Hasseho věta

$$|E(\mathbb{F}_q)| = q+1-t \qquad |t| \le 2\sqrt{q}$$

$t>0$ kolik afinních bodů chybí do q

$t<0$ kolik afinních bodů přebývá vůči

WK jediný bod v ∞

Každá konečná podgrupa $E(\overline{\mathbb{F}_q})$ tvaru $\mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2}$, kde $m_1 | m_2$

Plyne i zjištění, že $E[m] \cong \mathbb{Z}_m\times\mathbb{Z}_m$ pokud $\mathrm{char}(\mathbb{F}_q)$ nedělí m

pokud dělí „menší"

Víme také, že

$E[F_q] \leq E(\overline{F_q})$ proto $E[F_q] \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, kde $m_1 \mid m_2$

Navíc platí $m_1 \mid q-1$

Prozkoumejme nyní všechny WK nad $\mathbb{Z}_5$ hladké.

$y^2 = x^3 + ax + b$ $\quad 4a^3 + 27b^2 \overset{?}{=} 0$ $\quad$ $a = b = 0$

$a \neq 0$ $\quad$ $b \neq 0$ $\quad 2b^2 - a^3 = 0$

Singularitu máme pro $\quad a^4 = 1 \quad 2b^2a \equiv 1 \bmod 5$

$(a,b) = (0,0)\ (2,2)\ (2,3)\ (3,1)\ (3,4)$ $\quad$ NECTVERCE mod 5 pouze 2, 3 $\quad$ LZE PROPP

$b^2 = -1 = 4$

Kdy (a,b) a $(\hat{a},\hat{b})$ popisují ekvivalentní WK?

$\exists \lambda \neq 0 \quad \hat{a} = \lambda^4 a \quad \hat{b} = \lambda^6 b$

$\lambda^4 = 1 \qquad \lambda^6 b = \lambda^2 b$

$\hat{a} = a$

b je vždy až na násobek čtvercem $\quad b = 0, 1, 2$

Řešení pro (a,b) tedy jsou

(0,1) (0,2) (1,0) (1,1) (1,2) (2,0) (2,1) (3,0) (3,2)
(4,0) (4,1) (4,2)

12 křivek

Hasseho interval je $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$

$5+1-4=2 \quad 5+1+4=10$

Chceme zjistit, zda
každou uvidíme, čili
9 možných velikostí

ZDA $\exists$ křivka s i racionálními body, $i \in \{1,2,\dots,9\}$

$y^2 = x^3 + 2x = x(x^2+2)$ — když čtverec

Jediný bod z $A^2(\mathbb{F}_5)$

je $(0,0)$

$x = \pm 1 \quad x^2+2 = 3 \quad \pm 3$ nečtverec

$x = \pm 2 \quad 4+2 = 1 \quad \pm 2$ nečtverec

$y^2 = x^3 - 2x \qquad y^2 = x(x^2-2)$

$x = 1 \quad y^2 = 4 = -1$

$x = 2 \quad$ — " —

$x = 3 \quad y^2 = 1$

$x = 4 \quad y^2 = 1$

$2 \times 4 + 1 = 9$

$-2=3$

řád	(a,b)	grupa
2	$(2,0)$	$\cong \mathbb{Z}_2$
3	$(4,2)$	$\cong \mathbb{Z}_3$
4	$(1,0)$	$\cong \mathbb{Z}_2 \times \mathbb{Z}_2$
	$(1,2)$	$\cong \mathbb{Z}_4$
5	$(3,2)$	$\cong \mathbb{Z}_5$
6	$(0,1)$	$\cong \mathbb{Z}_6$
10	$(3,0)$	$\cong \mathbb{Z}_{10} \cong \mathbb{Z}_5 \times \mathbb{Z}_2$
9	$(1,1)$	$\cancel{\mathbb{Z}_3 \times \mathbb{Z}_3}$, $\mathbb{Z}_9$
8	$(4,0)$	$\cong \mathbb{Z}_2 \times \mathbb{Z}_4$
	$(4,1)$	$\cong \mathbb{Z}_8$
7	$(2,1)$	$\cong \mathbb{Z}_7$
6	$(0,2)$	$\cong \mathbb{Z}_6$

$x(x^2+1)=0$

koreny $0, \pm 2, 3$

$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ $\quad m_1 \mid m_2$, $\quad m_1 \mid q-1$, $\quad q=5$

$\cancel{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2}$

$x^3 - x$ nad koreny $\pm 1, 0$

$y^2 = x^3 - x + 1$ koren 3

řetězí rovnice

$\cancel{x^3} + x = 0$

$x^3 + x + 2 = 0$

$$\frac{\mathbb{Z}_2 \times \mathbb{Z}_4}{\mathbb{Z}_8} \qquad \frac{\mathbb{Z}_2 \times \mathbb{Z}_2}{\mathbb{Z}_4}$$

$(4,0)$

znamená 3 involuce (mají řád 2)

1 involuce

NAD WK TODO

Bod $(\alpha, 0)$

Nasazujme chvíli je případ $a \neq 0 \quad b \neq 0$

	$a\ b$	$a^3\ b^2$	$c=3$		(a,b)	(a^3, b^2)	
3	$(4,2)$	$(4,4)$	$c^2=-1=4$, $c^3=2$	9	$(1,1)$	$(1,1)$	$\frac{1}{1}=\frac{4}{4}=1$
4	$(1,2)$	$(1,4)$	$\leftarrow$	8	$(4,1)$	$(4,1)$	$\frac{1}{4}=\frac{4}{1}=-1$
5	$(3,2)$	$(2,4)$	$\leftarrow$	7	$(2,1)$	$(3,1)$	$\frac{2}{4}=\frac{3}{1}=3$

Křivky s doplněným se počtem bodů mají stejná hodnotu $\frac{a^3}{b^2}$

Proč? Proč mezi a^3/b^2 stejná hodnota?

$\boxed{y^2=x^3+ax+b}$ je K-ekvivalentní $y^2=x^3+c^4ax+c^6b$

mají stejný počet bodů

CO KDYŽ c není čtverec

$\boxed{y^2=x^3+c^2ax+c^3b}$

c je čtverec

c není čtverec

<u>Tvrzení</u> Ať C je křivka $y^2 = x^3 + ax + b \in \mathbb{F}_q[x]$, q liché
$\tilde{C}$ $\qquad y^2 = x^3 + c^2 a x + c^3 b \in \mathbb{F}_q[x]$, c nečtverec v $\mathbb{F}_q$

Potom celkový počet afinních bodů v C a $\tilde{C}$ je $= 2q$ (a tedy $|C(\mathbb{F}_q)| + |\tilde{C}(\mathbb{F}_q)| = 2q + 2$)

D: Stačí ukázat, že $\forall \alpha \in \mathbb{F}_q$ je $s(\alpha) + \tilde{s}(\alpha) = 2$, kde

$s(\alpha) = \#\beta$, že $(\alpha, \beta) \in C$ $\qquad c^3(\alpha^3 + a\alpha + b) = (c\alpha)^3 + c^2 a (c\alpha) + c^3 b$

$\tilde{s}(\alpha) = \#\beta$, že $(c\alpha, \beta) \in C$

$\alpha^3 + a\alpha + b$ je čtverec $\neq 0$ $\quad s(\alpha) = 2 \quad \tilde{s}(\alpha) = 0$

$\alpha^3 + a\alpha + b$ je nečtverec $\quad s(\alpha) = 0 \quad \tilde{s}(\alpha) = 2$

$\alpha^3 + a\alpha + b \quad 0 \quad s(\alpha) = 1 \quad \tilde{s}(\alpha) = 1$

(kořen $x^3 + ax + b$)

$$s(\alpha) + \tilde{s}(\alpha) = 2$$

j-invariant se definuje pro každou eliptickou křivku (tedy křivku rodu 1)

Nemění se při K-ekvivalenci, ale ani při $\overline{K}$-ekvivalenci

Platí dokonce 2 křivky nad K jsou $\overline{K}$-ekvivalentní $\iff$ mají stejný j-invariant

Pro křivky $\overbrace{y^2 = x^3+ax+b}^{C}$, $\mathrm{char}(K) \notin \{2,3\}$ platí

$$j(C) = 1728 \underbrace{\frac{4a^3}{4a^3+27b^2}}_{\tilde{j}(C)} \qquad 1728 = 12^3$$

$$j(C)=0 \iff \tilde{j}(C)=0 \iff a=0$$

$$j(C)=1728 \iff \tilde{j}(C)=1 \iff b=0$$

<u>Lemma</u> Ať $C: y^2 = x^3 + ax + b$ $\quad j(C) = j(\tilde{C}) \notin \{0, 1\}$

$\tilde{C}: y^2 = x^3 + \tilde{a}x + \tilde{b}$ $\quad 2 \nmid q \quad 3 \nmid q$

Pak $\exists c$, že $\tilde{a} = c^2 a \quad \tilde{b} = c^3 b$

D: $j(C) = j(\tilde{C}) \Longrightarrow \dfrac{4a^3}{4a^3 + 27b^2} = \dfrac{4\tilde{a}^3}{4\tilde{a}^3 + 27\tilde{b}^2} \Longrightarrow a^3\tilde{b}^2 = \tilde{a}^3 b^2$

$\alpha = \dfrac{\tilde{a}}{a} \quad \beta = \dfrac{\tilde{b}}{b} \qquad \alpha^3 = \beta^2 \qquad$ Položme $c = \dfrac{\beta}{\alpha}$

Pak $c^3 = \dfrac{a^3\tilde{b}^3}{\tilde{a}^3 b^3} = \dfrac{\tilde{a}^3 b^2 \tilde{b}}{\tilde{a}^3 b^3} = \dfrac{\tilde{b}}{b} \qquad \tilde{b} = c^3 b$

$c^2 = \dfrac{a^2\tilde{b}^2}{\tilde{a}^2 b^2} = \dfrac{a^2}{\tilde{a}^2} \cdot \dfrac{\tilde{a}^3}{a^3} = \dfrac{\tilde{a}}{a} \qquad \tilde{a} = c^2 a$

$\tilde{C}$

Pokud $y^2 = x^3 + c^2 a x + c^3 b$

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

C

$c = \lambda^2$ $\quad$ $\tilde{C}$ a C jsou K-ekvivalentní

c je nečtverec

$|C(\mathbb{F}_q)| + |\tilde{C}(\mathbb{F}_q)| = 2q + 2$

Pak se říká, že $\tilde{C}$ je přezglen / twist C

kvadratický přezglen $\quad$ quadratic twist C

kanonický předvedení

$j(\tilde{C}) = j(C) \notin \{0, 1728\}$ a $\tilde{C}$ a C nejsou K-ekvivalentní

kvadratický přezglen $\Leftrightarrow$ $\tilde{b} b$ není čtverec

$y^2 = x^3 + \tilde{a} x + \tilde{b}$ $\quad$ $y^2 = x^3 + ax + b$

$E(\mathbb{F}_q) \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ $\quad m_1 \mid m_2$

Mít ke každému bodu vyjádření, které umožňuje efektivně provádět operace $\oplus$ známe-li body Q a P ~~takové~~, že $\forall a$, $0<a<m_1$

$$[a]Q \neq O \;(=\infty) \qquad [m_1]Q = O$$

$$[b]P \neq O, \quad 0<b<m_2, \quad [m_2]P = O$$

$$[a]Q \neq [b]P, \text{ jinak}$$

$$0<a<m_1 \qquad 0<b<m_2$$

Pak každý prvek grupy lze jednoznačně zapsat jako $[a]Q + [b]P$

$0 \le a < m_1$,

$0 \le b < m_2$

$$([a]Q \oplus [b]P) \oplus ([a']Q + [b']P) = [a+a']Q \oplus [b+b']P$$

Někdy, pokud víme, že máme se do činění s bodem P jenž je prvočíselného řádu l kde $l \equiv 3,5 \bmod 8$, tak umíme se k vyjádření bodu $[2]P$ dostat pouze opakovaným zdvojováním. P $[2]P$ $[4]P$ $[8]P$ ... $[2^k]P$

Je-li $l \equiv 3,5 \bmod 8$ prvočíslo, je 2 primitivní prvek, takže každé $[2^k]P$ vyčerpají všechny nenulové (nenulové) prvky cyklické grupy generované P

Obecně, můžeme zjistit takto, přiřazení libovolného bodu $[T]$ řádu $n = 2^k m$, m liché, co je to ono k. A to tak, že počítáme P $[2]P$ ...

Prvním bodem, který se zopakuje bude $[2^k]P$