\mathcal{O}) \in \mathrm{Prin}(E)$
4. Дівізор $D' = -(\sum_{i=1}^{n-1}(P'_i) - (n-1)(\mathcal{O}))$ буде еквівалентним до D
5. Повторюємо процедуру, на кожному кроці скорочуємо степінь полінома на 2 допоки не отримаємо еквівалентний дівізор розміру 1: $D \sim (R) - (\mathcal{O})$
6. Зазначимо що на останньому кроці можемо отримати дівізор $D^{\sim} = (P^{\sim}_1) + (P^{\sim}_2) + (P^{\sim}_3) - 3(\mathcal{O})$ що еквівалентний $(\mathcal{O}) - (Q)$ через $(l_2) = (P^{\sim}_1) + (P^{\sim}_2) + (P^{\sim}_3) + (Q) - 4(\mathcal{O}) \in \mathrm{Prin}(E)$, дівізор $(\mathcal{O}) - (Q) \sim (-Q) - (\mathcal{O})$ через вертикаль $(v) = (Q) + (-Q) - 2(\mathcal{O})$

Завдання

1. Для еліптичної кривої $E/\mathbb{F}_{103} : y^2 + 20x + 20$ знайти еквівалентний дівізор у вигляді $(R) - (\mathcal{O})$ для дівізора

$$D = (P_1) + \cdots + (P_9) - 9(\mathcal{O}) \in \mathrm{Pic}^0(E)$$

$$P_1 = (57, 51), P_2 = (11, 52), P_3 = (96, 19), P_4 = (45, 90),$$

$$P_5 = (11, 51), P_6 = (70, 83), P_7 = (61, 73), P_8 = (59, 95), P_9 = (85, 76)$$

На кожному кроці зазначте поліном ℓ_n та дівізор (ℓ_n) що йому відповідає, а також раціональну функцію в проективній площині (для змінних X, Z) якій відповідає дівізор (ℓ_n)