Matematyka dyskretna

Wykład 12: Krzywe eliptyczne

Gniewomir Sarbicki

Rozważać będziemy przestrzeń $\mathbb{K}^n$

Definicja: $x \sim y \iff \exists \lambda \in \mathbb{K}\ x = \lambda y$. Relację $\sim$ nazywamy różnieniem się o skalar

Przykład: $[4, 10, 6, 14] \sim [6, 15, 9, 21]$, ale $[1, 2, 3, 4] \not\sim [2, 4, 6, 1]$.

Ćwiczenie: Relacja $\sim$ jest relacją równoważności w $\mathbb{K}^n \setminus \{0^n\}$.

Pozwala to na rozważanie zbioru klas abstrakcji - prostych przechodzących przez 0 w $\mathbb{K}^n$:

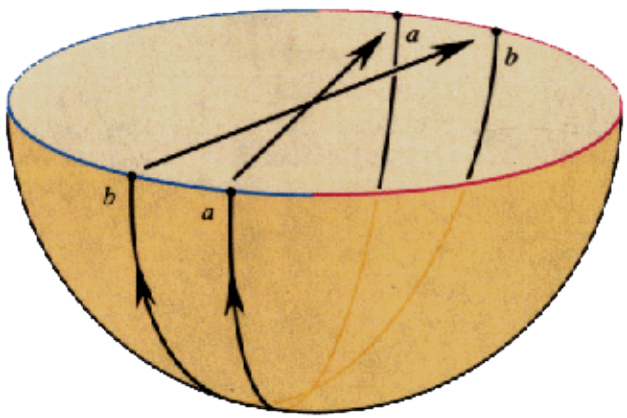
$$\mathbb{K}^n \setminus \{0^n\}/\sim = (\mathbb{K}^n \setminus \{0^n\})/(\mathbb{K} \setminus \{0\}) \stackrel{def}{=} \mathbb{K}P^{n-1}$$

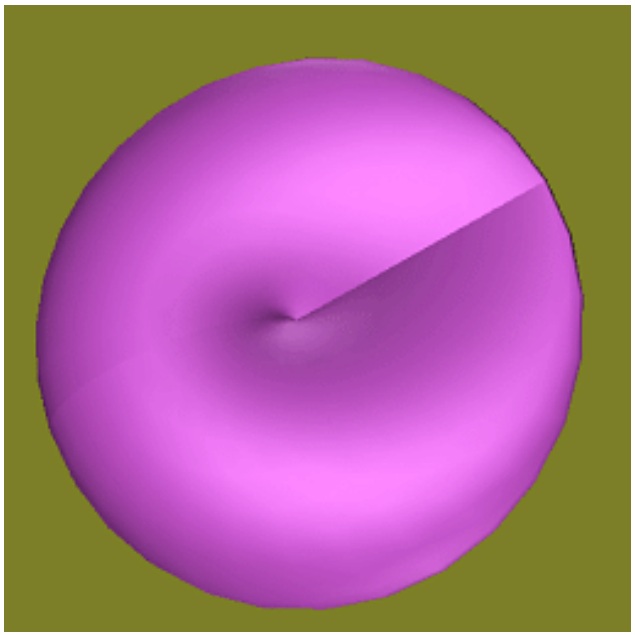
Zbiór ten nazywamy $n-1$ wymiarową przestrzenią rzutową nad $\mathbb{K}$.

Klasę abstrakcji elementu $[x_1, x_2, \ldots, x_n]$ (prostą przechodzącą przez 0^n i ten element) zapisujemy jako $[x_1 : x_2 : \cdots : x_n]$.

Przykład: $\mathbb{R}P^1$ - proste w $\mathbb{R}^2$ przechodzące przez 0. $\mathbb{R}P^2 = S^1/\mathbb{Z}_2 = S^1$.

Przykład: $\mathbb{R}P^2$ - proste w $\mathbb{R}^3$ przechodzące przez 0.





Sklejamy antypodyczne punkty na brzegu - przykład dwuwymiarowej rozmaitości, której nie można zanurzyć w $\mathbb{R}^3$!

Fakt: Każdą przestrzeń rzutową możemy (wyróżniając jedną ze współrzędnych) rozłożyć jako $\mathbb{K}P^n = \mathbb{K}^n + \mathbb{K}P^{n-1}$.

Dowód: Rozważmy element przestrzeni rzutowej $[x_1 : \cdots : x_{n+1}]$. Są możliwe dwa przypadki:

- $x_{n+1} \neq 0$. Definiujemy $\Phi(x) = [x_1/x_{n+1}, \ldots, x_n/x_{n+1}, 1]$.
  Odwzorowanie Φ jest różnowartościowe i na (ćwiczenie).
  Ustala to ciągłą bijekcję pomiędzy zbiorem takich x a zbiorem $\mathbb{K}^n$.
- $x_n = 0$. Zbiór takich x jest równy $(\mathbb{K}^n \setminus \{0^n\})/(\mathbb{K} \setminus \{0\}) = \mathbb{K}P^n$.

Mogliśmy podzielić $\mathbb{K}P^n$ ze względu na tę własność, ponieważ nie zależy ona od wyboru reprezentanta klasy abstrakcji (jest zatem własnością całych klas abstrakcji, czyli elementów $\mathbb{K}P^n$) $\square$

Wniosek: n-wymiarowa przestrzeń rzutowa to n-wymiarowa przestrzeń liniowa z dodanymi *punktami w nieskończoności*, których zbiór ma strukturę przestrzeni rzutowej mniejszego wymiaru i odpowiada kierunkom w $\mathbb{K}P^n$.

Dla funkcji wielomianowej $f : \mathbb{K}^n \to \mathbb{K}$ stopnia d możemy rozważać funkcję wielomianową $\tilde{f} : \mathbb{K}^{n+1} \to \mathbb{K}$ zdefiniowaną jako:

$$\tilde{f}(x_1, \ldots, x_{n+1}) = x_{n+1}^d \cdot \tilde{f}(x_1/x_{n+1}, \ldots, x_n/x_{n+1})$$

Jest to funkcja jednorodna, zatem warunek $\tilde{f}(\tilde{x}) = 0$ wycina pewien podzbiór $\mathbb{K}P^n$ ($\tilde{f}(\tilde{x}) = 0 \implies \forall \lambda \in \mathbb{K}\ \tilde{f}(\lambda \tilde{x}) = 0$)

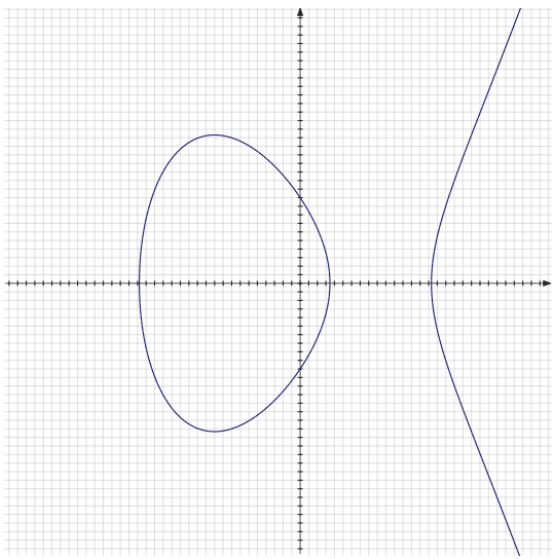
Dla punktów $\tilde{x} \in \mathbb{K}^{n+1}$ dla których $x_{n+1} \neq 0$,
$\tilde{f}(\tilde{x}) = 0 \iff f(x_1/x_{n+1}, \ldots, x_n/x_{n+1}) = 0$

Rozszerzenie $f \to \tilde{f}$ uzupełnia zbiór $\{x \in \mathbb{K}^n : f(x) = 0\}$ o punkty w nieskończoności (należące do $\mathbb{K}P^{n-1}$), robiąc z niego pewien podzbiór $\mathbb{K}^n$.

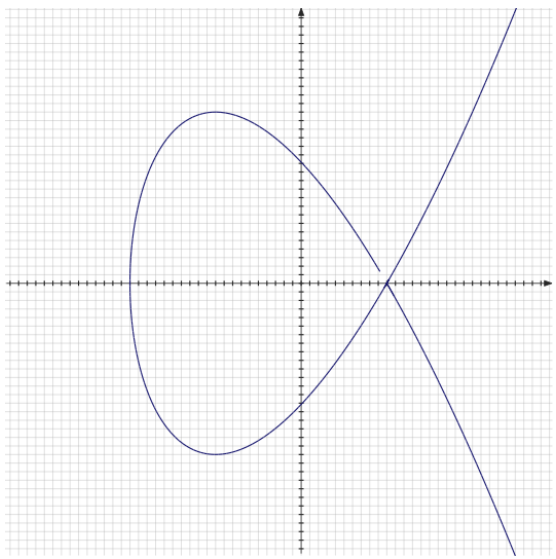
Przykład: Niech $f : \mathbb{R}^2 \to \mathbb{R}, f(x, y) = y - x^2$. Funkcja ta wycina parabolę na płaszczyźnie. $\tilde{f}(x, y, z) = yz - x^2$ wycina stożek w $\mathbb{R}^3$, w której płaszczyzna jest zanurzona warunkiem $z = 1$. Oprócz promieni przechodzących przez parabolę, $\tilde{f}$ zeruje się też dla $[0 : 1 : 0]$ (punkt w nieskończoności odpowiadający kierunkowi pionowemu)

Niech $\mathbb{K}$ - ciało o charakterystyce różnej od $2, 3$.
Rozważmy zbiór punktów w $\mathbb{K}^2$ spełniających równanie $y^2 = x^3 + ax + b$ (a, b są ustalonymi elementami $\mathbb{K}$).

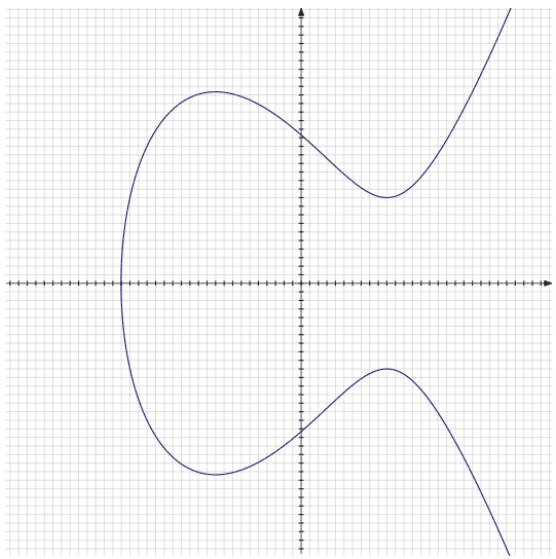
Krzywe nad $\mathbb{R}$:



a=3, b=1



a=3, b=2



a=3, b=3

Kiedy taka krzywa ma samoprzecięcie?

$$\partial_y(x^3 + ax + b - y^2) = 0 \quad \wedge \quad \partial_x(x^3 + ax + b - y^2) = 0$$
$$y = 0 \quad \wedge \quad 3x^2 + a = 0$$

$$y = x^3 + ax + b = \frac{1}{3}x(3x^2 + a + 2a) + b = \frac{2}{3}ax + b = 0$$
$$\implies x = -\frac{3}{2}\frac{b}{a}$$
$$\frac{27}{4}\frac{b^2}{a^2} + a = 0 \implies 27b^2 + 4a^3 = 0$$

Od tej pory będziemy rozważali krzywe bez samoprzecięcia: $27b^2 + 4a^3 \neq 0$

Rozszerzamy naszą krzywą do krzywej w przestrzeni $\mathbb{K}P^2$:

$$y^2z = x^3 + axz^2 + bz^3$$

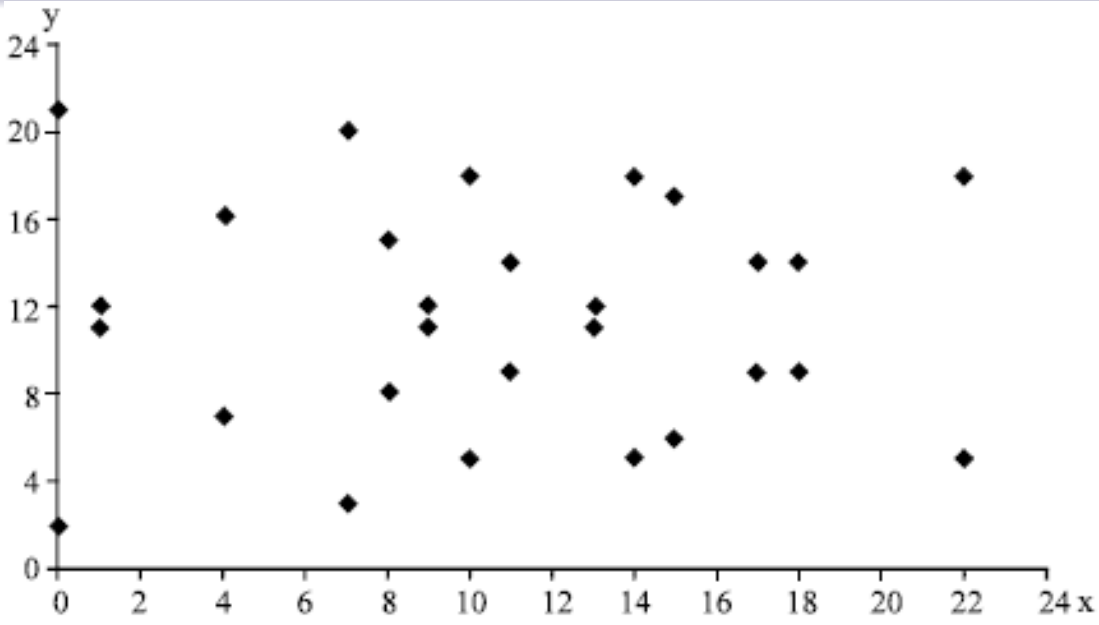
Dochodzi punkt w nieskończoności $[0 : 1 : 0]$ - tam spotyka się dolna gałąź z górną. Punkt ten leży na każdej prostej pionowej.

Definicja

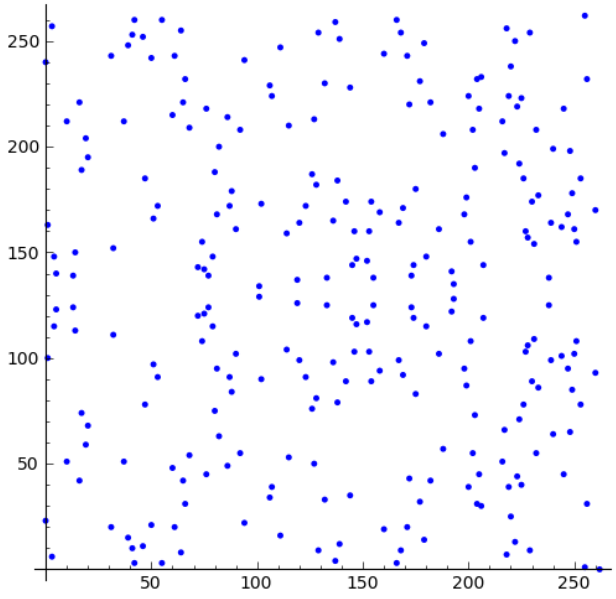
Niech $\mathbb{K}$ - ciało o charakterystyce różnej od $2, 3$ i niech $a, b \in \mathbb{K}$.
Zbiór punktów spełniających równanie

$$y^2 = x^3 + ax + b$$

wraz z punktem w nieskończoności nazywamy *krzywą eliptyczną*.
Będziemy ją oznaczać jako $E_{a,b}(\mathbb{K})$.



$E_{1,4}(\mathbb{Z}_{23})$
http://scialert.net/abstract/?doi=jas.2005.604.633



$E_{2,3}(\mathbb{Z}_{263})$
http://www.johannes-bauer.com/compsci/ecc/

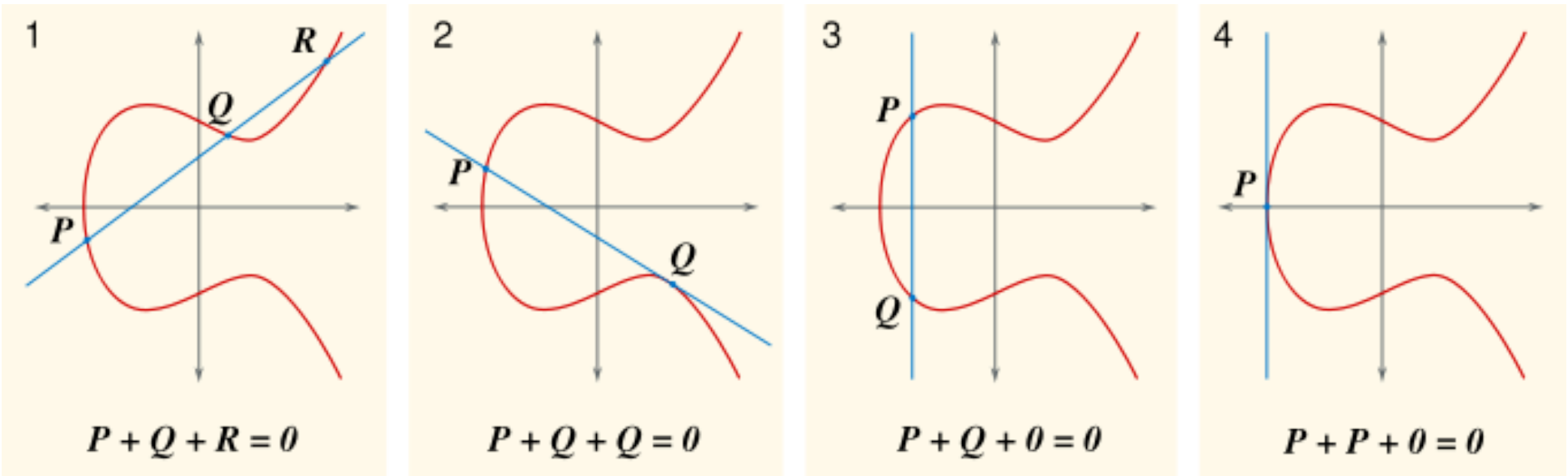
Twierdzenie Hassego

$$p + 1 - 2\sqrt{p} < \#E_{a,b}(\mathbb{Z}_p) < p + 1 + 2\sqrt{p}$$

co więcej, dla każdej liczby z tego zakresu znajdziemy krzywą eliptyczną nad $\mathbb{Z}_p$ o takiej liczbie elementów.

Na krzywej eliptycznej możemy określić dodawanie punktów:

- Przez punkty P i Q na krzywej prowadzimy prostą i otrzymujemy trzeci punkt przecięcia R. Sumą $P + Q$ jest odbicie tego punktu wzgl osi OX.
- elementem przeciwnym jest punkt odbity wzgl osi OX
- elementem neutralnym jest punkt ∞



Dodawanie jest przemienne i łączne (udowodnienie łączności jest trudniejsze).

Prowadzimy prostą przez punkty (x_1, y_1), (x_2, y_2):

$$\frac{y - y_2}{x - x_1} = \frac{y_2 - y_1}{x_2 - x_1} \implies y = \alpha x + \beta, \quad \alpha = \frac{y_2 - y_1}{x_2 - x_1}, \quad \beta = y_2 - \alpha x_2$$

W przypadku, gdy $(x_1, y_1) = (x_2, y_2)$, współczynnik kierunkowy jest równy pochodnej w (x_1, y_1):

$$\alpha = \frac{3x_1^2 + a}{2y_1}$$

Znajdujemy punkty na prostej $(x_1, y_1), (x_2, y_2), (x_3, y_3)$, które leżą na krzywej eliptycznej:

$$(\alpha x + \beta)^2 = x^3 + ax + b \implies x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + (b - \beta^2) = 0$$

Suma pierwiastków wielomianu: $x_1 + x_2 + x_3 = \alpha^2$. Stąd mamy:

$$x_3 = \alpha^2 - x_1 - x_2 \qquad y_3 = -\alpha x_3 - \beta$$

Zastępujemy w klasycznym systemie El-Gamal grupę $\mathbb{Z}_p^*$ pewną podgrupą cykliczną krzywej eliptycznej.

Ustalamy krzywą eliptyczną $E_{a,b}(\mathbb{Z}_p)$ i pewien punkt B na niej o **odpowiednio dużym rzędzie** wynoszącym n (generator podgrupy).

Użytkownik jako swój klucz klucz prywatny wybiera liczbę naturalną $m \in \{1, n-1\}$. Kluczem publicznym jest $[p, a, b, B, C = mB]$.

Nadawca koduje swój blok wiadomości jako punkt P na krzywej eliptycznej. Następnie losuje liczbę naturalną r i wysyła do nadawcy parę punktów:

$$(rB, P + r(mB))$$

Nadawca odkodowuje szyfrogram (X_1, X_2) wzorem: $P = X_2 - mX_1$.

Złamanie szyfru $\iff$ wyznaczenie m z mB i B $\iff$ rozwiązanie zagadnienia logarytmu dyskretnego w podgrupie krzywej eliptycznej. Jest to trudniejsze niż w przypadku logarytmu dyskretnego dla grupy $\mathbb{Z}_p^*$ i pozwala osiągnąć ten sam poziom bezpieczeństwa przy mniejszych p.

Jak, poprzednio, kluczem prywatnym jest m, a publicznym $[p, a, b, B, n, C = mB]$ (dodatkowo podajemy rząd podgrupy).

Podpisem bloku P jest para liczb (u, v). Wyznaczamy ją w następujący sposób:

1. Losujemy liczbę $0 < r < n$ i wyznaczamy punkt rB. $u = [rB]_x$.
2. Jeżeli $u = 0$, wracamy do punktu 1.
3. Liczbę v obliczamy jako $v = (P - mu)/r \mod n$.
4. Jeżeli $v = 0$, wracamy do punktu 1.

Weryfikacja podpisu:

- Obliczamy $(s_1, s_2) = (Pv^{-1}, uv^{-1})(\mod n)$
- Obliczamy $H = s_1 B - s_2 C$.
- Jeżeli $H = \infty$, odrzucamy podpis, w przeciwnym wypadku akceptujemy podpis, gdy $u = H_x$.

Dowód: $(s_1, s_2) = (r + \frac{mu}{v}, \frac{u}{v})$
$H = \left(r + \frac{mu}{v}\right) B - \frac{u}{v} mB = rB$
$H_x = [rB]_x = u \ \square$

Jest to po prostu system podpisu elektronicznego El-Gamal, gdzie grupa $\mathbb{Z}_p^*$ została zastąpiona krzywą eliptyczną.
Z przyczyn praktycznych, nie porównujemy punktów na krzywej eliptycznej, tylko ich pierwsze współrzędne modulo n.