Dá sa matematikou zarobiť milión?

alebo

Od eliptických kriviek cez Veľkú Fermatovu vetu ku kryptografii

Jozef Širáň

STU Bratislava

Namiesto úvodu:

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov?

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať?

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo???

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q:

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q:

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$!

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

O,

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),\ (\frac{1}{4}, \pm\frac{9}{8}),$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),\ (\frac{1}{4}, \pm\frac{9}{8}),\ (\frac{-287}{1296}, \pm\frac{40879}{46656}),$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),\ (\frac{1}{4}, \pm\frac{9}{8}),\ (\frac{-287}{1296}, \pm\frac{40879}{46656}),\ (\frac{43992}{82369}, \pm\frac{30699397}{23639903}),$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),\ (\frac{1}{4}, \pm\frac{9}{8}),\ (\frac{-287}{1296}, \pm\frac{40879}{46656}),\ (\frac{43992}{82369}, \pm\frac{30699397}{23639903}),$

$(\frac{26862913}{1493284}, \pm\frac{139455877527}{1824793048}),$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),\ (\frac{1}{4}, \pm\frac{9}{8}),\ (\frac{-287}{1296}, \pm\frac{40879}{46656}),\ (\frac{43992}{82369}, \pm\frac{30699397}{23639903}),$

$(\frac{26862913}{1493284}, \pm\frac{139455877527}{1824793048}),\quad (-\frac{3596697936}{8760772801}, \pm\frac{591456591665497}{819999573400799}),\ \ldots$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),\ (\frac{1}{4}, \pm\frac{9}{8}),\ (\frac{-287}{1296}, \pm\frac{40879}{46656}),\ (\frac{43992}{82369}, \pm\frac{30699397}{23639903}),$

$(\frac{26862913}{1493284}, \pm\frac{139455877527}{1824793048}),\ \ (-\frac{3596697936}{8760772801}, \pm\frac{591456591665497}{819999573400799}),\ \ \ldots$

Pr. 3. $y^2 = x^3+x-47$ nad Q:

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$$O,\ (0. \pm 1),\ (72, \pm 611),\ (\tfrac{1}{4}, \pm\tfrac{9}{8}),\ (\tfrac{-287}{1296}, \pm\tfrac{40879}{46656}),\ (\tfrac{43992}{82369}, \pm\tfrac{30699397}{23639903}),$$

$$(\tfrac{26862913}{1493284}, \pm\tfrac{139455877527}{1824793048}),\quad (-\tfrac{3596697936}{8760772801}, \pm\tfrac{591456591665497}{819999573400799}),\ \ldots$$

Pr. 3. $y^2 = x^3+x-47$ nad Q: $E_{-47} = \{O\}$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),\ (\frac{1}{4}, \pm\frac{9}{8}),\ (\frac{-287}{1296}, \pm\frac{40879}{46656}),\ (\frac{43992}{82369}, \pm\frac{30699397}{23639903}),$

$(\frac{26862913}{1493284}, \pm\frac{139455877527}{1824793048}),\ \ (-\frac{3596697936}{8760772801}, \pm\frac{591456591665497}{819999573400799}),\ \ldots$

Pr. 3. $y^2 = x^3+x-47$ nad Q: $E_{-47} = \{O\}$

Pr. 4. $y^2 = x^3+x+9$ nad Q:

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),\ (\frac{1}{4}, \pm\frac{9}{8}),\ (\frac{-287}{1296}, \pm\frac{40879}{46656}),\ (\frac{43992}{82369}, \pm\frac{30699397}{23639903}),$

$(\frac{26862913}{1493284}, \pm\frac{139455877527}{1824793048}),\ \ (-\frac{3596697936}{8760772801}, \pm\frac{591456591665497}{819999573400799}),\ \ldots$

Pr. 3. $y^2 = x^3+x-47$ nad Q: $E_{-47} = \{O\}$

Pr. 4. $y^2 = x^3+x+9$ nad Q: $E_{+9} \cong Z \times Z$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),\ (\frac{1}{4}, \pm\frac{9}{8}),\ (\frac{-287}{1296}, \pm\frac{40879}{46656}),\ (\frac{43992}{82369}, \pm\frac{30699397}{23639903}),$

$(\frac{26862913}{1493284}, \pm\frac{139455877527}{1824793048}),\ \ (-\frac{3596697936}{8760772801}, \pm\frac{591456591665497}{819999573400799}),\ \ldots$

Pr. 3. $y^2 = x^3+x-47$ nad Q: $E_{-47} = \{O\}$

Pr. 4. $y^2 = x^3+x+9$ nad Q: $E_{+9} \cong Z \times Z$ Hmm...

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),\ (\frac{1}{4}, \pm\frac{9}{8}),\ (\frac{-287}{1296}, \pm\frac{40879}{46656}),\ (\frac{43992}{82369}, \pm\frac{30699397}{23639903}),$

$(\frac{26862913}{1493284}, \pm\frac{139455877527}{1824793048}),\ \ (-\frac{3596697936}{8760772801}, \pm\frac{591456591665497}{819999573400799}),\ \ \ldots$

Pr. 3. $y^2 = x^3+x-47$ nad Q: $E_{-47} = \{O\}$

Pr. 4. $y^2 = x^3+x+9$ nad Q: $E_{+9} \cong Z \times Z$ Hmm...

Pr. 5. Pravouhlé Δ obsahu 6 s racionálnymi dĺžkami strán a, b, c?

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),\ (\frac{1}{4}, \pm\frac{9}{8}),\ (\frac{-287}{1296}, \pm\frac{40879}{46656}),\ (\frac{43992}{82369}, \pm\frac{30699397}{23639903}),$

$(\frac{26862913}{1493284}, \pm\frac{139455877527}{1824793048}),\ \ (-\frac{3596697936}{8760772801}, \pm\frac{591456591665497}{819999573400799}),\ \ldots$

Pr. 3. $y^2 = x^3+x-47$ nad Q: $E_{-47} = \{O\}$

Pr. 4. $y^2 = x^3+x+9$ nad Q: $E_{+9} \cong Z \times Z$ Hmm...

Pr. 5. Pravouhlé Δ obsahu 6 s racionálnymi dĺžkami strán a, b, c?

$y^2 = x^3 - 36x$ nad Q: $a = (x^2-36)/y,\ b = 12x/y,\ c = (x^2+36)/y.$

Namiesto úvodu: Eliptická krivka nad poľom F char. $\neq 2, 3$ je množina

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Počet bodov? Ako ich získať? A najmä – prečo??? Najprv príkladíky:

Pr. 1. $y^2 = x^3+x+2$ nad Q: $E_{+2} = \{O, (-1, 0), (1, \pm 2)\}$

Pr. 2. $y^2 = x^3+x+1$ nad Q: $|E_{+1}| = \infty$! Niekoľko bodov:

$O,\ (0. \pm 1),\ (72, \pm 611),\ (\frac{1}{4}, \pm\frac{9}{8}),\ (\frac{-287}{1296}, \pm\frac{40879}{46656}),\ (\frac{43992}{82369}, \pm\frac{30699397}{23639903}),$

$(\frac{26862913}{1493284}, \pm\frac{139455877527}{1824793048}),\quad (-\frac{3596697936}{8760772801}, \pm\frac{591456591665497}{819999573400799}),\ \ldots$

Pr. 3. $y^2 = x^3+x-47$ nad Q: $E_{-47} = \{O\}$

Pr. 4. $y^2 = x^3+x+9$ nad Q: $E_{+9} \cong Z \times Z$ Hmm...

Pr. 5. Pravouhlé Δ obsahu 6 s racionálnymi dĺžkami strán a, b, c?

$y^2 = x^3 - 36x$ nad Q: $a = (x^2-36)/y,\ b = 12x/y,\ c = (x^2+36)/y.$

Prečo sú eliptické krivky jednou z hybných síl matematiky?

História:

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály.

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ...

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

Prirodzená parametrizácia krivky $y^2 = h(x)$ pre výpočet integrálov: $x = u(t)$, $y = u'(t)$.

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

Prirodzená parametrizácia krivky $y^2 = h(x)$ pre výpočet integrálov: $x = u(t)$, $y = u'(t)$. Funkciu u nájdeme takto:

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

Prirodzená parametrizácia krivky $y^2 = h(x)$ pre výpočet integrálov: $x = u(t)$, $y = u'(t)$. Funkciu u nájdeme takto: Z $y = u'(t) = dx/dt$ máme $dt/dx = 1/y$ a potom $t = \int dx/y = \int dx/\sqrt{h(x)} = u^{-1}(x)$.

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

Prirodzená parametrizácia krivky $y^2 = h(x)$ pre výpočet integrálov: $x = u(t)$, $y = u'(t)$. Funkciu u nájdeme takto: Z $y = u'(t) = dx/dt$ máme $dt/dx = 1/y$ a potom $t = \int dx/y = \int dx/\sqrt{h(x)} = u^{-1}(x)$.

Meromorfná $f : \mathcal{C} \to \mathcal{C}$ je eliptická vzhľadom k mriežke $\Omega = \langle \omega_1, \omega_2 \rangle$ (t.j. *dvojito periodická*), ak $f(z + \omega) = f(z)$ pre všetky $z \in \mathcal{C}$ a $\omega \in \Omega$.

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

Prirodzená parametrizácia krivky $y^2 = h(x)$ pre výpočet integrálov: $x = u(t)$, $y = u'(t)$. Funkciu u nájdeme takto: Z $y = u'(t) = dx/dt$ máme $dt/dx = 1/y$ a potom $t = \int dx/y = \int dx/\sqrt{h(x)} = u^{-1}(x)$.

Meromorfná $f : \mathcal{C} \to \mathcal{C}$ je eliptická vzhľadom k mriežke $\Omega = \langle \omega_1, \omega_2 \rangle$ (t.j. *dvojito periodická*), ak $f(z + \omega) = f(z)$ pre všetky $z \in \mathcal{C}$ a $\omega \in \Omega$.

Weierstrassova eliptická f.: $f(z) = z^{-2} + \sum_{\omega \in \Omega'}((z-\omega)^{-2} - \omega^{-2})$.

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

Prirodzená parametrizácia krivky $y^2 = h(x)$ pre výpočet integrálov: $x = u(t)$, $y = u'(t)$. Funkciu u nájdeme takto: Z $y = u'(t) = dx/dt$ máme $dt/dx = 1/y$ a potom $t = \int dx/y = \int dx/\sqrt{h(x)} = u^{-1}(x)$.

Meromorfná $f : \mathcal{C} \to \mathcal{C}$ je eliptická vzhľadom k mriežke $\Omega = \langle \omega_1, \omega_2 \rangle$ (t.j. *dvojito periodická*), ak $f(z + \omega) = f(z)$ pre všetky $z \in \mathcal{C}$ a $\omega \in \Omega$.

Weierstrassova eliptická f.: $f(z) = z^{-2} + \sum_{\omega \in \Omega'}((z-\omega)^{-2} - \omega^{-2})$.

Prekvapenie 1:

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

Prirodzená parametrizácia krivky $y^2 = h(x)$ pre výpočet integrálov: $x = u(t)$, $y = u'(t)$. Funkciu u nájdeme takto: Z $y = u'(t) = dx/dt$ máme $dt/dx = 1/y$ a potom $t = \int dx/y = \int dx/\sqrt{h(x)} = u^{-1}(x)$.

Meromorfná $f : \mathcal{C} \to \mathcal{C}$ je eliptická vzhľadom k mriežke $\Omega = \langle \omega_1, \omega_2 \rangle$ (t.j. *dvojito periodická*), ak $f(z + \omega) = f(z)$ pre všetky $z \in \mathcal{C}$ a $\omega \in \Omega$.

Weierstrassova eliptická f.: $f(z) = z^{-2} + \sum_{\omega \in \Omega'}((z-\omega)^{-2} - \omega^{-2})$.

Prekvapenie 1: Prirodzená parametrizácia $x = f(z)$, $y = f'(z)$ definuje eliptickú krivku $E : (y/2)^2 = h(x) = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$.

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

Prirodzená parametrizácia krivky $y^2 = h(x)$ pre výpočet integrálov: $x = u(t)$, $y = u'(t)$. Funkciu u nájdeme takto: Z $y = u'(t) = dx/dt$ máme $dt/dx = 1/y$ a potom $t = \int dx/y = \int dx/\sqrt{h(x)} = u^{-1}(x)$.

Meromorfná $f : \mathcal{C} \to \mathcal{C}$ je eliptická vzhľadom k mriežke $\Omega = \langle \omega_1, \omega_2 \rangle$ (t.j. *dvojito periodická*), ak $f(z + \omega) = f(z)$ pre všetky $z \in \mathcal{C}$ a $\omega \in \Omega$.

Weierstrassova eliptická f.: $f(z) = z^{-2} + \sum_{\omega \in \Omega'}((z-\omega)^{-2} - \omega^{-2})$.

Prekvapenie 1: Prirodzená parametrizácia $x = f(z)$, $y = f'(z)$ definuje eliptickú krivku $E : (y/2)^2 = h(x) = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$. Ako vyššie, $z = \int dx/y = \int dx/\sqrt{h(x)} = f^{-1}(x)$

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

Prirodzená parametrizácia krivky $y^2 = h(x)$ pre výpočet integrálov: $x = u(t)$, $y = u'(t)$. Funkciu u nájdeme takto: Z $y = u'(t) = dx/dt$ máme $dt/dx = 1/y$ a potom $t = \int dx/y = \int dx/\sqrt{h(x)} = u^{-1}(x)$.

Meromorfná $f : \mathcal{C} \to \mathcal{C}$ je eliptická vzhľadom k mriežke $\Omega = \langle \omega_1, \omega_2 \rangle$ (t.j. *dvojito periodická*), ak $f(z + \omega) = f(z)$ pre všetky $z \in \mathcal{C}$ a $\omega \in \Omega$.

Weierstrassova eliptická f.: $f(z) = z^{-2} + \sum_{\omega \in \Omega'}((z-\omega)^{-2} - \omega^{-2})$.

Prekvapenie 1: Prirodzená parametrizácia $x = f(z)$, $y = f'(z)$ definuje eliptickú krivku $E : (y/2)^2 = h(x) = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$. Ako vyššie, $z = \int dx/y = \int dx/\sqrt{h(x)} = f^{-1}(x)$ ... opäť inverzia integrálu!

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

Prirodzená parametrizácia krivky $y^2 = h(x)$ pre výpočet integrálov: $x = u(t)$, $y = u'(t)$. Funkciu u nájdeme takto: Z $y = u'(t) = dx/dt$ máme $dt/dx = 1/y$ a potom $t = \int dx/y = \int dx/\sqrt{h(x)} = u^{-1}(x)$.

Meromorfná $f : \mathcal{C} \to \mathcal{C}$ je eliptická vzhľadom k mriežke $\Omega = \langle \omega_1, \omega_2 \rangle$ (t.j. *dvojito periodická*), ak $f(z + \omega) = f(z)$ pre všetky $z \in \mathcal{C}$ a $\omega \in \Omega$.

Weierstrassova eliptická f.: $f(z) = z^{-2} + \sum_{\omega \in \Omega'}((z-\omega)^{-2} - \omega^{-2})$.

Prekvapenie 1: Prirodzená parametrizácia $x = f(z)$, $y = f'(z)$ definuje eliptickú krivku $E : (y/2)^2 = h(x) = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$. Ako vyššie, $z = \int dx/y = \int dx/\sqrt{h(x)} = f^{-1}(x)$ ... opäť inverzia integrálu!

Prekvapenie 2:

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

Prirodzená parametrizácia krivky $y^2 = h(x)$ pre výpočet integrálov: $x = u(t)$, $y = u'(t)$. Funkciu u nájdeme takto: Z $y = u'(t) = dx/dt$ máme $dt/dx = 1/y$ a potom $t = \int dx/y = \int dx/\sqrt{h(x)} = u^{-1}(x)$.

Meromorfná $f : \mathcal{C} \to \mathcal{C}$ je eliptická vzhľadom k mriežke $\Omega = \langle \omega_1, \omega_2 \rangle$ (t.j. *dvojito periodická*), ak $f(z + \omega) = f(z)$ pre všetky $z \in \mathcal{C}$ a $\omega \in \Omega$.

Weierstrassova eliptická f.: $f(z) = z^{-2} + \sum_{\omega \in \Omega'}((z-\omega)^{-2} - \omega^{-2})$.

Prekvapenie 1: Prirodzená parametrizácia $x = f(z)$, $y = f'(z)$ definuje eliptickú krivku $E : (y/2)^2 = h(x) = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$. Ako vyššie, $z = \int dx/y = \int dx/\sqrt{h(x)} = f^{-1}(x)$ ... opäť inverzia integrálu!

Prekvapenie 2: $z \mapsto (f(z), f'(z)) = (x, y)$ je homeo $\mathcal{C}/\Omega \simeq E$

História: Prečo *názov* eliptické krivky? A prečo záujem o ne?

Cca 1670: $\int g(x, \sqrt{h(x)})dx$, $\deg(h) = 3, 4$; obvod elipsy, lemniskáty.

Gauss, cca 1800: Nápad *invertovať* eliptické integrály. Príklad: Tak, ako reálna inverzná funkcia k $\int dx/\sqrt{1-x^2}$ je periodická, komplexná inverzná funkcia k $\int dx/\sqrt{1-x^4}$ je *dvojito periodická*. ... Kontext nápadu?

Prirodzená parametrizácia krivky $y^2 = h(x)$ pre výpočet integrálov: $x = u(t)$, $y = u'(t)$. Funkciu u nájdeme takto: Z $y = u'(t) = dx/dt$ máme $dt/dx = 1/y$ a potom $t = \int dx/y = \int dx/\sqrt{h(x)} = u^{-1}(x)$.

Meromorfná $f : \mathcal{C} \to \mathcal{C}$ je eliptická vzhľadom k mriežke $\Omega = \langle \omega_1, \omega_2 \rangle$ (t.j. *dvojito periodická*), ak $f(z + \omega) = f(z)$ pre všetky $z \in \mathcal{C}$ a $\omega \in \Omega$.

Weierstrassova eliptická f.: $f(z) = z^{-2} + \sum_{\omega \in \Omega'}((z-\omega)^{-2} - \omega^{-2})$.

Prekvapenie 1: Prirodzená parametrizácia $x = f(z)$, $y = f'(z)$ definuje eliptickú krivku $E : (y/2)^2 = h(x) = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$. Ako vyššie, $z = \int dx/y = \int dx/\sqrt{h(x)} = f^{-1}(x)$ ... opäť inverzia integrálu!

Prekvapenie 2: $z \mapsto (f(z), f'(z)) = (x, y)$ je homeo $\mathcal{C}/\Omega \simeq E$ ... torus!

Ako zarobiť milión:

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa!

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E \backslash \{O\}$, tak $P_1 + P_2 = (x, -y)$, kde (x, y) je tretí bod na E kolineárny s P_1, P_2.

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E \backslash \{O\}$, tak $P_1 + P_2 = (x, -y)$, kde (x, y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E \backslash \{O\}$, tak $2P = (x, -y)$, kde $(x, y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E.

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E \backslash \{O\}$, tak $P_1 + P_2 = (x, -y)$, kde (x, y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E \backslash \{O\}$, tak $2P = (x, -y)$, kde $(x, y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E \backslash \{O\}$, tak $P_1 + P_2 = (x, -y)$, kde (x, y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E \backslash \{O\}$, tak $2P = (x, -y)$, kde $(x, y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

L. Mordell 1922 (H. Weyl; hypotéza H. Poincaré 1901); B. Mazur 1977: $E(Q) \simeq A \times Z^r$; $A \simeq Z_n$ alebo $Z_2 \times Z_{2m}$, $n \in \{1, \ldots, 10, 12\}$, $1 \leq m \leq 4$.

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E \backslash \{O\}$, tak $P_1 + P_2 = (x, -y)$, kde (x, y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E \backslash \{O\}$, tak $2P = (x, -y)$, kde $(x, y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

L. Mordell 1922 (H. Weyl; hypotéza H. Poincaré 1901); B. Mazur 1977: $E(Q) \simeq A \times Z^r$; $A \simeq Z_n$ alebo $Z_2 \times Z_{2m}$, $n \in \{1, \ldots, 10, 12\}$, $1 \leq m \leq 4$.

Nech $E = E(Q) :\ y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$, $a, b \in Z$,

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E \backslash \{O\}$, tak $P_1 + P_2 = (x, -y)$, kde (x, y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E \backslash \{O\}$, tak $2P = (x, -y)$, kde $(x, y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

L. Mordell 1922 (H. Weyl; hypotéza H. Poincaré 1901); B. Mazur 1977: $E(Q) \simeq A \times Z^r$; $A \simeq Z_n$ alebo $Z_2 \times Z_{2m}$, $n \in \{1, \ldots, 10, 12\}$, $1 \leq m \leq 4$.

Nech $E = E(Q) :\ y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$, $a, b \in Z$, a nech $E_p :\ y^2 = x^3 + ax + b \bmod p$;

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E \backslash \{O\}$, tak $P_1 + P_2 = (x, -y)$, kde (x, y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E \backslash \{O\}$, tak $2P = (x, -y)$, kde $(x, y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

L. Mordell 1922 (H. Weyl; hypotéza H. Poincaré 1901); B. Mazur 1977: $E(Q) \simeq A \times Z^r$; $A \simeq Z_n$ alebo $Z_2 \times Z_{2m}$, $n \in \{1, \ldots, 10, 12\}$, $1 \leq m \leq 4$.

Nech $E = E(Q):\ y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$, $a, b \in Z$, a nech $E_p:\ y^2 = x^3 + ax + b \bmod p$; p je *dobré*, ak E_p je opäť eliptická krivka.

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E \backslash \{O\}$, tak $P_1 + P_2 = (x, -y)$, kde (x, y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E \backslash \{O\}$, tak $2P = (x, -y)$, kde $(x, y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

L. Mordell 1922 (H. Weyl; hypotéza H. Poincaré 1901); B. Mazur 1977: $E(Q) \simeq A \times Z^r$; $A \simeq Z_n$ alebo $Z_2 \times Z_{2m}$, $n \in \{1, \ldots, 10, 12\}$, $1 \leq m \leq 4$.

Nech $E = E(Q):\ y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$, $a, b \in Z$, a nech $E_p:\ y^2 = x^3 + ax + b \bmod p$; p je *dobré*, ak E_p je opäť eliptická krivka.

H. Hasse, A. Weil 1977: $n_p := |E_p| = p + 1 - a_p$, pričom $|a_p| < 2\sqrt{p}$.

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E \backslash \{O\}$, tak $P_1 + P_2 = (x, -y)$, kde (x, y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E \backslash \{O\}$, tak $2P = (x, -y)$, kde $(x, y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

L. Mordell 1922 (H. Weyl; hypotéza H. Poincaré 1901); B. Mazur 1977: $E(Q) \simeq A \times Z^r$; $A \simeq Z_n$ alebo $Z_2 \times Z_{2m}$, $n \in \{1, \ldots, 10, 12\}$, $1 \leq m \leq 4$.

Nech $E = E(Q):\ y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$, $a, b \in Z$, a nech $E_p:\ y^2 = x^3 + ax + b \bmod p$; p je *dobré*, ak E_p je opäť eliptická krivka.

H. Hasse, A. Weil 1977: $n_p := |E_p| = p + 1 - a_p$, pričom $|a_p| < 2\sqrt{p}$.

Hypotéza Birch, Swinnerton-Dyer, nie 10^6:

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E \backslash \{O\}$, tak $P_1 + P_2 = (x, -y)$, kde (x, y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E \backslash \{O\}$, tak $2P = (x, -y)$, kde $(x, y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

L. Mordell 1922 (H. Weyl; hypotéza H. Poincaré 1901); B. Mazur 1977: $E(Q) \simeq A \times Z^r$; $A \simeq Z_n$ alebo $Z_2 \times Z_{2m}$, $n \in \{1, \ldots, 10, 12\}$, $1 \leq m \leq 4$.

Nech $E = E(Q):\ y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$, $a, b \in Z$, a nech $E_p:\ y^2 = x^3 + ax + b \bmod p$; p je *dobré*, ak E_p je opäť eliptická krivka.

H. Hasse, A. Weil 1977: $n_p := |E_p| = p + 1 - a_p$, pričom $|a_p| < 2\sqrt{p}$.

Hypotéza Birch, Swinnerton-Dyer, nie 10^6: $\prod'_{p \leq x} n_p p^{-1} \approx (\log x)^r$.

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E \backslash \{O\}$, tak $P_1 + P_2 = (x, -y)$, kde (x, y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E \backslash \{O\}$, tak $2P = (x, -y)$, kde $(x, y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

L. Mordell 1922 (H. Weyl; hypotéza H. Poincaré 1901); B. Mazur 1977: $E(Q) \simeq A \times Z^r$; $A \simeq Z_n$ alebo $Z_2 \times Z_{2m}$, $n \in \{1, \ldots, 10, 12\}$, $1 \leq m \leq 4$.

Nech $E = E(Q):\ y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$, $a, b \in Z$, a nech $E_p:\ y^2 = x^3 + ax + b \bmod p$; p je *dobré*, ak E_p je opäť eliptická krivka.

H. Hasse, A. Weil 1977: $n_p := |E_p| = p + 1 - a_p$, pričom $|a_p| < 2\sqrt{p}$.

Hypotéza Birch, Swinnerton-Dyer, nie 10^6: $\prod'_{p \leq x} n_p p^{-1} \approx (\log x)^r$.

Nech $L(E, s) = \prod'_p (1 - a_p p^{-s} + p^{1-2s})^{-1}$

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$E = \{O\} \cup \{(x,y) \in F^2;\ y^2 = x^3 + ax + b,\ a,b \in F,\ 4a^3 + 27b^2 \neq 0\}$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E\backslash\{O\}$, tak $P_1 + P_2 = (x,-y)$, kde (x,y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E\backslash\{O\}$, tak $2P = (x,-y)$, kde $(x,y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

L. Mordell 1922 (H. Weyl; hypotéza H. Poincaré 1901); B. Mazur 1977: $E(Q) \simeq A \times Z^r$; $A \simeq Z_n$ alebo $Z_2 \times Z_{2m}$, $n \in \{1,\ldots,10,12\}$, $1 \leq m \leq 4$.

Nech $E = E(Q):\ y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$, $a,b \in Z$, a nech $E_p:\ y^2 = x^3 + ax + b \bmod p$; p je *dobré*, ak E_p je opäť eliptická krivka.

H. Hasse, A. Weil 1977: $n_p := |E_p| = p + 1 - a_p$, pričom $|a_p| < 2\sqrt{p}$.

Hypotéza Birch, Swinnerton-Dyer, nie 10^6: $\prod'_{p \leq x} n_p p^{-1} \approx (\log x)^r$.

Nech $L(E,s) = \prod'_p (1 - a_p p^{-s} + p^{1-2s})^{-1} = \sum_{n \geq 1} c_n n^{-s}$,

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$E = \{O\} \cup \{(x, y) \in F^2;\ y^2 = x^3 + ax + b,\ a, b \in F,\ 4a^3 + 27b^2 \neq 0\}$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E \backslash \{O\}$, tak $P_1 + P_2 = (x, -y)$, kde (x, y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E \backslash \{O\}$, tak $2P = (x, -y)$, kde $(x, y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

L. Mordell 1922 (H. Weyl; hypotéza H. Poincaré 1901); B. Mazur 1977: $E(Q) \simeq A \times Z^r$; $A \simeq Z_n$ alebo $Z_2 \times Z_{2m}$, $n \in \{1, \ldots, 10, 12\}$, $1 \leq m \leq 4$.

Nech $E = E(Q):\ y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$, $a, b \in Z$, a nech $E_p:\ y^2 = x^3 + ax + b \bmod p$; p je *dobré*, ak E_p je opäť eliptická krivka.

H. Hasse, A. Weil 1977: $n_p := |E_p| = p + 1 - a_p$, pričom $|a_p| < 2\sqrt{p}$.

Hypotéza Birch, Swinnerton-Dyer, nie 10^6: $\prod'_{p \leq x} n_p p^{-1} \approx (\log x)^r$.

Nech $L(E, s) = \prod'_p (1 - a_p p^{-s} + p^{1-2s})^{-1} = \sum_{n \geq 1} c_n n^{-s}$, rozšírená na $\mathcal{C}$.

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$E = \{O\} \cup \{(x,y) \in F^2;\ y^2 = x^3 + ax + b,\ a,b \in F,\ 4a^3 + 27b^2 \neq 0\}$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E\backslash\{O\}$, tak $P_1 + P_2 = (x,-y)$, kde (x,y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E\backslash\{O\}$, tak $2P = (x,-y)$, kde $(x,y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

L. Mordell 1922 (H. Weyl; hypotéza H. Poincaré 1901); B. Mazur 1977: $E(Q) \simeq A \times Z^r$; $A \simeq Z_n$ alebo $Z_2 \times Z_{2m}$, $n \in \{1,\ldots,10,12\}$, $1 \leq m \leq 4$.

Nech $E = E(Q):\ y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$, $a,b \in Z$, a nech $E_p:\ y^2 = x^3 + ax + b \bmod p$; p je *dobré*, ak E_p je opäť eliptická krivka.

H. Hasse, A. Weil 1977: $n_p := |E_p| = p + 1 - a_p$, pričom $|a_p| < 2\sqrt{p}$.

Hypotéza Birch, Swinnerton-Dyer, nie 10^6: $\prod'_{p \leq x} n_p p^{-1} \approx (\log x)^r$.

Nech $L(E,s) = \prod'_p (1 - a_p p^{-s} + p^{1-2s})^{-1} = \sum_{n \geq 1} c_n n^{-s}$, rozšírená na $\mathcal{C}$.

Birch, Swinnerton-Dyer, 10^6:

Ako zarobiť milión: Hypotéza – B. Birch a P. Swinnerton-Dyer 1965

$E = \{O\} \cup \{(x,y) \in F^2;\ y^2 = x^3 + ax + b,\ a,b \in F,\ 4a^3 + 27b^2 \neq 0\}$

Prekvapenie 3: Poincaré 1901: E je aditívna grupa! Operácia sčítania:

Ak $P_1 \neq P_2 \in E\backslash\{O\}$, tak $P_1 + P_2 = (x,-y)$, kde (x,y) je tretí bod na E kolineárny s P_1, P_2. Ak $P \in E\backslash\{O\}$, tak $2P = (x,-y)$, kde $(x,y) \in E$ je druhý priesečník dotyčnice k E v P s krivkou E. Prvok O je nulou v E.

L. Mordell 1922 (H. Weyl; hypotéza H. Poincaré 1901); B. Mazur 1977: $E(Q) \simeq A \times Z^r$; $A \simeq Z_n$ alebo $Z_2 \times Z_{2m}$, $n \in \{1,\ldots,10,12\}$, $1 \leq m \leq 4$.

Nech $E = E(Q):\ y^2 = x^3 + ax + b$, $4a^3 + 27b^2 \neq 0$, $a,b \in Z$, a nech $E_p:\ y^2 = x^3 + ax + b \bmod p$; p je *dobré*, ak E_p je opäť eliptická krivka.

H. Hasse, A. Weil 1977: $n_p := |E_p| = p + 1 - a_p$, pričom $|a_p| < 2\sqrt{p}$.

Hypotéza Birch, Swinnerton-Dyer, nie 10^6: $\prod'_{p \leq x} n_p p^{-1} \approx (\log x)^r$.

Nech $L(E,s) = \prod'_p (1 - a_p p^{-s} + p^{1-2s})^{-1} = \sum_{n \geq 1} c_n n^{-s}$, rozšírená na $\mathcal{C}$.

Birch, Swinnerton-Dyer, 10^6: $s{=}1$ je r-násobným koreňom fukcie $L(E,s)$.

Ako už bol zarobený ‘milión’:

Ako už bol zarobený ‘milión’: Eliptické krivky a Veľká Fermatova veta

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.

Ako už bol zarobený ‘milión’: Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv:

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$,

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne,

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^* : y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^*: \ y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^*: y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Modulárnosť:

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^* : y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Modulárnosť': $E = E(Q) : y^2 = x^3 + ax + b$, $a, b \in Z$, $4a^3 + 27b^2 \neq 0$;
$E_p : y^2 = x^3 + ax + b \bmod p$.

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^* : y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Modulárnosť': $E = E(Q) : y^2 = x^3 + ax + b$, $a, b \in Z$, $4a^3 + 27b^2 \neq 0$;
$E_p : y^2 = x^3 + ax + b \bmod p$. *Dobré p* je také, že E_p je opäť eliptická krivka (nad F_p).

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^* : y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Modulárnosť: $E = E(Q) : y^2 = x^3 + ax + b$, $a, b \in Z$, $4a^3 + 27b^2 \neq 0$;
$E_p : y^2 = x^3 + ax + b \bmod p$. *Dobré p* je také, že E_p je opäť eliptická krivka (nad F_p). Ak p je dobré, tak $a_p := p + 1 - |E_p|$

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^* : y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Modulárnosť: $E = E(Q) : y^2 = x^3 + ax + b$, $a, b \in Z$, $4a^3+27b^2 \neq 0$;
$E_p : y^2 = x^3 + ax + b \bmod p$. *Dobré p* je také, že E_p je opäť eliptická krivka (nad F_p). Ak p je dobré, tak $a_p := p + 1 - |E_p|$ (HW: $|a_p| < 2\sqrt{p}$).

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^* : y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Modulárnosť: $E = E(Q) : y^2 = x^3 + ax + b$, $a, b \in Z$, $4a^3+27b^2 \neq 0$;
$E_p : y^2 = x^3 + ax + b \bmod p$. *Dobré p* je také, že E_p je opäť eliptická krivka (nad F_p). Ak p je dobré, tak $a_p := p + 1 - |E_p|$ (HW: $|a_p| < 2\sqrt{p}$).
Ak nie, $a_p := 0$ ak E_p má 3-nás. koreň;

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^* : y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Modulárnosť: $E = E(Q) : y^2 = x^3 + ax + b$, $a, b \in Z$, $4a^3+27b^2 \neq 0$;
$E_p : y^2 = x^3 + ax + b \bmod p$. *Dobré p* je také, že E_p je opäť eliptická krivka (nad F_p). Ak p je dobré, tak $a_p := p + 1 - |E_p|$ (HW: $|a_p| < 2\sqrt{p}$). Ak nie, $a_p := 0$ ak E_p má 3-nás. koreň; $a_p := 1$ ak E_p má 2-nás. koreň a smernice dotyčníc v ňom sú v F_p;

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^* : y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Modulárnosť: $E = E(Q) : y^2 = x^3 + ax + b$, $a, b \in Z$, $4a^3+27b^2 \neq 0$; $E_p : y^2 = x^3 + ax + b \bmod p$. *Dobré p* je také, že E_p je opäť eliptická krivka (nad F_p). Ak p je dobré, tak $a_p := p + 1 - |E_p|$ (HW: $|a_p| < 2\sqrt{p}$). Ak nie, $a_p := 0$ ak E_p má 3-nás. koreň; $a_p := 1$ ak E_p má 2-nás. koreň a smernice dotyčníc v ňom sú v F_p; $a_p := -1$ inak. Ak $q = p^t$, tak a_q máme z $(1 - a_p p^{-s} + p^{1-2s})^{-1} = 1 + \sum_{t \geq 1} a_{p^t} p^{-st}$.

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^* : y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Modulárnosť: $E = E(Q) : y^2 = x^3 + ax + b$, $a, b \in Z$, $4a^3+27b^2 \neq 0$; $E_p : y^2 = x^3 + ax + b \bmod p$. *Dobré p* je také, že E_p je opäť eliptická krivka (nad F_p). Ak p je dobré, tak $a_p := p + 1 - |E_p|$ (HW: $|a_p| < 2\sqrt{p}$). Ak nie, $a_p := 0$ ak E_p má 3-nás. koreň; $a_p := 1$ ak E_p má 2-nás. koreň a smernice dotyčníc v ňom sú v F_p; $a_p := -1$ inak. Ak $q = p^t$, tak a_q máme z $(1 - a_p p^{-s} + p^{1-2s})^{-1} = 1 + \sum_{t \geq 1} a_{p^t} p^{-st}$. Multiplikatívne: a_n pre $n \in N$.

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^* : y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Modulárnosť: $E = E(Q) : y^2 = x^3 + ax + b$, $a, b \in Z$, $4a^3+27b^2 \neq 0$; $E_p : y^2 = x^3 + ax + b \bmod p$. *Dobré p* je také, že E_p je opäť eliptická krivka (nad F_p). Ak p je dobré, tak $a_p := p + 1 - |E_p|$ (HW: $|a_p| < 2\sqrt{p}$). Ak nie, $a_p := 0$ ak E_p má 3-nás. koreň; $a_p := 1$ ak E_p má 2-nás. koreň a smernice dotyčníc v ňom sú v F_p; $a_p := -1$ inak. Ak $q = p^t$, tak a_q máme z $(1 - a_p p^{-s} + p^{1-2s})^{-1} = 1 + \sum_{t \geq 1} a_{p^t} p^{-st}$. Multiplikatívne: a_n pre $n \in N$. Pre každé $w \in \mathcal{H} = \{z \in \mathcal{C};\ Im(z) > 0\}$ nech $f_E(w) = \sum_n a_n \exp(2\pi i w n)$.

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^* : y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Modulárnosť: $E = E(Q) : y^2 = x^3 + ax + b$, $a, b \in Z$, $4a^3+27b^2 \neq 0$; $E_p : y^2 = x^3 + ax + b \bmod p$. *Dobré p* je také, že E_p je opäť eliptická krivka (nad F_p). Ak p je dobré, tak $a_p := p + 1 - |E_p|$ (HW: $|a_p| < 2\sqrt{p}$). Ak nie, $a_p := 0$ ak E_p má 3-nás. koreň; $a_p := 1$ ak E_p má 2-nás. koreň a smernice dotyčníc v ňom sú v F_p; $a_p := -1$ inak. Ak $q = p^t$, tak a_q máme z $(1 - a_p p^{-s} + p^{1-2s})^{-1} = 1 + \sum_{t \geq 1} a_{p^t} p^{-st}$. Multiplikatívne: a_n pre $n \in N$. Pre každé $w \in \mathcal{H} = \{z \in \mathcal{C};\ Im(z) > 0\}$ nech $f_E(w) = \sum_n a_n \exp(2\pi i w n)$.

E je modulárna, ak existuje $j \in N$; že pre každé $w \in \mathcal{H}$ a $\alpha, \beta, \gamma, \delta \in Z$, $\alpha\delta - \beta\gamma = 1$, $\gamma \equiv 0 \bmod j$, platí: $f_E(\frac{\alpha w + \beta}{\gamma w + \delta}) = (\gamma w + \delta)^2 f_E(w)$.

Ako už bol zarobený 'milión': Eliptické krivky a Veľká Fermatova veta

Nech $k^p + \ell^p = m^p$ pre nejaké $k, \ell, m \in N$ a nepárne prvočíslo p.
Búnv: $(k, \ell, m) = 1$, ℓ je párne, $k \equiv -1 \bmod 4$.

Frey, Serre; Ribet 1990: *Ak existujú k, ℓ, m ako vyššie, tak eliptická krivka $E_p^* : y^2 = x(x - k^p)(x + \ell^p)$ nad Q nie je modulárna.*

Wiles (a Taylor) 1995: *Každá eliptická krivka nad Q je modulárna.* □

Modulárnosť: $E = E(Q) : y^2 = x^3 + ax + b$, $a, b \in Z$, $4a^3+27b^2 \neq 0$; $E_p : y^2 = x^3 + ax + b \bmod p$. *Dobré p* je také, že E_p je opäť eliptická krivka (nad F_p). Ak p je dobré, tak $a_p := p + 1 - |E_p|$ (HW: $|a_p| < 2\sqrt{p}$). Ak nie, $a_p := 0$ ak E_p má 3-nás. koreň; $a_p := 1$ ak E_p má 2-nás. koreň a smernice dotyčníc v ňom sú v F_p; $a_p := -1$ inak. Ak $q = p^t$, tak a_q máme z $(1-a_p p^{-s}+p^{1-2s})^{-1} = 1 + \sum_{t \geq 1} a_{p^t} p^{-st}$. Multiplikatívne: a_n pre $n \in N$. Pre každé $w \in \mathcal{H} = \{z \in \mathcal{C};\ Im(z) > 0\}$ nech $f_E(w) = \sum_n a_n \exp(2\pi i w n)$.

E je modulárna, ak existuje $j \in N$; že pre každé $w \in \mathcal{H}$ a $\alpha, \beta, \gamma, \delta \in Z$, $\alpha\delta - \beta\gamma = 1$, $\gamma \equiv 0 \bmod j$, platí: $f_E(\frac{\alpha w+\beta}{\gamma w+\delta}) = (\gamma w + \delta)^2 f_E(w)$. Hmm...

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

DiscLogProb pre $E(F_p)$: Pre $P, P' \in E$ určiť s mod p tak, aby $P' = sP$.

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

DiscLogProb pre $E(F_p)$: Pre $P, P' \in E$ určiť s mod p tak, aby $P' = sP$.
Zatiaľ sa nenašiel algoritmus polynomiálnej zložitosti v p na určenie s.

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

DiscLogProb pre $E(F_p)$: Pre $P, P' \in E$ určiť s mod p tak, aby $P' = sP$. Zatiaľ sa nenašiel algoritmus polynomiálnej zložitosti v p na určenie s.

Najjednoduchší druh eliptického kryptosystému (ElGamal) pre $A \to B$:

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

DiscLogProb pre $E(F_p)$: Pre $P, P' \in E$ určiť s mod p tak, aby $P' = sP$. Zatiaľ sa nenašiel algoritmus polynomiálnej zložitosti v p na určenie s.

Najjednoduchší druh eliptického kryptosystému (ElGamal) pre $A \to B$:

1. B vyberie krivku E nad F_p a bod $P \in E$ (obvykle veľkého prvočíselného rádu); ďalej vyberie s mod p a vypočíta $P' = sP$.

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

DiscLogProb pre $E(F_p)$: Pre $P, P' \in E$ určiť s mod p tak, aby $P' = sP$. Zatiaľ sa nenašiel algoritmus polynomiálnej zložitosti v p na určenie s.

Najjednoduchší druh eliptického kryptosystému (ElGamal) pre $A \to B$:

1. B vyberie krivku E nad F_p a bod $P \in E$ (obvykle veľkého prvočíselného rádu); ďalej vyberie s mod p a vypočíta $P' = sP$. Štvorica (p, E, P, P') je verejným kľúčom a s je súkromným kľúčom účastníka B.

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

DiscLogProb pre $E(F_p)$: Pre $P, P' \in E$ určiť s mod p tak, aby $P' = sP$. Zatiaľ sa nenašiel algoritmus polynomiálnej zložitosti v p na určenie s.

Najjednoduchší druh eliptického kryptosystému (ElGamal) pre $A \to B$:

1. B vyberie krivku E nad F_p a bod $P \in E$ (obvykle veľkého prvočíselného rádu); ďalej vyberie s mod p a vypočíta $P' = sP$. Štvorica (p, E, P, P') je verejným kľúčom a s je súkromným kľúčom účastníka B.

2. A zakóduje svoju správu v tvare bodu $M \in E$, náhodne vygeneruje k mod p, vypočíta $M_1 = kP$, $M_2 = M + kP'$ a odošle M_1, M_2 ku B.

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

DiscLogProb pre $E(F_p)$: Pre $P, P' \in E$ určiť s mod p tak, aby $P' = sP$. Zatiaľ sa nenašiel algoritmus polynomiálnej zložitosti v p na určenie s.

Najjednoduchší druh eliptického kryptosystému (ElGamal) pre $A \to B$:

1. B vyberie krivku E nad F_p a bod $P \in E$ (obvykle veľkého prvočíselného rádu); ďalej vyberie s mod p a vypočíta $P' = sP$. Štvorica (p, E, P, P') je verejným kľúčom a s je súkromným kľúčom účastníka B.

2. A zakóduje svoju správu v tvare bodu $M \in E$, náhodne vygeneruje k mod p, vypočíta $M_1 = kP$, $M_2 = M + kP'$ a odošle M_1, M_2 ku B.

3. B rozšifruje správu výpočtom $M_2 - sM_1$

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

DiscLogProb pre $E(F_p)$: Pre $P, P' \in E$ určiť s mod p tak, aby $P' = sP$. Zatiaľ sa nenašiel algoritmus polynomiálnej zložitosti v p na určenie s.

Najjednoduchší druh eliptického kryptosystému (ElGamal) pre $A \to B$:

1. B vyberie krivku E nad F_p a bod $P \in E$ (obvykle veľkého prvočíselného rádu); ďalej vyberie s mod p a vypočíta $P' = sP$. Štvorica (p, E, P, P') je verejným kľúčom a s je súkromným kľúčom účastníka B.

2. A zakóduje svoju správu v tvare bodu $M \in E$, náhodne vygeneruje k mod p, vypočíta $M_1 = kP$, $M_2 = M + kP'$ a odošle M_1, M_2 ku B.

3. B rozšifruje správu výpočtom $M_2 - sM_1 = M + kP' - s(kP) = M$.

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

DiscLogProb pre $E(F_p)$: Pre $P, P' \in E$ určiť s mod p tak, aby $P' = sP$. Zatiaľ sa nenašiel algoritmus polynomiálnej zložitosti v p na určenie s.

Najjednoduchší druh eliptického kryptosystému (ElGamal) pre $A \to B$:

1. B vyberie krivku E nad F_p a bod $P \in E$ (obvykle veľkého prvočíselného rádu); ďalej vyberie s mod p a vypočíta $P' = sP$. Štvorica (p, E, P, P') je verejným kľúčom a s je súkromným kľúčom účastníka B.

2. A zakóduje svoju správu v tvare bodu $M \in E$, náhodne vygeneruje k mod p, vypočíta $M_1 = kP$, $M_2 = M + kP'$ a odošle M_1, M_2 ku B.

3. B rozšifruje správu výpočtom $M_2 - sM_1 = M + kP' - s(kP) = M$.

Príklad: Krivka sepc160k1 – súčasť Firefox: $E: \ y^2 = x^3 + 7$ nad Z_p

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

DiscLogProb pre $E(F_p)$: Pre $P, P' \in E$ určiť s mod p tak, aby $P' = sP$. Zatiaľ sa nenašiel algoritmus polynomiálnej zložitosti v p na určenie s.

Najjednoduchší druh eliptického kryptosystému (ElGamal) pre $A \to B$:

1. B vyberie krivku E nad F_p a bod $P \in E$ (obvykle veľkého prvočíselného rádu); ďalej vyberie s mod p a vypočíta $P' = sP$. Štvorica (p, E, P, P') je verejným kľúčom a s je súkromným kľúčom účastníka B.

2. A zakóduje svoju správu v tvare bodu $M \in E$, náhodne vygeneruje k mod p, vypočíta $M_1 = kP$, $M_2 = M + kP'$ a odošle M_1, M_2 ku B.

3. B rozšifruje správu výpočtom $M_2 - sM_1 = M + kP' - s(kP) = M$.

Príklad: Krivka sepc160k1 – súčasť Firefox: $E: \ y^2 = x^3 + 7$ nad Z_p pre $p = 1461501637330902918203684832716283019651637554291$.

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

DiscLogProb pre $E(F_p)$: Pre $P, P' \in E$ určiť s mod p tak, aby $P' = sP$. Zatiaľ sa nenašiel algoritmus polynomiálnej zložitosti v p na určenie s.

Najjednoduchší druh eliptického kryptosystému (ElGamal) pre $A \to B$:

1. B vyberie krivku E nad F_p a bod $P \in E$ (obvykle veľkého prvočíselného rádu); ďalej vyberie s mod p a vypočíta $P' = sP$. Štvorica (p, E, P, P') je verejným kľúčom a s je súkromným kľúčom účastníka B.

2. A zakóduje svoju správu v tvare bodu $M \in E$, náhodne vygeneruje k mod p, vypočíta $M_1 = kP$, $M_2 = M + kP'$ a odošle M_1, M_2 ku B.

3. B rozšifruje správu výpočtom $M_2 - sM_1 = M + kP' - s(kP) = M$.

Príklad: Krivka sepc160k1 – súčasť Firefox: $E: \ y^2 = x^3 + 7$ nad Z_p pre $p = 1461501637330902918203684832716283019651637554291$. Ale aj $q = |E| = 1461501637330902918203686915170869725397159163571$ je prvočíslo!!!

"Šteklenie" miliónového P-NP problému: Eliptická kryptografia

DiscLogProb pre $E(F_p)$: Pre $P, P' \in E$ určiť s mod p tak, aby $P' = sP$. Zatiaľ sa nenašiel algoritmus polynomiálnej zložitosti v p na určenie s.

Najjednoduchší druh eliptického kryptosystému (ElGamal) pre $A \to B$:

1. B vyberie krivku E nad F_p a bod $P \in E$ (obvykle veľkého prvočíselného rádu); ďalej vyberie s mod p a vypočíta $P' = sP$. Štvorica (p, E, P, P') je verejným kľúčom a s je súkromným kľúčom účastníka B.

2. A zakóduje svoju správu v tvare bodu $M \in E$, náhodne vygeneruje k mod p, vypočíta $M_1 = kP$, $M_2 = M + kP'$ a odošle M_1, M_2 ku B.

3. B rozšifruje správu výpočtom $M_2 - sM_1 = M + kP' - s(kP) = M$.

Príklad: Krivka sepc160k1 – súčasť Firefox: $E: \ y^2 = x^3 + 7$ nad Z_p pre $p = 1461501637330902918203684832716283019651637554291$. Ale aj $q = |E| = 1461501637330902918203686915170869725397159163571$ je prvočíslo!!! Teda, $E \cong Z_q$ a ľubovoľný nenulový prvok tu má rád q.