STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Isogenie v kryptografii

Zdeněk Pezlar
Jihomoravský kraj

Brno 2021

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Isogenie v kryptografii

Isogeny Based Cryptography

Autor: Zdeněk Pezlar
Škola: Gymnázium Brno, třída Kapitána Jaroše, p. o.
Kraj: Jihomoravský
Konzultant: Bc. Vojtěch Suchánek

Prohlášení

Prohlašuji, že jsem svou práci SOČ vypracoval samostatně a použil jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů. Prohlašuji, že tištěná verze a elektronická verze soutěžní práce SOČ jsou shodné. Nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Brně dne: ..... Podpis: .....

jihomoravský kraj

Poděkování

++Tato práce byla vypracována za finanční podpory JMK.

Abstrakt

abstrakt

Klíčová slova

isogenie;klíčové slovo.

Abstract

abstrakt

Key words

isogenie;klíčové slovo.

Obsah

Úvod

celkem úvod

Použitá značení

$a \mid b$	a dělí b
$\frac{1}{a}$	multiplikativní inverz a, tj. a^{-1}
$\mathcal{D}(a,b)$	největší společný dělitel a, b
$v_p(n)$	p-adická valuace n
$\left(\frac{a}{p}\right)$	Legendreův symbol a vzhledem k p
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	množina přirozených, celých, racionálních, reálných, komplexních čísel
$\mathbb{Z}_d$	okruh zbytků modulo d
$\mathbb{F}_q$	konečné těleso s q prvky
$\overline{\mathbb{F}}$	algebraický uzávěr $\mathbb{F}$
$\mathbb{F}^\times$	multiplikativní podrupa $\mathbb{F}$
$\mathbb{F}^*$	$\mathbb{F} \setminus \{0\}$
$\mathbb{P}^n(K)$	projektivní prostor nad K o rozměru $n+1$
$E(K)$	množina bodů křivky E nad K
$[n]_E, [n]$	násobení n na křivce E
$E[n]$	n-torze křivky E
$\mathrm{End}(E)$	okruh endomorfismů E
$j(E)$	j-invariant křivky E
$R[x]$	okruh polynomů s koeficienty nad okruhem R
$K(a_1, \ldots, a_n)$	nejmenší podtěleso L, které obsahuje těleso K i prvky $a_1, \ldots, a_n \in L$
$[K : L]$	stupeň rozšíření tělesa K nad L, tj. dimenze vektorového prostoru K/L
$\mathcal{O}_K$	okruh celých algebraických čísel tělesa K
$Cl(\mathcal{O})$	grupa tříd ideálů pořádku $\mathcal{O}$
$h_\mathcal{O}$	řád grupy $Cl(\mathcal{O})$
(a)	hlavní ideál generovaný prvkem a
$\frac{\mathcal{I}}{m}$	lomený ideál $\frac{\mathcal{I}}{m}$

$\left(\frac{a}{m}\right)$	hlavní lomený ideál $\frac{(a)}{m}$
$N(a)$	norma prvku a
$N((a))$	norma ideálu generovaného a
$\mathcal{I}\|\mathcal{J}$	ideál $\mathcal{I}$ dělí ideál $\mathcal{J}$
G/H	faktorgrupa G podle H
$\deg f$	stupeň polynomu f
f'	derivace f
$f \in O(g)$	f roste asymptoticky nejvýše stejně rychle jako g
$f \in \Theta(g)$	f roste asymtoticky stejně rychle jako g
$f \in \Omega(g)$	f roste asymtoticky alespoň tak rychle jako g

Kapitola 1

Eliptické křivky

V naší první kapitole se budeme věnovat isogeniím eliptických křivek a práci s nimi. Budeme budovat teorii a intuici potřebnou k smysluplné diskuzi protokolu SIDH. Pro porozumění textu je třeba ovládat základy abstraktní algebry, viz [20]. Budeme postupovat volně dle [27], nicméně další vhodný úvodní materiál se nachází na [5]. Ne vždy budeme uvádět důkazy tvrzení, neboť jsou mnohdy příliš pokročilé či technické, v takových případech se odkážeme na relevantní literaturu.

1.1 Základy

Po celou dobu budeme pracovat nad projektivním prostorem nad uzávěrem tělesa K, což je množina bodů v $\overline{K}^n$, kde dva body považujeme za ekvivalentní, pokud leží v přímce s počátkem, můžeme proto místo jednotlivých bodů pracovat s přímkami skrz počátek. Chtěli bychom, aby se každé dvě $n-1$ rozměrné roviny protínaly, a s tím máme problém pouze pokud protínáme dvě rovnoběžné. V každém směru si tak můžeme definovat projektivní prostor stupně $n-1$ v nekonečnu, kde se protínají rovnoběžné roviny.

Definice 1.1.1. Buďte K těleso a n přirozené číslo. *Projektivní prostor* $\mathbb{P}^n(\overline{K})$ definujeme jako množinu tříd nenulových vektorů $(a_0, \ldots, a_n) \in \overline{K}^{n+1}$ s ekvivalentní relací $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$, pokud existuje $\lambda \in \overline{K}$, že $(a_0, \ldots, a_n) = \lambda(b_0, \ldots, b_n)$. Tyto třídy ekvivalence budeme značit $(a_0 : \cdots : a_n)$.

Pokud je jedno z a_i nulové, získáme $n-1$ rozměrný prostor v nekonečnu.

Projektivní prostor $\mathbb{P}^2(\mathbb{R})$ je známý jako projektivní rovina. Každé dvě přímky se protínají v jednom bodě, přičemž rovnoběžné přímky se protínají v bodě v nekonečnu v daném směru. Přímky procházející počátkem tak můžeme ztotožnit s jejich průsečíkem s rovinou neprocházíjí začátek, tedy každé takové přímce přiřadíme právě třídu, ve které leží její příslušný průsečík. Přímky s touto rovnou rovnoběžné, které v ní neleží, ji protínají v nekonečnu, a přiřadíme jim body v nekonečnu v jejich směru.

Poznámka 1.1.2. Je zajímavé uvážit souvislost projektivních prostorů s barycentrickými souřadnicemi, kde je každý bod vyjádřen jako vážený průměr vrcholů referenčního simplexu. Tyto souřadnice jsou též homogenní a každé dvě přímky se protínají, byť některé v nekonečnu, takové body mají součet vah roven 0. Můžeme o barycentrických souřadnicích tedy přemýšlet jako o projektivním prostoru s jiným základem.

Připomeňme si pak definici eliptické křivky. Často se definuje jako nesingulární projektivní křivka genu 1, pro naše účely si definici zúžíme.

Definice 1.1.3. Mějme K těleso charakteristiky různé od 2 a 3. Pro $a, b \in K$, že $4a^2+27b^3 \neq 0$, definujeme v $\mathbb{P}^2(\overline{K})$ *eliptickou křivku* jako množinu bodů $(X : Y : Z) \in \overline{K}^3$ splňující:

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Definice vylučující tělesa s charakteristikou 2 a 3 nám umožňuje zapsat křivku ve výše uvedené jednoduché formě. Avšak čtenář, jenž je již obeznámen s eliptickými křivkami, může protestovat, že eliptická křivka je množina bodů $x, y \in \overline{K}$ splňující:

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

Pokud bod eliptické křivky leží na přímce $Z = 0$, leží i na $X = 0$, a máme jediný bod $(0 : 1 : 0)$. Jinak můžeme celou rovnici podělit Z^3, přejít na proměnné $x := \frac{X}{Z}, y := \frac{Y}{Z}$ a získat nám známou formu, kterou budeme dále označovat jako *afinní*, často se v literatuře uvádí jako *Weierstrassova*. Naše křivka je poté množinou bodů $(x, y) \in \overline{K}^2$ splňujících $y^2 = x^3 + ax + b$ spolu s bodem v nekonečnu $\mathcal{O} = (0 : 1 : 0)$.

Definice 1.1.4. Množinu všech bodů E nad konečným tělesem K (společně s $\mathcal{O}$) budeme značit $E(K)$ a počet jejích prvků budeme značit $\#E(K)$.

Počet bodů na E nad konečným tělesem $\mathbb{F}_q$ je shora ohraničen číslem $2q+1$, protože pro každé $x \in \mathbb{F}_q$ existují v $\mathbb{F}_q$ nejvýše 2 odmocniny z x^3+ax+b, a poslední bod do počtu je $\mathcal{O}$. V $\mathbb{F}_q$ leží právě $\frac{q+1}{2}$ čtverců, tudíž za předpokladu, že $x^3 + ax + b$ pokrývá $\mathbb{F}_q$ rovnoměrně, bychom na E očekávali okolo q bodů, společně s bodem v nekonečnu $q + 1$. Roku 1933 tento odhad Helmut Hasse dokázal, tedy skutečně se $\#E(\mathbb{F}_q)$ nepříliš liší od $q + 1$.

Věta 1.1.5. *(Hasse) Nechť E je eliptická křivka nad $\mathbb{F}_q$. Pak:*

$$|q + 1 - \#E(\mathbb{F}_q)| \leqslant 2\sqrt{q}.$$

Důkaz je k nalezení v [22, Thm V.1.1].

Definice 1.1.6. Pod bodem $P \in E$ rozumíme $P = (x, y) \in E(\overline{K})$.

Podívejme se nyní na eliptickou křivku E geometricky, tedy v rovině vyznačme všechny body, které na ní leží. Je zjevné, že E je symetrická podle osy x, definujme proto k $P \in E$ opačný bod $-P \in E$ jako obraz P podle osy x. Pokud bychom na bodech naší křivky

definovali součet, chtěli bychom, aby součet P a $-P$ byl $\mathcal{O}$.

OBrázky

Pokud řekneme, že tečna k E ji protíná ve dvou stejných bodech, pak každá přímka protíná E v právě třech bodech včetně multiplicity. Speciálně tečna v bodě s $y = 0$ tento bod protíná dvakrát a ten třetí je bod v nekonečnu E. Sčítání $+$ si na E můžeme definovat tak, že součet každých tří bodů v přímce je $\mathcal{O}$. Pokud tak přímka procházející $P, Q \in E$ protíná E potřetí v R, pak definujeme $P + Q = -R$. Pro součet bodů $P, Q \in E$ můžeme poté odvodit několik důležitých vlastností:

(i) $P + Q = Q + P$,

(ii) $(P + Q) + R = P + (Q + R)$,

(iii) $P + \mathcal{O} = P$,

(iv) $P + (-P) = \mathcal{O}$.

Při takto definovaném součtu můžeme s body na E pracovat jako s abelovskou grupou se sčítáním $+$ a neutrálním prvkem $\mathcal{O}$. Samozřejmě součet dvou bodů dokážeme za pomocí analytické geometrie přímo spočíst:

Věta 1.1.7. *Buďte $P = (x_1, y_1), Q = (x_2, y_2)$ afinní body s $P \neq -P$. Pak $P + Q = (x_3, y_3)$ je daný:*

$$x_3 = \lambda^2 - x_1 - x_2,$$
$$y_3 = -\lambda x_3 - y_1 + \lambda x_1,$$

kde:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{pokud } x_1 \neq x_2, \\ \frac{3x_1^2 + a}{2y_1}, & \text{pokud } x_1 = x_2. \end{cases}$$

Důkaz s dovolením neuvádím. Pro zkrácení zápisu si budeme definovat skálární násobky bodů následovně:

Definice 1.1.8. Mějme bod $P \in E$. Pak pro n přirozené definujeme jeho n-násobek:

$$[n]_E P = \underbrace{P + \cdots + P}_{n},$$

příčemž pro $n < 0$ definujeme $[n]_E P = [-n]_E(-P)$ a $[0]_E P = \mathcal{O}$.

Pokud bude z kontextu jasné, nad kterou eliptickou křivkou pracujeme, budeme značit násobení skalárem pouze $[n]P$. Pojďme se pokusit n-násobek bodu spočíst co nejrychleji, zjevně se stačí omezit na případ $n > 0$.

Naivní postup výpočtu $[n]P$ jímá $n-1$ sčítání, to jistě dokážeme vylepšit. Analogickým postupem jako při rychlém umocňování využijeme zápis n v binární soustavě. Inicializujeme $P_0 = [n \pmod 2]P$ a bod $Q = P$. Dále v i-tém kroku si budeme pamatovat $[2^i]P$ a n_0, přičemž při přechodu na další krok spočteme $Q \mapsto [2]Q = [2^{i+1}]P$. Navíc pokud je i-tý bit n roven 1, aktualizujeme $P_0 \mapsto P_0 + Q$. Skončíme na $i = \lfloor \log_2(n) \rfloor$, když $P_0 = [n]P$, a dohromady při výpočtu užijeme nejvýše $\lfloor \log_2(n) \rfloor - 1 \leqslant \log_2(n) - 1$ operací sčítání i dvojnásobení. Dvojnásobek prvků spočteme alespoň tak rychle jako součet dvou bodů, tedy tímto postupem spočteme $[n]P$ v nejvýše $2(\log_2(n) - 1)$ sčítáních.

Příklad 1.1.9. tu příklad sčítání, jak v Q tak v Fq, hezky graficky

Příklad 1.1.10. Určeme dvojnásobek bodu $P = (x, y)$ na $E : y^2 = x^3 + ax + b$.

Řešení. V duchu značení věty 1.1.7 máme pro $[2]P = (x_1, y_1)$:

$$\begin{aligned}
x_1 &= \lambda^2 - 2x = \frac{(3x^2+a)^2}{4y^2} - 2x = \frac{(3x^2+a)^2 - 8y^2x}{4y^2} = \frac{(3x^2+a)^2 - 8(x^3+ax+b)x}{4(x^3+ax+b)} \\
&= \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3+ax+b)}, \\
y_1 &= -\lambda x_1 - y + \lambda x = -\frac{(3x^2+a)[(3x^2+a)^2 - 8y^2x]}{8y^3} - y + \frac{x(3x^2+a)}{2y} \\
&= \frac{(3x^2+a)[-(3x^2+a)^2 + 12y^2x] - 8y^4}{8y^4} y \\
&= \frac{(3x^2+a)[-(3x^2+a)^2 + 12(x^3+ax+b)x] - 8(x^3+ax+b)^2}{8(x^3+ax+b)^2} y \\
&= \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{8(x^3+ax+b)^2} y.
\end{aligned}$$

□

Všimneme si, že pro $P = (x, y)$ na eliptické křivce s $y = 0$ je $[2]P = \mathcal{O}$. Pro bod $Q = (6, 27) := (x_0, y_0)$ na křivce:

$$y^2 = x^3 + 54x + 189$$

nad $\mathbb{Q}$ zase ověříme, že:

$$x_0^6 + 5ax_0^4 + 20bx_0^3 - 5a^2x_0^2 - 4abx_0 - a^3 - 8b^2 = 0,$$

tedy $[3]Q = \mathcal{O}$. Obecně by nás mohlo zajímat, které body pošle násobení n do nekonečna.

Definice 1.1.11. Buď n celé číslo. O množině všech $P \in E$, že $[n]P = \mathcal{O}$, řekneme, že tvoří *n-torzi* E a tuto množinu budeme značit $E[n]$.

Definice 1.1.12. Buď P bod na E. Pokud n je nejmenší kladné číslo, že $[n]P = \mathcal{O}$, nazveme n *řádem* P. Pokud takové n neexistuje, řekneme, že P má nekonečný řád.

n-torze na eliptické křivce E tvoří podgrupu $E(\overline{K})$, neboť pokud $[n]P = \mathcal{O} = [n]Q$, tak $[n](P+Q) = [n]P + [n]Q = \mathcal{O}$. Torzní grupy nám pomáhají hlouběji studovat eliptické křivky v mnohých směrech. Zprvu si můžeme všimnout, že $E(\mathbb{F}_q)$ je průnikem všech torzních grup, tedy že každý bod má konečný řád.

Věta 1.1.13. *Každý bod P na eliptické křivce E nad konečným tělesem má konečný řád.*

Důkaz. Dejme tomu, že existuje

Například pro eliptickou křivku E nad konečným tělesem $\mathbb{F}_q$, je konečná grupa $E(\mathbb{F}_q)$ průnikem všech torzních podgrup, protože každý bod na E má konečný řád.

Zatímco $E(\mathbb{F}_q)$ je konečná grupa, grupa bodů na racionální křivce $E(\mathbb{Q})$ je nekonečná a existují i body nekonečného řádu. Příkladem mřížového bodu nekonečného řádu na křivce je bod $(70, 13)$ na křivce:

$$E : y^2 = x^3 - 13,$$

tedy jeho násobením můžeme získat nekonečně mnoho racionálních bodů na E. Body nekonečného řádu jsou obecně těžko spočitatelné, nicméně body s řádem konečným dokážeme všechny najít za pomocí věty Lutz-Nagella [29, Thm. 8.7], dle které všechny takové racionální body (x, y) jsou mřížové a buď 2-torzní, či y^2 dělí diskriminant naší křivky.

1.2 Zobrazení mezi eliptickými křivkami

Násobení bodů v E skalárem dává homomorfismus $E(\overline{K}) \longrightarrow E(\overline{K})$. Definuje proto endomorfismus na E daný lomenou funkcí nad K. My se nyní podíváme na zobrazení mezi jednotlivými eliptickými křivkami, konkrétně homomorfismy grup $E_1(\overline{K}) \longrightarrow E_2(\overline{K})$.

Uvažme zobrazení $(x, y) \mapsto (u^2x, u^3y)$, které převádí křivky:

$$E_1 : y^2 = x^3 + u^4ax + u^6b \mapsto E_2 : y^2 = x^3 + ax + b$$

pro libovolné $u \in \overline{K}$. To je lineární zobrazení mezi E_1 a E_2, které zachovává přímky a tedy i součet bodů na našich křivkách, definuje proto homomorfismus z $E_1(\overline{K})$ do $E_2(\overline{K})$. Navíc je zobrazení zjevně invertibilní, tudíž dokonce mezi $E_1(\overline{K})$ a $E_2(\overline{K})$ dává isomorfismus nad $\overline{K}$.

Věta 1.2.1. *(Sato-Tate) Dvě křivky E_1, E_2 nad konečným tělesem K jsou nad K isomorfní právě pokud $\#E_1(K) = \#E_2(K)$.*

Ne vždy máme nutně isomorfismus nad K, ale nad jeho rozšířením. Aby byl náš isomorfismus nad $\overline{K}$ definovaný, musí být díky předpisu $(x, y) \mapsto (u^2x, u^3y)$ nutně nad rozšířením K stupně dělícího 6.

Definice 1.2.2. Buďte E, E' křivky isomorfní nad rozšířením K, ale ne nad K. Pak řekneme, že E' je *twistem* E nad K.

Zobrazení z $E: y^2 = x^3 + ax + b$ dané $(x, y) \mapsto \left(\frac{x}{d}, \frac{y}{\sqrt{d^3}}\right)$ pro $\sqrt{d} \notin K, d \in K$, nám dává isomorfismus do:

$$E_d : y^2 = x^3 + d^2ax + d^3b,$$

avšak ne nad K, ale nad jeho kvadratickým rozšířením $K(\sqrt{d})$. E_d nazveme *kvadratickým twistem* E.

Pro křivky s $a = 0$, resp. $b = 0$, můžeme analogicky najít *kubický* a *sextický*, resp. *kvartický* twist:

$$y^2 = x^3 + b \mapsto y^2 = x^3 + d^2b,$$
$$y^2 = x^3 + b \mapsto y^2 = x^3 + db,$$
$$y^2 = x^3 + ax \mapsto y^2 = x^3 + dax,$$

dané po řadě $(x, y) \mapsto \left(\frac{x}{\sqrt[3]{d^2}}, \frac{y}{d}\right)$ a $(x, y) \mapsto \left(\frac{x}{\sqrt[3]{d}}, \frac{y}{\sqrt{d}}\right)$, resp. $(x, y) \mapsto \left(\frac{x}{\sqrt{d}}, \frac{y}{\sqrt[4]{d^3}}\right)$. Vidíme, že poslední dvě zmíněné křivky jsou navíc kvadratickými twisty po řadě kubického a kvadratického twistu E.

Chtěli bychom říci, kdy mezi dvěma eliptickými křivkami existuje isomorfismus, tedy najít nějaký invariant, který isomorfní křivky sdílí. Takovou funkci splňuje právě j-invariant.

Definice 1.2.3. Pro eliptickou křivku $E : y^2 = x^3 + ax + b$ definujeme její *j-invariant* jako:

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Poznamenejme, že ten je vždy nad K definovaný, neboť eliptické křivky mají nenulový diskriminant.

Věta 1.2.4. *Dvě křivky definované nad K jsou isomorfní nad $\overline{K}$, právě pokud mají stejný j-invariant.*

Důkaz. Nejprve předpokládejme, že křivky $E_1 : y^2 = x^3 + a_1x + b_1$ a $E_2 : y^2 = x^3 + a_2x + b_2$ jsou nad $\overline{K}$ isomorfní. Máme pak $a_2 = u^2a_1$ a $b_2 = u^3b_1$ pro nějaké $b \in \overline{K}$. Spočtěme j-invariant obou křivek:

$$j(E_2) = 1728\frac{4u^6a_1^3}{4u^6a_1^3 + 27u^6b_1^2} = 1728\frac{4a_1^3}{4a_1^3 + 27b_1^2} = j(E_1),$$

j-invarianty isomorfních křivek se proto rovnají.

Nyní předpokládejme, že $j(E_1) = j(E_2)$. Počítejme:

$$\begin{aligned} 1728\frac{4a_1^3}{4a_1^3+27b_1^2} &= 1728\frac{4a_2^3}{4a_2^3+27b_2^2}, \\ a_1^3(4a_2^3+27b_2^2) &= a_2^3(4a_1^3+27b_1^2), \\ a_1^3b_2^2 &= a_2^3b_1^2. \end{aligned}$$

Pokud by například a_1 bylo nulové, je z nesingularity E_1 nutně b_1 nenulové, tudíž $a_2 = 0$. Proto ani b_2 není rovno nule, tedy pro $u \in \overline{K}$ s $u^3 = \frac{b_1}{b_2}$ máme $(0, b_1) = (0, u^3b_2)$. Analogicky pokud b_i jsou nulová, máme $(a_1, 0) = (u^2a_2, 0)$ pro u s $u^2 = \frac{a_1}{a_2} \in \overline{K}$.

Konečně v případě, že $a_1a_2b_1b_2 \neq 0$, máme $\frac{a_1^3}{a_2^3} = \frac{b_1^2}{b_2^2}$, což je druhou i třetí mocninou, tedy i šestou mocninou nějakého $u \in \overline{K}$. Toto číslo je tak šestou mocninou i všech šestých odmocnin u^6 v $\overline{K}$, pro tato u je tak $\frac{a_1}{a_2}$ rovno u^2 násobeno třetí odmocninou z 1 (ne nutně primitivní) a $\frac{b_1}{b_2}$ rovno u^3 násobeno druhou odmocninou z 1. Pro nějaké z těchto šesti u se obě odmocniny rovnají 1, čili $a_1 = u^2a_2$ a $b_1 = u^3b_2$. □

Mějme následujících pět křivek nad $\mathbb{Z}_{101}$:

$$\begin{aligned} E_1 &: y^2 = x^3 + x + 1, \\ E_2 &: y^2 = x^3 + 5x + 23, \\ E_3 &: y^2 = x^3 + x - 1, \\ E_4 &: y^2 = x^3 + 2, \\ E_5 &: y^2 = x^3 + 2x, \end{aligned}$$

a spočtěme si jejich j-invarianty (což jsou čísla v $\mathbb{Z}_{101}$):

$$\begin{aligned} j(E_1) &= 1728\frac{4}{31}, \\ j(E_2) &= 1728\frac{4\cdot 5^3}{4\cdot 5^3+27\cdot 23^2} = 1728\frac{4\cdot 24}{4\cdot 24+27\cdot 24} = 1728\frac{4}{31}, \\ j(E_3) &= 1728\frac{4}{31}, \\ j(E_4) &= 1728, \\ j(E_5) &= 0. \end{aligned}$$

Vidíme, že j-invarianty E_1 a E_2 se rovnají, přičemž v $\mathbb{Z}_{101}$ se oba rovnají $1728 \cdot 4 \cdot 88$, nutně mezi nimi nad $\overline{\mathbb{Z}_{101}}$ existuje isomorfismus. Snadno ověříme, že zobrazení:

$$(x, y) \mapsto (3^2x, 3^3y) = (9x, 27y)$$

převádí:

$$\begin{aligned} y^2 = x^3 + x + 1 \qquad \longrightarrow \qquad 27^2y^2 &= 9^3x^3 + 9x + 1, \\ 22y^2 &= 22x^3 + 9x + 1, \\ 22y^2 &= 22x^3 + 110x + 506, \\ y^2 &= x^3 + 5x + 23. \end{aligned}$$

Inverzní isomorfismus $E_2 \longrightarrow E_1$ je pak daný $(x, y) \mapsto (34^2x, 34^3y) = (45x, 15y)$, neboť multiplikativní inverz 3 v $\mathbb{Z}_{101}$ je 34.

Křivka E_3 má stejný j-invariant jako E_1 a E_2, nad $\mathbb{Z}_{101}$ mezi nimi a E_3 přesto isomorfismus neexistuje. E_3 je kvadratickým twistem E_1 nad $\mathbb{Z}_{101^2} = \mathbb{Z}_{101}[i]$, jakožto zobrazení $(x, y) \mapsto \left(\frac{x}{i^2}, \frac{y}{i^3}\right) = (-x, iy)$ převádí:

$$\begin{aligned} y^2 = x^3 + x + 1 \longrightarrow -y^2 &= -x^3 - x + 1, \\ y^2 &= x^3 + x - 1. \end{aligned}$$

Dvě speciální hodnoty j-invariantu jsou 0 a 1728, kterých nabývají křivky, které mají po řadě lineární, resp. konstantní člen roven 0. Právě křivky s j-invariantem 0 mají kubický (a sextický) twist, ty s j-invariantem 1728 zase kvartický.

Důležitost twistů křivek

Věta 1.2.5. *Uvažme křivku $E : y^2 = x^3 + ax + b$ nad $\mathbb{F}_q$ a její twist $\tilde{E} : y^2 = x^3 + g^2ax + g^3b$*

Mohli bychom si nicméně osvětlit, proč se v j-invariantu násobí číslem 1728. Důvodem jsou tělesa charakteristik 2 a 3, j-invariant se totiž klasicky definuje pro libovolnou nesingulární projektivní křivku genu 1, tj.:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

jako:

$$\frac{(b_2^2 - 24b_4)^2}{\Delta},$$

kde Δ je diskriminant naší křivky a $b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3$. Pro tělesa s char $K \notin \{2, 3\}$ můžeme definovat zobrazení, která převádí naši křivku na nám známý afinní tvar, detaily důkazu jsou k nalezení v [22, Ch. 3]. Obraz rovnice j-invariantu je právě takový, jak ho zde definujeme, násoben konstantou 1728.

Počet různých j-invariantů v K určuje počet tříd isomorfismů křivek nad $\overline{K}$, případně kterých hodnot j-invariant nikdy nenabude. Jak si nyní ukážeme, tento počet je nejvyšší možný.

Věta 1.2.6. *Pro každé $s \in K$ existuje eliptická křivka E nad K s $j(E) = s$.*

Důkaz. Pro $s \in \{0, 1728\}$ poslouží jako příklady po řadě křivky $y^2 = x^3 + x, y^2 = x^3 + 1$. Pro zbylá $s \in K$ uvažme křivku:

$$E : y^2 = x^3 + 3s(1728 - s)x + 2s(1728 - s)^2.$$

Za předpokladu $\operatorname{char} K \notin \{2, 3\}$ je E vskutku eliptická, můžeme tedy definovat j-invariant. Ten je roven:

$$\begin{aligned} j(E) &= 1728\frac{4[3s(1728-s)]^3}{4[3s(1728-s)]^3 + 27[2s(1728-s)^2]^2} \\ &= 1728s\frac{4 \cdot 27s^2(1728-s)^3}{4 \cdot 27s^2(1728-s)^3(s+1728-s)} = \frac{1728}{1728}s = s. \end{aligned}$$

Křivka E proto má j-invariant roven s. □

Věta 1.2.7. *Pro každé $s \in \overline{K}$ existuje eliptická křivka E nad $K(s)$, že $j(E) = s$.*

Důkaz. Opět si rozmyslíme, že křivka $y^2 = x^3 + 3s(1728 - s)x + 2s(1728 - s)^2$ je definovaná nad $K(s)$, tedy může posloužit jako řešení. □

Jak násobení bodů E skalárem, tak braní twistu, jsou homomorfismy bodů křivek nad tělesem K, resp. jeho rozšířením. Spadají tak pod rodinu zobrazení eliptických křivek zvaných *isogenie*, o kterých se budeme dále bavit.

1.3 Isogenie

Definice 1.3.1. Ať $E_1, E_2 \in \overline{K}$ jsou eliptické křivky. Surjektivní morfismus $\phi : E_1 \longrightarrow E_2$ daný racionální funkcí nad K, který posílá bod v nekonečnu E_1 na bod v nekonečnu E_2, nazveme *isogenií*. Pokud mezi E_1, E_2 existuje isogenie, nazveme je *isogenní*.

Isogenie ϕ pak tedy definuje homomorfismus $E_1(\overline{K}) \longrightarrow E_2(\overline{K})$. Pokud naši isogenii uvážíme jako zobrazení:

$$\phi : E_1 \longrightarrow E_2 : (x, y) \mapsto (u(x, y), v(x, y))$$

pro u, v lomené funkce nad K, tak po substituci $(x, y) \mapsto (x/z, y/z)$, požadujeme, aby $(0 : 1 : 0) \mapsto (0 : 1 : 0)$.

Definice 1.3.2. Pod *stupněm* isogenie ϕ budeme rozumět jejímu stupni jako lomené funkci v x, budeme značit $\deg \phi$.

Stejně jako jsme se zabývali torzní podgrupou našich křivek, nebude překvapením, že bude pro studium isogenií důležité, které body zobrazí do nekonečna. Tyto body i v případě isogenií tvoří podgrupu $E(\overline{K})$.

Definice 1.3.3. Pod *jádrem* isogenie ϕ rozumíme jádru ϕ, ve smyslu homomorfismu grup $E_1(\overline{K}) \longrightarrow E_2(\overline{K})$. Značíme $\ker\phi$ a počet jeho prvků $\#\ker\phi$.

Definice 1.3.4. Skládání, resp. sčítání isogenií definujeme následovně: $\phi\circ\psi := \phi(\psi)$, resp. $(\phi+\psi)P \;:=\; \phi\,(P) \;+\; \psi\,(P)$.

S isogeniemi jsme se již na naší (prozatím) krátké cestě několikrát setkali, jak násobení skalárem, tak isomorfismy zmíněné v předchozí kapitole, jsou isogeniemi. Násobení $[n]$ má jádro $E[n]$ a za chvíli si ukážeme, že má coby isogenie stupeň n^2. Isomorfismy jsou isogenie lineární a mají pouze triviální jádro. Zobrazení:

$$\phi : y^2 = x^3 + x \longrightarrow y^2 = x^3 + 11x + 62$$

mezi křivkami nad $\mathbb{Z}_{101}$ dané $(x,y) \mapsto \left(\frac{x^2+10x-2}{x+10}, \frac{x^2y+20xy+y}{x^2+20x-1}\right)$ je též isogenií, tentokrát stupně dvě. Jádrem ϕ je množina $\{\mathcal{O}, 10\}$, protože $x^2 + 20x - 1 = (x+10)^2$ v $\mathbb{Z}_{101}$.

Jedním z nejdůležitějších zobrazení na $\overline{\mathbb{F}_p}$ je tzv. *Frobeniův endomorfismus*, pojmenované po Ferdinandu Frobeniovi, kterému diktuje předpis $(x,y) \mapsto (x^p, y^p)$. Pevné body Frobeniova endomorfismu jsou přesně prvky $\mathbb{F}_p$, tudíž pro lomenou funkci f nad $\mathbb{F}_p$ platí: $f(x_1^p, \ldots, x_n^p) = f(x_1, \ldots, x_n)^p$. Speciálně: $0^p = 0, 1^p = 1, a^p + b^p = (a+b)^p$ a $a^p \cdot b^p = (ab)^p$. Navíc toto zobrazení je nad $\overline{\mathbb{F}_p}$ prosté, pokud $a^p = b^p$:

$$0 = a^p - b^p = (a-b)^p,$$

tedy $a = b$. Frobeniův endomorfismus je proto nad $\overline{\mathbb{F}_p}$ automorfismem.

n-tou mocninu Frobeniova endomorfismu definujeme jako $\pi^n : x \mapsto x^{p^n}$, přičemž víme, že pevné body π^n jsou právě prvky $\mathbb{F}_{p^n}$, tedy π^n je automorfismem je právě nad $\mathbb{F}_q$, kde $q = p^k, k \leqslant n$. Zobrazení s podobným předpisem převádějící eliptické křivky též nese jméno po Frobeniovi.

Definice 1.3.5. Buď $y^2 = x^3 + ax + b$ eliptická křivka nad $\mathbb{F}_q$. Zobrazení:

$$\pi_E : y^2 = x^3 + ax + b \longrightarrow y^2 = x^3 + a^q x + b^q,$$

dané:

$$(x,y) \mapsto (x^q, y^q),$$

se nazývá *Frobeniovým endomorfismem.*

Frobeniův morfismus fixuje právě $E(\mathbb{F}_q)$ a má pouze triviální jádro. Díky vlastnostem Frobeniova automorfismu můžeme říci, že komutuje s libovolnou isogenií nad $\mathbb{F}_q$, tj.:

$$\pi_E \circ \phi = \phi \circ \pi_E$$

pro libovolnou isogenii ϕ z E. Mocninu Frobeniova morfismu analogicky definujeme jako ${\pi^n}_E := \underbrace{\pi_E \circ \pi_E \circ \circ \circ \pi_E}_{n}$.

p-Frobeniův morfismus $(x, y) \mapsto (x^p, y^p)$ na E nad $\mathbb{F}_q$ pro $q \neq p$ již ne nutně definuje endomorfismus.

Když již máme solidní představu pojmu isogenie, pojďme se nyní pobavit o několika jejich základních vlastnostech.

Věta 1.3.6. *Buď $\phi : E \longrightarrow E_1$ isogenie stupně n. Pak existuje jediná isogenie $\hat{\phi} : E_1 \longrightarrow E$, která pro každou jinou isogenii $\psi : E_1 \longrightarrow E_2$ splňuje:*

(i) $\phi \circ \hat{\phi} = [n]_{E'}$,

(ii) $\hat{\phi} \circ \phi = [n]_E$,

(iii) $\widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi}$,

(iv) $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$,

(v) $\hat{\hat{\phi}} = \phi$.

Isogenii $\hat{\phi}$ budeme označnovat jako isogenii duální k ϕ.

Důkaz je k nalezení v [22, Thm. III.6.1].

Lemma 1.3.7. *Platí:*

$$\widehat{[n]} = [n] \qquad a \qquad \deg[n] = n^2.$$

Důkaz. Zjevně $\widehat{[0]} = [0]$ a $\widehat{[1]} = [1]$, dále postupujme indukcí dle n. Za pomocí věty 1.3.6, (iv), máme:

$$\widehat{[n+1]} = \widehat{[n]} + \widehat{[1]} = [n] + [1] = [n+1].$$

Protože $[-1] : P \mapsto -P$ je isogenií stupně 1, je $[-1]$ též duálem sama sebe. Pak díky $[-1] \circ [n] = [-n]$ máme první část hotovou. Z definice sčítání máme $[m] \circ [n] = [mn]$, tudíž $[n] \circ \widehat{[n]} = [n^2]$. Dle věty 1.3.6, (i), je $[n]$ isogenií stupně n^2. □

Duální isogenie k ϕ je pak z našeho lemmatu též isogenií stupně n. Navíc pro libovolnou isogenii ϕ z E stupně n je $\ker \phi \subseteq \ker[n]$, neboť libovolný prvek v jádře ϕ se $\hat{\phi}$ pošle do nekonečna E.

Jádro má isogenie nejvýše tak velké jádro jako její stupeň

Definice 1.3.8. Mějme $E, E' \in K$ a $\phi : E \longrightarrow E'$ isogenie stupně n. Pokud je $\#\ker \phi = n$, pak o ϕ řekneme, že je *separabilní*. V opačném případě řekneme, že ϕ je *neseparabilní*. V případě, že je $\deg \phi$ roven mocnině $\operatorname{char} K$, mluvíme o ϕ jako o *čistě neseparabilní*.

Pozoruhodné na tomto pojmenování je fakt, že separabilita a čistá neseparabilita se ne nutně vylučují. Každý isomorfismus je isogenií stupně 1 s jádrem velikosti 1, tedy separabilní, přičemž $p^0 = 1$, takže isomorfismy jsou čistě neseparabilní. Naopak Frobeniův automorfismus je isogenie neseparabilní i čistě neseparabilní. Charakterizujme dále separabilní isogenie.

Věta 1.3.9. *Ať $E, E' \in K$ jsou eliptické křivky a isogenie $\phi : E \longrightarrow E'$, která převádí $x \mapsto \frac{u(x)}{v(x)}$ pro $u, v \in K[x]$ nesoudělné. Pak ϕ je separabilní, právě pokud $\left(\frac{u}{v}\right)' = 0$.*

Důkaz. Rovnost $0 = \left(\frac{u(x)}{v(x)}\right)' = \frac{u'v - v'u}{v^2}$ v K nastane právě pokud $u'v = v'u$. Za předpokladu nesoudělnosti polynomů u, v mají v $\overline{K}$ u, u' stejnou množinu kořenů (včetně násobnosti). Protože ale $\deg u > \deg u'$, ekvivalentně platí $\deg u' = 0$, obdobně pro v.

Speciálně nad tělesem s nulovou charakteristikou jsou všechny isogenie neseparabilní. Zaměřme se na konečný případ:

Důsledek 1.3.10. *Isogenie ϕ z křivky E nad tělesem $\mathbb{F}_q$ charakteristiky p je separabilní právě pokud existuje isogenie ψ taková, že $\phi(x) = \psi(x^p)$.*

Důkaz. Mějme $\phi = \frac{u}{v}$. Rovnost $u' = 0$ nastane právě pokud má každý jednočlen x^i s nenulovým koeficientem exponent dělitelný p, neboli $u(x) = f(x^p)$ pro polynom $f \in \mathbb{F}_q[x]$. Obdobná rovnost platí i pro v. Rovnost $u' = 0 = v'$ nastane proto právě pokud $\phi(x) = \psi(x^p)$ pro ψ lomenou funkci nad $\mathbb{F}_q$. π je automorfismem na $\mathbb{F}_q$, tedy $\phi(x) = \psi(x^p)$ je isogenie právě pokud ψ je isogenie. □

Iterací této věty a faktem, že Frobenius komutuje s libovolnou isogenií nad $\mathbb{F}_q$, máme:

Důsledek 1.3.11. *Buď ϕ isogenie nad $\mathbb{F}_q$. Pak existuje separabilní isogenie ψ a $n \in \mathbb{N}_0$, že:*

$$\phi = \psi \circ \pi^n.$$

Věta 1.3.12. *Každá separabilní isogenie ϕ z E je, až na isomorfismus, jednoznačně určena svým jádrem. Pokud je tak $G = \ker \phi$ grupa tvořená jádrem ϕ, můžeme značit E/G cílovou křivku ϕ.*

Důkaz tvrzení je podán v [29, Prop. 12.12], nicméně autor využívá nástrojů Galoisovy teorie, jejíž znalost od čtenáře nepředpokládáme.

Separabilní isogenie z $E \longrightarrow E'$ je daná lomenou funkcí nad K a známe-li její jádro, dokážeme ji explicitně spočíst, přičemž libovolná podgrupa $E(\overline{K})$ je jádrem separabilní isogenie. Vzorce udávající (až na isomorfismus) přesný tvar separabilní isogenie z $E \longrightarrow E'$ s daným jádrem se nazývají *Véluovy* po Jeanu Véluovy, který je první publikoval roku 1971 ve [28]. Jejich zápis je obecně velmi nezáživný a pro nás je nepodstatný, stačí nám mít v povědomí, že separabilní isogenie s daným jádrem můžeme explicitně vyjádřit, jejich

přesnou formu a důkaz správnosti jsou k uvedeny v [4, Ch. 8.2]. V Sage 9.0 jsou Véluovy vzorce implementovány pro isogenii z E s jádrem G v $O(\#G)$ příkazem:

`EllipticCurveIsogeny(E,ker G)`,

Tvrzení 1.3.12 můžeme konkrétněji formulovat následovně:

$$(E/\langle A\rangle)/\langle B\rangle \cong (E/\langle B\rangle)/\langle A\rangle.$$

Věta 1.3.13. *Sutherland 6.11*

1.4 Torzní body

Vraťme se k operaci násobení bodů. U lemmatu 1.3.7 jsme si ukázali, že $\deg[m]$, jakožto racionální funkce, je m^2. Díky [22, Exc. 3.30] ((((tohle bych asi chtěl rozepsat)))) můžeme proto říci:

Věta 1.4.1. *Nechť je E eliptická křivka nad K a m nenulové číslo. Pak:*

- *Pokud* $\operatorname{char} K \nmid m$, *tak* $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$,
- *Pokud* $p = \operatorname{char} K > 0$*:*

$$E[p^i] \cong \begin{cases} \{\mathcal{O}\}, & \text{pro každé nezáporné } i, \\ \mathbb{Z}_{p^i}, & \text{pro každé nezáporné } i. \end{cases}$$

Plný důkaz je k nalezení v [22, Cor. III.6.4].

V každém případě je $[m]$ pro $\operatorname{char} K \nmid m$ isogenie separabilní, $[p^i]$ je pozoruhodně separabilní i čistě neseparabilní.

Vidíme, že existuje rodina křivek, která má pouze triviální p-torzi.

Definice 1.4.2. Pokud máme $E[p] \cong \{\mathcal{O}\}$, nazveme E *supersingulární*. Jinak E budeme říkat *obyčejná*.

Poznámka 1.4.3. Algebraický uzávěr $\mathbb{F}_p$ je shodný s uzávěrem $\mathbb{F}_{p^n}$ pro každé n, neboť kořeny $x^{p^n-1} - 1$ jsou právě prvky $\mathbb{F}_{p^n}^*$. Protože je n-torze množinou $P \in E(\overline{K})$, že $[n]P = \mathcal{O}$, je supersingularita E nad $\mathbb{F}_p$ ekvivalentní její supersingularitě nad $\mathbb{F}_{p^n}$.

Rozdělení křivek na obyčejné a supersingulární bude vhodné v mnoha ohledech, jak při diskuzi vlastností křivek, tak z kryptografického hlediska, k tomu však musíme hlouběji tyto křivky studovat.

1.5 Supersingulární křivky

Slovo supersingulární napovídá, že na křivky takto pojmenované nenarazíme příliš často, tedy že jsou mezi všemi eliptickými křivkami vzácné. Tato malá větev křivek se od obyčejných křivek fundamentální liší, přičemž jejich nespočetné rozdíly jsou mnohdy těsně provázáné. Ve skutečnosti většina vlastností, o kterých se zmíníme, se bere jako ekvivalentní definice supersingularity, každá vhodná v jistém úhlu pohledu. Jejich vlastnosti ve všech směrech, které jsme prozatím zmínili, do podrobna prozkoumáme, počínaje jejich definicí za pomocí torze.

Počítání celé p-torze je pro velká prvočísla výpočetně náročné, chtěli bychom najít vhodnější kritéria. Ukáže se, že eliptické křivky nesou pouze specifické počty bodů.

Věta 1.5.1. *Nechť E je křivka nad $\mathbb{F}_q$, kde $q = p^r$ je mocnina prvočísla $p > 3$. Pak:*

$$\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$$

nastane právě pokud E je supersingulární.

Důkaz je k nalezení v [29, Prop. 4.31].

Důsledek 1.5.2. *Ať E je křivka nad $\mathbb{F}_p$ s $p > 3$. Pak:*

$$\#E(\mathbb{F}_p) = p + 1$$

nastane právě pokud E je supersingulární.

Důkaz. Pokud $\#E(\mathbb{F}_p) = p + 1$, tak dle předchozí věty je E supersingulární. Pro E supersingulární je $\#E(\mathbb{F}_p) \equiv 1 \pmod{p}$, tedy jestli $\#E(\mathbb{F}_p) \neq p + 1$, je $p + 1 - \#E(\mathbb{F}_p)$ v absolutní hodnotě alespoň p. Dle Hasseho věty 1.1.5 je toto číslo v absolutní hodnotě rovno nejvýše $2\sqrt{p}$, neboli:

$$2\sqrt{p} \geqslant |p + 1 - \#E(\mathbb{F}_p)| \geqslant p,$$

což je spor s $p > 3$. □

Pro určení supersingularity E nás tak bude do jisté míry zajímat číslo $t = p+1-\#E(\mathbb{F}_p)$. Číslo t je úzce spojené s Frobeniovým endomorfismem ??. O tomto propojení se budeme podrobněji bavit v naší 3. kapitole.

Samotné počítání bodů na eliptické křivce je pro nás zatím obtížný úkon, pro $\mathbb{F}_p$ s malým p můžeme jednoduše projít všechny možné hodnoty x, jak můžeme vidět na následujícím příkladu:

Příklad 1.5.3. Ukažme, že křivka:

$$E : y^2 = x^3 + 10x + 7$$

nad $\mathbb{F}_{13}$ je supersingulární.

Řešení. Mějme $(x, y) \in E(\mathbb{F}_{13})$. Pokud je číslo $x^3 + 10x + 7$ v $\mathbb{F}_{13}$ nenulový čtverec, existují dvě vyhovující y, jedno, pokud je rovno nule, a jinak žádné. Můžeme si proto vypsat hodnoty pravé strany ve všech možných hodnotách a za pomocí Eulerova kritéria snadno určit, zda je výraz čtvercem, viz následující tabulka:

x	$x^3 + 10x + 7$	$\left(\frac{x^3+10x+7}{13}\right)$	počet řešení
0	7	-1	0
1	5	-1	0
2	9	1	2
3	12	1	2
4	7	-1	0
5	0	0	1
6	10	1	2
7	4	1	2
8	1	1	2
9	7	-1	0
10	2	-1	0
11	5	-1	0
12	9	1	2

Spolu s bodem v nekončnu je $\#E(\mathbb{F}_{13}) = 13 + 1 = 14$ a jsme hotovi z důsledku 1.5.2. □

U speciálních případů křivek můžeme rafinovaně využít poznatky z elementární teorie čísel:

Příklad 1.5.4. Ukažme, že křivka:

$$E : y^2 = x^3 + x$$

nad $\mathbb{F}_p$ pro $p \equiv -1 \pmod 4$ je supersingulární.

Řešení. Pro $p \equiv -1 \pmod 4$ je $\left(\frac{-1}{p}\right) = -1$, takže pokud pro a, b platí $p \mid a^2 + b^2$, jsou obě dělitelná p. V opačném případě totiž z $a^2 \equiv -b^2 \pmod p$ vyvodíme:

$$\left(\frac{a}{b}\right)^2 \equiv -1 \pmod p,$$

spor. Nenulových čtverců v $\mathbb{F}_p$ je právě $\frac{p-1}{2}$, tudíž každý prvek $\mathbb{F}_p$ je buď čtverec, nebo mínus čtverec. Pro $x = 0$ máme pouze $y = 0$ a pro každé $x \in \mathbb{F}_p^*$ je právě jedno z čísel $x^3 + x, (-x)^3 - x$ nenulovým čtvercem, protože je $x^2 \neq -1$. Pro každou dvojici $(x, -x)$ tak máme právě dvě řešení, dohromady $p - 1$. Spolu s $(0, 0)$ a bodem v nekonečnu je $\#E(\mathbb{F}_p) = p + 1$, díky větě 1.5.2 je E supersingulární. □

Díky poznámce 1.4.3 je křivka $E : y^2 = x^3 + x$ supersingulární nad konečným tělesem s charakteristikou $p \equiv -1 \pmod 4$.

Náš první postup počítání počtu bodů na křivce běží nejlépe v $O(p)$ čase, což je pro prvočísla $\log_2(p) > 500$, tedy praktické kryptografické velikosti, jednoduše příliš pomalé. Jedním z nejdřívějších velkých pokroků v počítání bodů byl *Schoofův algoritmus*, poprvé zveřejněn roku 1985 v [23], který $\#E(\mathbb{F}_q)$ jako první dokáže spočíst deterministicky v čase polynomiálním v $\log(q)$. Poskytuje tedy exponenciální zrychlení oproti našemu předchozímu postupu.

Pojďme se podívat na samotnou strukturu bodů na supersingulární E nad $\mathbb{F}_q$.

Věta 1.5.5. *Buď E supersingulární eliptická křivka nad $\mathbb{F}_p$. Pak $j(E) \in \mathbb{F}_{p^2}$.*

Důkaz.

Věta 1.5.6. *Buď E eliptická křivka nad $\mathbb{F}_p$. Pak libovolná křivka $E' \cong E$ nad $\mathbb{F}_p$ je supersingulární právě pokud je E supersingulární.*

Pokud uvážíme graf všech j-invariantů nad $\overline{\mathbb{F}_p}$ (kterým přiřadíme jejich příslušnou třídu isomorfismů), kde dva vrcholy jsou propojené právě pokud jejich křivky jsou isogenní, tento graf je rozdělen na obyčejné a supersingulární komponenty.?? z každého vrcholu vede $0, 1, 2, p+1$ hran, přičemž supersingulární komponenty jsou $p+1$-regulární, zatímco komponenty obyčejné tvoří zásadně odlišnou strukturu, tzv. *vulkány*, kde „kráter“ je tvořen regulárním grafem stupně nejvýše 2 a každý jiný vrchol je buď listem, či má $p+1$ sousedů.

obrázek vulkánu.

Věta 1.5.7. *Buď E supersingulární eliptická křivka nad $\overline{\mathbb{F}}$. Pak existuje E' nad $\mathbb{F}_{p^2}$, že $E \cong E'$.*

Věta 1.5.8. *Thm 54 v DeFeo.*

Kapitola 2

Uplatnění v kryptografii

Přes Caesarovu šifru až po šifrování za pomocí Enigmy v období druhé světové války, po většinu lidské historie se využívaly kryptografické systémy založené na faktu, že obě komunikující partie si po domluvě vyberou způsob maskování zprávy a ten pro ostatní zůstává skrytý. Příkladem je právě o kolik písmen v Caesarově šifře transponujeme. Tento způsob nutně závisí na faktu, že se obě strany před výměnou mají možnost přes bezpečný kanál na tomto způsobu domluvit. S přibývajícím počtem účastníků a frekvencí komunikace, na příklad našeho každodenního interagování na internetu, kde musí konverzace mezi všemi účastníky být bezpečná, je bohužel na úkor ceny přenosu třeba vyšší počet a velikost klíčů, a přibývá risk kompromitace.

Kvůli takovým obavám přišli Whitfield Diffie a Martin Hellman [7] roku 1976 s revolučním nápadem: asymetrickou kryptografií, kde každý z účastníků má svůj vlastní *privátní klíč*, který s nikým nesdílí. Všechny strany, i potenciální útočník, znají několik informací, které jsou známé jako *veřejné parametry*. Obě komunikující strany za pomocí veřejných informací tajně transformují svůj privátní klíč a výsledek, který budeme nazývat *veřejným klíčem*, publikují. Oba účastnící vezmou veřejný klíč toho druhého a provedou s ním ty samé tajné kroky závisící na jejich privátním klíči. Podstatou takové výměny je, že na jejím konci získají obě původní strany netriviální informaci, tedy informaci takovou, že žádná třetí strana ji nedokáže snadno uhodnout, za pomocí níž poté mohou společnou komunikaci šifrovat a nikdo jiný již jejich zprávy neuvidí. Předpokládá se, že pouze ze znalosti veřejného klíče je pro každou další partii těžké replikovat klíč privátní a že pole možných sdílených informací je obrovské. Vyhneme se tak přímočarým řešením hrubou silou.

Pojďme se podívat na protokol, který Diffie a Hellman navrhli. Budeme o něm dále mluvit jako o *Diffie-Hellmanově výměně*. Je založena na problému *diskrétního logaritmu* prvku $a \in \mathbb{Z}_p^*$. Tento problém po nás ze znalosti primitivního kořene g modulo p žádá najít k, že $g^k = a$ v $\mathbb{Z}_p$. Obecně můžeme $\mathbb{Z}_p$ nahradit cyklickou grupou G a mít g její generátor. Protokol požaduje, aby nebyl diskrétní logaritmus spočitatelný efektivně, tj. v polynomiálním čase vzhledem k velikosti grupy, jinak může útočník jednoduše privátní klíče obou stran

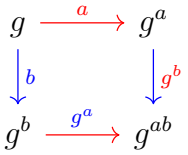
spočíst, ale mocnění bylo. Umocnit číslo dokážeme v logaritmickém čase, a v konečné grupě nám stačí umocnit pouze na exponent modulo řádu grupy.

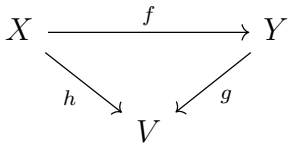
Veřejné parametry: Grupa G řádu p, kde p je prvočíslo, s generátorem g.

Alfréd		Blažena
Vstup: $a \in G^*$		**Vstup:** $b \in G^*$
	$\xrightarrow{g^a}$	
	$\xleftarrow{g^b}$	
$G_{AB} := \left(g^b\right)^a = g^{ab}$		$G_{BA} := \left(g^a\right)^b = g^{ba}$
Výstup: G_{AB}		**Výstup:** G_{BA}

Algoritmus 1: Diffie-Hellmanova výměna

Díky předpokladu, že G je cyklická, je i abelovská, tedy $G_{AB} = g^{ab} = g^{ba} = G_{BA}$.





Řád G se prakticky bere prvočíslo $q = 2p + 1$ takové, že p je prvočíslo, pak p nazveme tzv. *Sophie-Germainovým prvočíslem* a q zase *bezpečným prvočíslem*. V takovém případě má G podgrupu (velkého) prvočíselného řádu p, což je z kryptografického hlediska žádané, tuto grupu totiž je obtížnější spočíst. Navíc bezpečná prvočísla skýtají i výhody pro inicializování výměny, pro taková prvočísla dokážeme totiž snadno nalézt primitivní kořen v $\mathbb{Z}_q$. Konkrétně, je-li g primitivní kořen modulo q, má řád $q - 1 = 2p$ modulo q, právě pokud $g^p \equiv -1 \pmod{q}$. Stačí nám pak najít $g^p \pmod{q}$, což nám mohou usnadnit nástroje jako Eulerovo kritérium, díky kterému je postačující mít g kvadratický nezbytek modulo q.

Veřejné klíče g^a, g^b, jsou nicméně, jak jejich název napovídá, veřejné, a má k nim přístup libovolná jiná osoba. Dejme tomu, že Eva, která má přístup pouze k veřejně dostupným informacím G, g, g^a, g^b, by chtěla též znát sdílené tajemství. Jeden způsob, jak by mohla tajnou informací získat, je pokud by spočítala diskrétní logaritmus $\log_g(g^a) = a$, nicméně

předpokládáme, že to je obtížné. Na klasických počítačích jsou nejlepší známé útoky na problémy, jako diskrétní logaritmus a faktorizace čísla, na čemž jsou založené mnohé známé protokoly, subexponenciální, nicméně na počítačích kvantových jsou už od poloviny 90. let známé algoritmy polynomiální. V čem však takto podstatné zrychlení spočívá?

2.1 Kvantové počítače

If computers that you build are quantum,
Then spies of all factions will want 'em.
Our codes will all fail,
And they'll read our email,
Till we've crypto that's quantum, and daunt 'em.

Jennifer a Peter Shorovi

Ve světě kvantových obvodů místo s klasickými bity pracuje s *qubity*. V n bitovém systémů máme 2^n různých stavů, které v n qubitovém systému tvoří generátory našeho prostoru. Podstatou je, že před pozorováním nemá daný qubit jednu z těchto hodnot, ale jejich (komplexní) superpozici. Generátory systému s jedním qubitem jsou stavy $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$, systém je tedy:

$$\alpha|0\rangle + \beta|1\rangle,$$

kde α, β jsou komplexní čísla $|\alpha|^2 + |\beta|^2 = 1$. Zápis $|\psi\rangle$ je tzv. *ket* notace, kde ψ je vektor.

V dvojqubitovém systému máme čtyři báze a stav takového systému je:

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle,$$

kde $\alpha, \beta, \gamma, \delta$ jsou komplexní čísla s $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. Qubity jsou značně nestabilní, musí být uchovány v izolované soustavě, nejčastěji v neutrinu, přičemž jakékoli narušení, i pouhé pozorování hodnoty qubitu, ho kolapsuje na jednu hodnotu, kterou už pak zůstane. Při pozorování má qubit pravděpodobnost ukázat stav právě takovou, kolik je druhá mocnina absolutní hodnoty příslušného koeficientu, proto ona normalizační podmínka. Pokud bychom pozorovali náš jedno-qubitový systém, s pravděpodobností $|\alpha|^2$ získáme výstup 0, s pravděpodobností $|\beta|^2$ získáme 1.

Můžeme ale též náš qubit vyjádřit ve vektorovém zápisu:

$$|\psi\rangle = \begin{bmatrix}\alpha\\\beta\\\gamma\\\delta\end{bmatrix},$$

což samozřejmě zobecníme pro systémy více qubitů. Tento vektor je díky naší podmínce jednotkový. V klasických obvodech máme brány, které jsou lineární zobrazení našich stavů,

příklady takových bran jsou OR a NOT. V kvantových obvodech bereme jako brány právě unitární matice a jejich operaci násobení, neboť ty zachovávají normu vektoru, jejich výsledky jsou proto opět qubity.

Nedá moc práce ukázat, že všechny operace proveditelné na klasickém obvodu jsou replikovatelné kvantovými branami, model kvantového počítače, jakožto obvodu, je tak alespoň stejně silný jako počítač klasický.

Jedním z důvodů, proč se věří, že s veřejně dostupnými kvantovými počítači přijde nová éra výpočetní techniky je, že existují procesy, o kterých se dodnes neví, zda jsou v polynomiálním čase proveditelné na počítači klasickém, a jejichž kvantové algoritmy již byly nalezené. Klasické násobení čísel (n bitových), zabere $O(n^2)$ klasických operací, případně až $O(n^2 \log n)$ pro velká čísla, neboť jejich násobení neprovedeme v konstantním čase. Násobení dvou čísel se dá redukovat na problém násobení dvou polynomů, přičemž diskrétní Fourierova transformace z našeho polynomu nám dá informaci o hodnotách polynomu v odmocninách z jednotky, což je vše, co potřebujeme k určení polynomu. Rychlá Fourierova transformace toto dokáže pouze v $\Theta(n \log n)$ čase. Díky její multiplikativitě, linearitě a její inverzní funkci pak dokážeme zpětně v tomto čase získat součin dvou čísel.

Kvantová Fourierova transofrmace (QFT), která obdobnou operaci aplikuje na náš vektor, na klasickém počítači s n qubity počítá s 2^n prvky a nejlepší známé algoritmy ji provádí v $O(n^2 2^n)$ čase, zatímco na kvantových počítačích pracuje v kvadratickém čase a s jistou přesností i v $\Theta(n \log n)$, viz [1, Ch. 4. a 5.] pro více informací. Vynásobit dvě matice řádu n na klasickém počítači zjevně nedokážeme rychleji než v řádově n^2 operacích, neboť musíme pracovat se všemi prvky matice. Kvantový počítač dokáže dvě matice řádu n vynásobit užitím $O(n^{5/3})$ kvantových bran.

Faktorizaci celého čísla dokážeme snadno převést na problém hledání řádu čísla a modulo n. V devadesátých letech minulého století přišel Peter Shor [24] s řešením problému diskrétního logaritmu na kvantovém počítači užívajícím polynomiálního počtu kvantových bran, čímž je řešen i problém rozkladu celého čísla. Mnoho v té době užívaných protokolů na šifrování a podpis dat bylo založeno na jednom z těchto dvou problém, nejprominentější z nich je známý jako RSA [19].

Poznamenejme, že nejefektivnější známé klasické algoritmy rozkládající velká čísla (dejme tomu $\log_2(n) > 200$) užívají poznatky z teorie eliptických křivek a algebraické teorie čísel, na kterou ještě přijde řeč. Tyto algoritmy nesou názvy *Elliptic-curve factorization* a *General number field sieve*, první z nich je založen. Oba běží v očekávaném subexponenciálním čase.

2.2 Kryptosystémy založené na isogeniích

Nyní, když jsme již trochu obeznámeni s kvantovými algoritmy, vraťme se zpět k eliptickým křivkám. Zjevnou adaptací Diffie-Hellmanova protokolu je protokol, který nese název ECDH (Elliptic Curve Diffie-Hellman):

Veřejné parametry: Prvočíslo p a eliptická křivka E nad $\mathbb{Z}_p$ s generátorem $G \in E(\mathbb{Z}_p)$.

Alfréd		Blažena
Vstup: $a \leqslant \#E(\mathbb{Z}_p) - 1$		**Vstup:** $b \leqslant \#E(\mathbb{Z}_p) - 1$
	$\xrightarrow{[a]G}$	
	$\xleftarrow{[b]G}$	
$G_{AB} := [a]([b]G) = [a][b]G$		$G_{BA} := [b]([a]G) = [b][a]G$
Výstup: G_{AB}		**Výstup:** G_{BA}

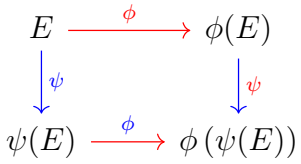
Algoritmus 2: Protokol ECDH

Tento protokol je založen na předpokladu, že diskrétní logaritmus na eliptických křivkách, tedy ze znalosti P a $[n]P$ spočíst n, je těžký problém. Není znám žádný algoritmus, který by nezískal společné tajemství výpočtem privátních klíčů obou stran. ???

První kryptografické schéma založené na isogeniích obyčejných eliptických křivek navrhl Couveignes [3] již v roce 1997, nicméně nepublikoval jej po dalších deset let. Grafy isogenií byly studovány přes přelom tisíciletí [8], ?. Roku 2006 Rostovtsev a Stolbunov [21] nezávisle na Couveignovi navrhli protokol založen na cestách v grafu obyčejných isogenií.

???
Po celou tuto dobu se supersingulárním křivkám nevěnovalo druhé myšlenky,

Pojďme se nyní znovu podívat na větu 1.3.12. Křivky $\phi(\psi(E)), \psi(\phi(E))$ sdílí j-invariant, neboť jsou isomorfní, což by v potenciálním protokolu založeném na isogeniích mohlo být sdílené tajemství obou stran.
Pokud tak mají obě strany danou počáteční křivku E nad $\overline{\mathbb{F}_q}$ a vyberou si tajné separabilní isogenie ϕ_A, resp. ϕ_B, kter pošlou druhé straně $\phi_A(E)$, resp. $\phi_B(E)$, pouze již s malým množstvím dalších informací obě strany snadno spočtou své tajemství. Takové myšlenky měli De Feo, Jao a Plût v [6], nicméně než se dostaneme přímo k jejich navrhovaném protokolu SIDH, musíme diskutovat několik důležitých detailů, které výměnu umožňují.



Jak napovídá název protokolu, budeme pracovat se supersingulárními eliptickými křivkami E nad $\mathbb{F}_{p^2}$ pro prvočíslo $p = \ell_A^{e_A}\ell_B^{e_B} - 1$, kde ℓ_A, ℓ_B jsou (malá) prvočísla. Pokud E má Frobeniův endomorfismus, že $\pi^2 = [-2p]$, díky **??** je $\#E(\mathbb{F}_{p^2}) = (p+1)^2$, přičemž $E[p+1] \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$, tedy

Pak totiž z věty ? je $\#E(\mathbb{F}_{p^2}) = (p+1)^2$ a dle věty 1.5.1: $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$. Pro prvočíslo $p = \ell_A^{e_A}\ell_B^{e_B} - 1$, kde ℓ_A, ℓ_B jsou (malá) prvočísla, proto existují dva body G_1, G_2 řádu $\ell_A^{e_A}\ell_B^{e_B}$, které generují $E(\mathbb{Z}_{p^2})$. Speciálně dvojice $\langle P_A, Q_A\rangle := \langle [\ell_B^{e_B}]G_1, [\ell_B^{e_B}]G_2\rangle$, resp. $\langle P_B, Q_B\rangle := \langle [\ell_A^{e_A}]G_1, [\ell_A^{e_A}]G_2\rangle$, generují po řadě $\ell_A^{e_A}$, $\ell_B^{e_B}$ torzi.

Uvažme bod $P \in E[\ell_A^{e_A}]$ řádu ℓ_A^t a separabilní isogenii $\phi : E \longrightarrow E/\langle P\rangle$. Pokud bychom chtěli $E/\langle P\rangle$ spočíst, stačilo by spočítat celou $\langle P\rangle$ a za pomocí Véluových formulí spočíst výslednou křivku v čase $O(\ell_A^t)$, což zjevně není optimální.

Veřejné parametry: Grupa G řádu p, kde p je prvočíslo, s generátorem g.

Alfréd		Blažena
Vstup: $a \in G$		**Vstup:** $b \in G$
	$\xrightarrow{g^a}$	
	$\xleftarrow{g^b}$	
$G_{AB} := \left(g^b\right)^a = g^{ab}$		$G_{BA} := \left(g^a\right)^b = g^{ba}$
Výstup: G_{AB}		**Výstup:** G_{BA}

Algoritmus 1: Diffie-Hellmanova výměna

Poznámka 2.2.1. Dle věty 1.3.12 jsou křivky, které obě partie na konci protokolu získají, isomorfní. Nicméně pokud na výpočet isogenií užíváme Véluovy formule, tak můžeme heuristicky ověřit, že křivky vždy vycházejí dokonce shodné. Tato domněnka byla dokázána pravdivou v [10]. Místo j-invariantu konečné křivky tak můžeme za sdílené tajmenství považovat přímo koeficienty konečné křivky. Tímto krokem rozlišujeme isomorfní křivky a tedy ? útoky hrubou silou.

2.3 Možné útoky na SIDH

Když jsme obeznámeni s vnitřními machinacemi protokolu SIDH, pojďme se pokusit najít způsoby, jak jej rozbít.

Nejprve pozapomeňme na fakt, že známe obrazy generátorů ℓ torzí. Uvažme graf ℓ_A-isogenií ze supersingulární křivky E. Známe počáteční i koncový vrchol E, resp. E_A cesty na našem grafu, která je složená z kroků ϕ_i, což jsou ℓ_A-isogenie, a hledáme posloupnost ϕ_i. Náš úkol tak můžeme přefrázovat čistě jako hledání cesty v grafu ℓ_A isogenií.

Víme, že hledaná cesta má délku e_A, a každý j-invariant sousedí s právě $p+1$ dalšími. Můžeme jednoduše začít prohledávat graf z E, dokud nenarazíme na E_A. Ze všech ? cest končí ? v E_A, očekáváme proto, že na E_A narazíme v $O(\sqrt{p})$ evaluacích ℓ_A isogenie.

Tento postup můžeme vylepšit takzvaným „Meet in The Middle“ útokem, který běží rychleji na úkor prostorové náročnosti. Pod jeho návodem prohlédáváme jak z E, tak i z E_A, přičemž z E hledáme cesty délky $\left\lfloor \frac{e_A}{2} \right\rfloor$ a z E_A cesty délky $\left\lceil \frac{e_A}{2} \right\rceil$. Dle narozeninového paradoxu bychom očekávali shodu v ? evaluacích ℓ_A isogenie.

2.4 Varianty protokolu SIDH

Od jeho publikace v roce 2011 pár kolektivů autorů našlo varianty SIDH založené na různých vlastnostech isogenií. Pár z nich zde uveďme.

eSIDH.

BSIDH.

CSIDH.

SeaSign.

Kapitola 3

Algebraická teorie čísel

Ve snaze vybudovat teorii k hlubšímu studiu eliptických křivek a isogenií, natož diskuzi protokolu CSIDH, se musíme na tyto objekty podívat v naprosto odlišném světle. Opustíme proto na okamžik eliptické křivky a ponoříme se do světa algebraické teorie čísel.

Na světě se nachází myriáda kvalitních a podrobných materiálů ke studiu této krásné oblasti matematiky, já osobně vřele doporučuji [11],[15] či [17]. Jako stručný úvod motivovaný poznatky z elementární teorie čísel může též posloužit má SOČ, [16, kap. 2].

3.1 Moduly nad okruhem

Při definici vektorového prostoru požadujeme, aby byl sestrojen nad tělesem. Můžeme nicméně analogický objekt obecněji sestrojit nad libovolným okruhem.

Definice 3.1.1. Mějme grupu G s a množinu X. Pod *levou akcí* G na X rozumíme zobrazení $\cdot : G \times X \longrightarrow X$, pro které platí $1 \cdot x = x$ a $g \cdot (h \cdot x) = (g \cdot h) \cdot x$ pro $g, h \in G, x \in X$.

Definice 3.1.2. Akci $\cdot : G \times X \longrightarrow X$ nazveme *volnou*, pokud pro libovolná $x \in X$ a $g \in G$ rovnost $g \cdot x = x$ znamená $g = 1$.

Definice 3.1.3. Grupu M s operací $+$ pro okruh R nazveme *levým R-modulem* s akcí $\cdot : R \times M \longrightarrow M$, pokud $\cdot$ je asociativní a na $+$ oboustranně distributivní.

Analogicky definujeme i pravou akci G na X a pravý modul.

Vzpomeňme na definici volné grupy G, jakožto $G \cong \mathbb{Z}^r$ pro nějaké celé r, obdobně definujeme i volný modul.

Definice 3.1.4. Modul M okruhu R nazveme *volným*, pokud má $R-$bázi, tj. pro nějaká $m_i \in M$ lineárně nezávislá nad R je $M = \{r_1 m_1 + \cdots + r_k m_k | r_i \in R\}$. Říkáme, že množina $\{m_1, \ldots, m_k\}$ *generuje* M.

Definice 3.1.5. Pokud je k nejmenší přirozené číslo takové, že existuje k prvků M generujících M, řekneme, že *R-rank M* je k.

Pro R těleso je M volným modulem, tedy vektorovým prostorem nad R. R-rank M je pak roven stupni rozšíření $[R : M]$.

Každý komutativní okruh R je volným R-modulem, jehož R-rank je 1. Mezi $\mathbb{Z}$-moduly patří například okruh Gaussových celých čísel, jenž je volným modulem se $\mathbb{Z}$-rankem 2, či grupa $E[n]$ pro křivku nad K s $\operatorname{char} K \nmid n$, která má díky větě 1.4.1 rank 2. Naopak tělesa $\mathbb{Q}, \mathbb{C}$ jsou po řadě $\mathbb{Z}$-modul, resp. $\mathbb{Q}$-modul bez konečné báze, nejsou proto volné.

Trochu zajímavějším příkladem modulu je množina kvadratických polynomů nad reálnými čísly, což je volný $\mathbb{R}$-modul ranku 3 s bází $\{1, x, x^2\}$.

Příklad 3.1.6. Ukažme, že grupa je abelovská právě pokud je $\mathbb{Z}$-modulem.

Důkaz. Každá abelovská grupa G s operací $+$ je $\mathbb{Z}$-modulem s akcí $n \cdot a$, jakožto součet n čísel $a \in G$, pro záporná čísla $(-n) \cdot a = -(n \cdot a)$. Navíc pro $\mathbb{Z}$-modul s jednotkou 1 s operací $+$ platí:

$$x+y+x+y = 1\cdot(x+y)+1\cdot(x+y) = (1+1)\cdot(x+y) = (1+1)\cdot x+(1+1)\cdot y = x+x+y+y,$$

tedy $y + x = x + y$. □

Poznámka 3.1.7. Roku 1922 Luis Mordell v [13] dokázal, že pro libovolnou eliptickou křivku E je grupa $E(\mathbb{Q})$ konečně generovaná. Tento výsledek rozšířil André Weil v roce 1928 pro libovolnou projektivní křivku nad číselným tělesem [30], což je pojem, který si za chvíli objasníme. Obecně charakterizovat tuto grupu, či efektivně spočíst její rank, jsou dnes problémy stále velmi obtížné. Clayův institut tuto oblast matematiky považoval za tak důležitou, že roku 2000 mezi problémy tisíciletí (Millenium Prize Problems) zařadil tzv. *Birch-Swinnerton-Dyerovu domněnku*, která se zabývá asymptotickým chováním $E(\mathbb{F}_p)/p$ vzhledem k ranku naší křivky.

Podmnožiny R-modulů M, které jsou uzavřené na sčítání a násobení prvky R, jsou též R-moduly. Takový modul pak nazveme podmodulem.

Definice 3.1.8. Nechť M a N jsou R-moduly, přičemž $N \subseteq M$. Pak N nazveme *podmodulem M*. *Index* podmodulu N v M definujeme jako počet prvků faktorgrupy $M \setminus N$.

Věta 3.1.9. *Nechť M je volný $\mathbb{Z}$-modul a N jeho podmodul. Pak rank N je nejvýše tak velký, jako rank M. Speciálně je N volný.*

Hezký důkaz indukcí je podán v [17, Věta 1.3.8]. Pokud bychom však místo $\mathbb{Z}$ uvážili libovolný komutativní okruh R, tvrzení již ne nutně platí!

Příklad 3.1.10. Ukažme, že $\mathbb{Z}_6$-podmodul $2\mathbb{Z}_6 = \{0, 2, 4\}$ není volný.

Řešení. Pokud by modul $2\mathbb{Z}_6$ měl nad $\mathbb{Z}_6$ bází, musí být její prvky nad $\mathbb{Z}_6$ lineárně nezávislé. Nicméně $0 \cdot 3 = 2 \cdot 3 = 4 \cdot 3 = 0$, přičemž $3 \neq 0$ v $\mathbb{Z}_6$. Žádná podmnožina $S \subseteq 2\mathbb{Z}_6$ tedy není nad naším okruhem lineárně nezávislá, protože $3S = \{0\}$. □

Obdobně vidíme, že pokud R je okruh, který není oborem integrity, obsahující nenulové prvky x, y se součinem 0, a M je jeho volný podmodul, pak xM je podmodul M, který není volný.

Čtenář se mohl setkat s pojmem *tenzorový součin* vektorových prostorů V a W, neboli vektorový prostor U disponující bilineárním zobrazení $V \times W \longrightarrow U$. My tuto definici rozšíříme na moduly nad komutativním okruhem.

Definice 3.1.11. Budiž R komutativní okruh a a, b jeho prvky. Pak jejich *tenzorový součin* $a \otimes b$ definujeme jako výraz, který je na sčítání oboustranně distributivní a pro každé $r \in R$:

$$(ra) \otimes b = r(a \otimes b) = a \otimes (rb).$$

Definice 3.1.12. Buďte R okruh a M a N levý, resp. pravý R-modul. Pak *tenzorový součin* M a N je volný R-modul definovaný následovně:

$$M \otimes_R N = \sum r_i m_i \otimes n_i$$

pro každá $r_i \in R, m_i \in R, n_i \in N$. Jeho prvky nazveme *tenzory*.

Definice tenzorového součinu je unikátní až na isomorfismus.

Příklad 3.1.13. Buďte m, n nesoudělná celá čísla. Ukažme, že $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n = \{0\}$.

Řešení. Máme:

$$m(1 \otimes 1) = m \otimes 1 = 0 \otimes 1 = 0,$$
$$n(1 \otimes 1) = 1 \otimes n = 1 \otimes 0 = 0.$$

Dle Euklidova algoritmu existují $x, y \in \mathbb{Z}$, že $xm + yn = 1$. Pak:

$$1 \otimes 1 = (xm + yn)(1 \otimes 1) = xm(1 \otimes 1) + yn(1 \otimes 1) = 0.$$

Pro každá $x \in \mathbb{Z}_m, y \in \mathbb{Z}_n$ pak platí $x \otimes y = x(1 \otimes y) = xy(1 \otimes 1) = 0$. □

Věta 3.1.14. *Každý prvek $M \otimes_R N$ se dá zapsat jako:*

$$\sum m_i \otimes n_i$$

pro nějaká $m_i \in M, n_i \in N$.

3.2 Číselná tělesa

Definice 3.2.1. Komplexní číslo α, které je kořenem polynomu $P \in \mathbb{Z}[x]$, nazveme *algebraické*. Pokud je navíc α kořenem monického (normovaného) polynomu nad $\mathbb{Z}$, nazveme jej *celým algebraickým* číslem.

Definice 3.2.2. Konečná rozšíření racionálních čísel obsahují pouze čísla algebraická, tato tělesa proto nazveme *algebraická číselná tělesa*, pro jednoduchost je budeme nazývat pouze *číselná tělesa*.

Definice 3.2.3. Pod stupněm číselného tělesa rozumíme stupni jeho rozšíření nad $\mathbb{Q}$ jakožto vektorového prostoru. Číselná tělesa stupně 2 nazveme *kvadratická*.

Věta 3.2.4. *Buď K kvadratické těleso. Pak $K = \mathbb{Q}(\sqrt{m})$ pro nějaké celé m.*

Důkaz. K je $\mathbb{Q}$-modul ranku $[K : \mathbb{Q}] = 2$, má tedy bázi velikosti nejvýše 2, je ve tvaru $\{ax + by | x, y \in \mathbb{Q}\}$ pro nějaká $x, y \in K$. Nutně tak každý prvek K má minimální polynom nad $\mathbb{Z}$ nejvýše kvadratický, tedy je tvaru $a+b\sqrt{m}$ pro celá m a a, b racionální. Pokud by v K ležely dvě různé celé odmocniny, tj. lineárně nezávislá čísla $\sqrt{m}$ a $\sqrt{n}$ pro $m, n \in \mathbb{Z} \setminus \{1\}$ bezčtvercová, tak v K leží i $\sqrt{m} + \sqrt{n}$. Nicméně minimální polynom tohoto čísla má za kořeny všechna čísla $\pm\sqrt{m} \pm \sqrt{n}$, je tedy alespoň kvartický, spor.

Pokud tedy v K leží iracionální $\sqrt{m}$, pak 1 a $\sqrt{m}$ jsou dva prvky našeho tělesa lineárně nezávislé nad $\mathbb{Q}$, tak protože báze K obsahuje nejvýše 2 prvky, je $\{1, \sqrt{m}\}$ bází K. Každý prvek K je pak tvaru $n = a + b\sqrt{m}$ pro racionální a, b. Protože všechny prvky $\mathbb{Q}(\sqrt{m})$ jsou právě tohoto tvaru, je $K = \mathbb{Q}(\sqrt{m})$. □

Pokud $m > 0$, nazveme K *reálným* kvadratickým tělesem, v opačném případě jej nazveme *imaginárním* kvadratickým tělesem.

Pojďme si trochu charakterizovat celá algebraická čísla našeho tělesa.

Věta 3.2.5. *Komplexní číslo α je celé algebraické právě pokud je $\mathbb{Z}[\alpha]$ volným $\mathbb{Z}$-modulem.*

Důkaz. Je-li α celé algebraické číslo s minimálním polynomem $f \in \mathbb{Z}[x]$ stupně n, pak $\mathbb{Z}[\alpha]$ je volný $\mathbb{Z}$-modul s bází $\{1, \alpha, \ldots, \alpha^{n-1}\}$, číslo α^k pro $k \geqslant n$ totiž dokážeme z $\alpha^{k-n}P(\alpha) = 0$ vyjádřit jako $\mathbb{Z}$-lineárních kombinace mocnin α ostře nižších k, protože je P monický.

Naopak pokud je $\mathbb{Z}[\alpha]$ volný $\mathbb{Z}$-modul, je generovaný prvky $f_i(\alpha) \in \mathbb{Z}[\alpha]$ pro polynomy $f_1, \ldots, f_k \in \mathbb{Z}[x]$. Pro číslo t ostře větší $\max(\deg f_i)$, leží α^t v $\mathbb{Z}[\alpha]$, je proto vyjádřitelné jako $\mathbb{Z}$-lineární kombinace $f_i(\alpha)$. Pro nějaká $a_i \in \mathbb{Z}$:

$$\alpha^t = \sum a_i f_i(\alpha),$$

tedy α je kořenem monického polynomu $x^t - \sum a_i f_i(x)$, dle definice je celé algebraické. □

Díky tomuto tvrzení můžeme jednoduše odůvodnit, proč necelá racionální čísla nejsou celá algebraická.

Příklad 3.2.6. Ukažme, že pro a, b nesoudělná celá s $|b| > 1$ je racionální číslo $\frac{a}{b}$ algebraické číslo, ale již není celé algebraické.

Důkaz. Číslo $\frac{a}{b}$ je kořenem polynomu $bx - a \in \mathbb{Z}[x]$, tedy je algebraické. Dále za předpokladu $|b| > 1$ uvažme p prvočíslo dělící b. Pokud by bylo $\frac{a}{b}$ celým algebraickým číslem, díky větě 3.2.5 by byl okruh $\mathbb{Z}\left[\frac{a}{b}\right]$ konečně generovaný $\mathbb{Z}$-modul s bází $\{a_1, \ldots, a_k\}$ obsahující racionální čísla a_i (můžeme předpokládat nenulová), která mají danou p-adickou valuaci. Násobení racionálního čísla celým nesníží jeho p-valuaci a $v_p(x + y) \geqslant \min(v_p(x), v_p(y))$, tedy p-valuace každého prvku $\mathbb{Z}\left[\frac{a}{b}\right]$ je rovna nejméně $\min(v_p(a_i))$. To je spor, neboť posloupnost čísel $\frac{a}{b}, \left(\frac{a}{b}\right)^2, \ldots, \left(\frac{a}{b}\right)^i, \cdots \in \mathbb{Z}\left[\frac{a}{b}\right]$ má klesající celé hodnoty p-valuace. □

Poznámka 3.2.7. Předchozí příklad je možno dokázat elementárněji za pomocí tvaru racionálních kořenů polynomů nad celočíselnými kořeny. Konkrétně, mějme $P \in \mathbb{Z}[x]$ polynom stupně n a $\frac{p}{q}$ jeho racionální kořen zapsán v ireducibilním tvaru. Pokud rovnici $P\left(\frac{p}{q}\right) = 0$ přenásobíme q^n, snadno získáme z nesoudělnosti p, q, že p dělí konstantní člen P a q dělí jeho člen vedoucí. Pokud je P monický, je nutně q rovno ± 1.

Důležitým faktem o celých algebraických číslech je, že v číselném tělese tvoří okruh, jak si dále ukážeme.

Věta 3.2.8. *Celá algebraická čísla číselného tělesa K tvoří okruh $\mathcal{O}_K$.*

Důkaz. Ukážeme, že součet a součin dvou algebraických čísel α a β je opět algebraické číslo. Mějme $\mathbb{Z}[\alpha]$ a $\mathbb{Z}[\beta]$ volné moduly a uvažme okruh $\mathbb{Z}[\alpha, \beta]$, jenž je množinou všech polynomů ve dvou proměnných nad celými čísly evaluovaných v bodě (α, β). Ten je abelovskou grupou a díky příkladu 3.1.6 i $\mathbb{Z}$-modulem.

V důkazu věty 3.2.5 jsme si ukázali, že pokud minimální polynom P_α má stupeň n, číslo α^k pro $k \geqslant n$ se dá vyjádřit jako $\mathbb{Z}$-lineární kombinace prvků α s mocninami ostře nižšími n. Víme, že $\mathbb{Z}[\alpha, \beta]$ je množinou $\mathbb{Z}$-lineárních kombinací čísel $\alpha^i \cdot \beta^j$, z čehož plyne, že $\mathbb{Z}[\alpha, \beta]$ je generovaný množinou $\{\alpha^i \beta^j | i \in \{0, 1, \ldots, n-1\}, j \in \{0, 1, \ldots, m-1\}\}$, kde minimální polynom β, P_β, má stupeň m. Okruh $\mathbb{Z}[\alpha, \beta]$ je proto volným $\mathbb{Z}$-modulem ranku mn.

Okruhy $\mathbb{Z}[\alpha + \beta]$ a $\mathbb{Z}[\alpha\beta]$ jsou díky jejich komutativitě $\mathbb{Z}$-moduly a navíc jsou oba zjevně podmoduly $\mathbb{Z}[\alpha, \beta]$. Díky větě 3.1.9 jsou oba volnými $\mathbb{Z}$-moduly (ranku nejvýše mn), tedy $\alpha + \beta$ a $\alpha\beta$ jsou celá algebraická čísla. Speciálně pro libovolné α celé algebraické je $-\alpha$ celé algebraické. Množina $\mathcal{O}_K$ celých algebraických čísel tělesa K proto tvoří okruh. □

Dle příkladu 3.2.6 je okruhem celých algebraických čísel tělesa $\mathbb{Q}$ množina celých čísel.

V kvadratickém tělese dokážeme $\mathcal{O}_K$ za pomocí znalosti řešení kvadratické rovnice popsat.

Věta 3.2.9. *Nechť $m \neq 0, 1$ je bezčtvercové celé číslo a $K = \mathbb{Q}(\sqrt{m})$ je algebraické číselné těleso. Pak platí:*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}], & \text{pokud} \quad m \equiv 2, 3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right], & \text{pokud} \quad m \equiv 1 \pmod 4. \end{cases}$$

Důkaz. Jistě $\mathbb{Z} \subseteq \mathcal{O}_K$. Dále $\mathbb{Z}[\sqrt{m}]$, resp. $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$, je podmnožinou $\mathcal{O}_K$, neboť minimální polynomy prvků $a + b\sqrt{m}$, resp. $a + b\frac{1+\sqrt{m}}{2}$, jsou po řadě $(x-a)^2 - bm^2$, resp. $(x-a)^2 - bx + ab + b^2\frac{1-m}{4}$.

Ze tvaru řešení kvadratické rovnice plyne, že prvky $\mathcal{O}_K$ jsou ve tvaru $\frac{a+b\sqrt{m}}{2}$ pro $a, b \in \mathbb{Z}$. Zjevně pro $b \neq 0$ sdílí $\frac{a+b\sqrt{m}}{2}$ a $\frac{a-b\sqrt{m}}{2}$ minimální polynom, musí nutně být:

$$\left(x - \frac{a + b\sqrt{m}}{2}\right)\left(x - \frac{a - b\sqrt{m}}{2}\right) = x^2 - ax + \frac{a^2 - b^2 m}{4}.$$

Pokud $\frac{a+b\sqrt{m}}{2} \in \mathcal{O}_K$, je tento monický polynom nutně nad celými čísly. Proto $a^2 - b^2 m$ je dělitelné čtyřmi. Je-li m je sudé, je a též, tedy a^2 je dělitelné čtyřmi. Za předpokladu, že m je bezčtvercové, je $m \equiv 2 \pmod 4$, tedy i b je sudé.

Nyní již předpokládejme, že m je liché. Pokud je $m \equiv 3 \pmod 4$, je $a^2 + b^2 \equiv 0 \pmod 4$, což nutně znamená $2 \mid a, b$, protože kvadráty dávají zbytky $0, 1$ po dělení čtyřmi. Pak $\frac{a+b\sqrt{m}}{2} \in \mathbb{Z}[\sqrt{m}]$. Konečně uvažme $m \equiv 1 \pmod 4$. Máme $a^2 \equiv b^2 \pmod 4$, tedy $a \equiv b \pmod 2$. To ale znamená, že $\frac{a+b\sqrt{m}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. □

Dále budeme studovat speciální okruhy číselného tělesa, které mají rank shodný se stupněm tělesa.

Definice 3.2.10. Okruh $\mathcal{O}$ v číselném tělese K nazveme *pořádkem*, pokud je $\mathcal{O}$ volným $\mathbb{Z}$-modulem ranku $[K : \mathbb{Q}]$.

Nejprve si všimněme, že $\mathcal{O}_K$ je pořádkem K. Dalším příkladem pořádku je okruh $\mathbb{Z}[3i]$ v $\mathbb{Q}(i)$, který není okruhem Gaussových celých čísel, nicméně je v něm obsažen.

Věta 3.2.11. *Nechť K je číselné těleso stupně n a $\mathcal{O}$ jeho pořádek. Pak $\mathcal{O} \subseteq \mathcal{O}_K$.*

Důkaz. Buď $\{a_1, \ldots, a_n\}$ báze $\mathcal{O}$ nad $\mathbb{Z}$. Protože $\mathcal{O} = \mathbb{Z}[a_1, \ldots, a_n]$ je volný modul a $\mathbb{Z}[a_i]$ jsou jeho podmoduly, podle věty 3.1.9 jsou všechny volné. Díky větě 3.2.5 jsou a_i celá algebraická čísla, tedy $a_i \in \mathcal{O}_K$. Protože $\mathbb{Z} \subseteq \mathcal{O}_K$, leží každá $\mathbb{Z}$-lineární kombinace a_i v $\mathcal{O}_K$, jinak řečeno $\mathcal{O} \subseteq \mathcal{O}_K$. □

O $\mathcal{O}_K$ tak můžeme hovořit jako o „maximálním“ pořádku.

3.3 Ideály

Připomeňme si pár základních faktů ohledně okruhu R.

Definice 3.3.1. Neprázdnou aditivní podgrupu $\mathcal{I}$ okruhu R takovou, že $a \cdot r \in \mathcal{I}$, resp. $r \cdot a \in \mathcal{I}$ pro $a \in \mathcal{I}, r \in R$ označíme jako *pravý*, resp. *levý ideál*. Ideál, který je pravý i levý nazveme *oboustranným*.

O (levém) ideálu tak můžeme přemýšlet jako o (levém) R-modulu.

V případě, že pracujeme nad komutativním okruhem R, pravé a levé ideály nerozlišujeme. Oboustranné ideály R budeme nazývat jednoduše ideály.

Definice 3.3.2. Pokud $\theta_1, \ldots, \theta_k \in R$ jsou generátory ideálu (ve smyslu R-modulu) $\mathcal{I}$, značíme:

$$\mathcal{I} = (\theta_1, \ldots, \theta_k).$$

Příklad 3.3.3. Ukažme, že každý ideál eukleidovského okruhu R je generovaný jediným prvkem.

Řešení. Pokud je d v absolutní hodnotě nejmenším nenulovým prvkem $\mathcal{I}$, ukážeme, že $\mathcal{I}$ je generovaný d. Dle Bezoutova lemmatu každý jiný prvek $a \in \mathcal{I}$ splňuje $a = b|d| + r$ pro $b \in R, r \in \mathcal{I}$, tedy $r = 0$. Každý prvek ideálů je tak dělitelný d, přičemž každý násobek d v ideálu leží, $\mathcal{I}$ je tedy generovaný d. □

Okruhy $\mathbb{Z}$ a $\mathbb{Z}[i]$ jsou eukleidovské, z čehož plyne, že každý jejich ideál je generovaný jediným prvkem, ideály celých čísel jsou tak speciálně právě násobky celých čísel.

Definice 3.3.4. Ideály generované jediným prvkem označíme jako *hlavní*.

Hlavní ideál generovaný prvkem $\alpha \in R$, tedy množinu αR, pak značíme (α). Pojďme si dále definovat sčítání a násobení ideálů.

Definice 3.3.5. Buďte $\mathcal{I}, \mathcal{J}$ ideály okruhu R. Pak jejich součet a součin definujeme následovně:

- $\mathcal{I} + \mathcal{J} = \{a + b | a \in \mathcal{I}, b \in \mathcal{J}\}$,
- $\mathcal{I} \cdot \mathcal{J} = \{\sum_{i=1}^{n} a_i b_i |\, a_i \in \mathcal{I}, b_i \in \mathcal{J}, n \in \mathbb{N}\}$.

Vidíme, že jak součet, tak součin dvou ideálů je též ideálem. Sčítání je jistě asociativní a jeho neutrální prvek je nulový ideál $(0) = \{0\}$. Násobení ideálů je taktéž asociativní, neboť:

$$(\mathcal{I} \cdot \mathcal{J}) \cdot \mathcal{K} = \left\{ \sum_{i=1}^{n} a_i b_i c_i \,\middle|\, a_i \in \mathcal{I}, b_i \in \mathcal{J}, c_i \in \mathcal{K}, n \in \mathbb{N} \right\} = \mathcal{I} \cdot (\mathcal{J} \cdot \mathcal{K}),$$

a neutrální prvek je vždy celý okruh R. Ideály okruhu R proto tvoří se sčítáním a násobením monoid.

Definice 3.3.6. Buď K podílové těleso okruhu R. Pokud $\mathcal{J} = m\mathcal{I}$ je ideál R pro $m \in R$, nazveme $\mathcal{I}$ lomeným ideálem K. Budeme značit $\mathcal{I} = \frac{\mathcal{J}}{m}$.

Definice 3.3.7. Buď K podílové těleso R. Pro $\alpha \in K$ nazveme $(\alpha) = \alpha K$ *hlavním lomeným ideálem* R.

Příkladem hlavního lomeného ideálu okruhu celých čísel tělesa $\mathbb{Q}$ je $\frac{(3)}{2} = \frac{3}{2}\mathbb{Z}$.

Definice 3.3.8. Nechť je $\mathcal{I}$ nenulový lomený ideál okruhu R. Pak normou ideálu $N(\mathcal{I})$ rozumíme počet prvků faktorokruhu $R/\mathcal{I}$. Definujeme $N((0)) = 0$.

3.4 Grupa tříd ideálů

Mějme $\mathcal{I}, \mathcal{J}$ ideály pořádku $\mathcal{O}$. Definujme relaci *ekvivalence* $\sim$ s tím, že $\mathcal{I}, \mathcal{J}$ jsou ekvivalentní, pokud existují $a, b \in \mathcal{O}$ taková, že $\mathcal{I} \cdot (a) = \mathcal{J} \cdot (b)$. Relace $\sim$ pak dělí ideály $\mathcal{O}$ na třídy ekvivalence $[\mathcal{I}]$. Násobení ideálu hlavní ideálem nezmění jeho třídu. Snadno nahlédneme, že součin libovolné dvojice ideálů z dané dvojice tříd vždy spadá do stejné třídy, neboli $[\mathcal{I}] \cdot [\mathcal{J}] = [\mathcal{I} \cdot \mathcal{J}]$. Tyto třídy ekvivalence z asociativity násobení ideálů proto tvoří grupu.

Definice 3.4.1. Buď $\mathcal{O}$ pořádek číselného tělesa K. Označme $\mathsf{G}(\mathcal{O})$ množinu všech lomených ideálů $\mathcal{O}$ a množinu hlavních lomených ideálů $\mathsf{H}(\mathcal{O})$. *Grupu tříd ideálů* $\mathcal{O}$ definujeme jako faktorgrupu $Cl(\mathcal{O}) = \mathsf{G}(\mathcal{O})/\mathsf{H}(\mathcal{O})$.

Z předchozí diskuze plyne, že neutrálním prvkem grupy $Cl(\mathcal{O})$ je právě množina hlavních ideálů $\mathcal{O}$.

Kapitola 4

Okruhy Endomorfismů

Vraťme se k eliptickým křivkám. Jak napovídá název této sekce, endomorfismy na křivce E tvoří okruh. Tento okruh se budeme snažit s pomocí teorie představené v předchozích kapitolách charakterizovat.

Definice 4.0.1. Označme $\mathrm{End}(E)$ množinu isogenií $E \longrightarrow E$ na E spolu s $[0]$. Prvky $\mathrm{End}(E)$ nazvěme *endomorfismy* na E.

Věta 4.0.2. *Množina* $\mathrm{End}(E)$ *tvoří okruh s operacemi* $+$ *a* $\circ$.

Důkaz. Sčítání endomorfismů na E je komutativní i asociativní, přičemž $[0]$ je neutrálním prvkem pro sčítání. Ke každé isogenii ϕ je isogenie $[-1] \circ \phi$ opačnou k ϕ vzhledem ke sčítání. Dále skládání isogenií je asociativní a $[1]$ je jeho neutrálním prvkem. Konečně, skládání je na sčítání oboustranně distributivní, protože isogenie na E jsou homomorfismy $E(\overline{K}) \longrightarrow E(\overline{K})$. □

Definice 4.0.3. $\mathrm{End}(E)$ nazveme *okruhem endomorfismů* E. Též místo $\phi \circ \psi$ budeme jednoduše psát $\phi\psi$.

Protože platí $[m] + [n] = [m + n]$ a $[m][n] = [mn]$, je okruh n-násobků, tedy isogenií $[n]$ pro $n \in \mathbb{Z}$, isomorfní okruhu celých čísel. Můžeme proto indentifikovat $[m]$ s m a říci, že $\mathbb{Z} \subseteq \mathrm{End}(E)$.

Věta 4.0.4. *Okruh* $\mathrm{End}(E)$ *je oborem integrity.*

Důkaz. Rovnost $\phi\psi = 0$ znamená i rovnost stupňů obou stran, tedy $\deg\phi \cdot \deg\psi = 0$, jedna z našich isogenií je proto 0. □

Speciálně pro $\phi = m \neq 0$ získáváme:

Důsledek 4.0.5. *Okruh* $\mathrm{End}(E)$ *má nulovou charakteristiku.*

Definice 4.0.6. V okruhu endomorfismů definujme $\phi^m = \underbrace{\phi\phi\cdots\phi}_{m}$.

4.1 Frobeniův endomorfismus

Tvar Hasseho věty 1.1.5 připomíná diskriminant kvadratické rovnice. Vskutku, dá se ukázat, že v $\mathrm{End}(E)$ splňuje Frobeniův endomorfismus kvadratický vztah.

Věta 4.1.1. *Frobeinův endomorfismus π na křivce E nad $\mathbb{F}_q$ v $\mathrm{End}(E)$ splňuje:*

$$\pi^2 - t\pi + q = 0$$

pro nějaké $t \in \mathbb{Z}$, které nazveme stopou Frobenia.

4.2 Obyčejné křivky

4.3 Supersingulární křivky

Konečně se obraťme zpět k supersingulárním křivkám. Víme, že stopa Frobenia je nulová, tedy $\pi^2 = -p$ v $\mathrm{End}(E)$. To znamená, že $\mathbb{Z}[\sqrt{-p}] \subseteq \mathrm{End}(E)$.

Závěr

zu ende

Literatura

[1] Chuang, Isaac L. a Nielsen, Michael A.: *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[2] Costello, Craig: *Supersingular isogeny key exchangefor beginners*. Microsoft Research, USA, 2019. Dostupné z: https://eprint.iacr.org/2019/1321.

[3] Couveignes, Jean-Marc: *Hard Homogenous Spaces*. 2006. Dostupné z: https://eprint.iacr.org/2006/291.pdf.

[4] De Feo, Luca: *Fast Algorithms for Towers of Finite Fields and Isogenies*. EcolePolytechnique X, 2010.

[5] De Feo, Luca.: *Mathematics of Isogeny Based Cryptography*. Université de Versailles & Inria Saclay, 2017. Dostupné z: https://arxiv.org/abs/1711.04062.

[6] De Feo, Luca, Jao, David a Plût, Jérôme.: *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*. Math. Cryptol. 8(3): 209-247, 2014. Dostupné z: https://eprint.iacr.org/2011/506.pdf.

[7] Diffie, Whitfield a Hellman, Martin: *New Directions in Cryptography*. IEEE Transactions on Information Theory 22, 1976.

[8] Galbraith, Steven D.: *Constructing Isogenies Between Elliptic Curves Over Finite Fields*. LMS J. Comput. Math., 199, 118-138. Dostupné z: https://www.math.auckland.ac.nz/~sgal018/iso.pdf.

[9] Kuřil, Martin: *Základy teorie grup*.

[10] Leonardi, Christopher. *A Note on the Ending Elliptic Curve in SIDH*. 2020. Dostupné z: https://eprint.iacr.org/2020/262.

[11] Marcus, Daniel A.: *Number fields*. New York: Springer-Verlag, 1977.

[12] Matushak, Andy a Nielsen, Michael A.: *Quantum computing for the very curious*. San Francisco, 2019. Dostupné z: https://quantum.country/qcvc.

[13] Mordell, Luis J.: *On the rational solutions of the indeterminate equations of the third and fourth degrees*. Cambridge, 1922.

[14] Perutka, Tomáš: *Vyjadřování prvočísel kvadratickými formami.* Středoškolská odborná činnost. Brno: Masarykova univerzita, 2017.

[15] Perutka, Tomáš: *Užití dekompoziční grupy k důkazu zákona kvadratické reciprocity.* Středoškolská odborná činnost. Brno: Masarykova univerzita, 2018.

[16] Pezlar, Zdeněk: *Zajímavá využití algebraické teorie čísel.* Středoškolská odborná činnost. Brno: Masarykova univerzita, 2020.

[17] PUPÍK, Petr. *Užití grupy tříd ideálů při řešení některých diofantických rovnic.* Brno, 2009. Dostupné z: https://is.muni.cz/th/v8xsj/. Diplomová práce. Masarykova univerzita, Přírodovědecká fakulta. Vedoucí práce Radan Kučera.

[18] Raclavský, Marek: *Racionální body na eliptických křivkách.* Diplomová práce. Praha, 2014.

[19] Rivest, Ronald L., Shamir, Adi a Adleman, Leonard M.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. 1977. Dostupné z: https://people.csail.mit.edu/rivest/Rsapaper.pdf.

[20] Rosický, Jiří: *Algebra.* Brno: Masarykova univerzita, 2002.

[21] Rostovtsev, Alexander a Stolbnov, Anton: Public-key cryptosystem based on isogenies. 2006. Dostupné z: http://eprint.iacr.org/2006/145/.

[22] Silverman, Joseph H.: *The Arithmetic of Elliptic Curves.* New York: Springer-Verlag, 1992.

[23] Schoof, René: *Elliptic Curves Over Finite Fields and the Computation of Square Roots* mod p. J. Théor. Nombres Bordeaux 7 Dostupné z: https://www.ams.org/journals/mcom/1985-44-170/S0025-5718-1985-0777280-6/S0025-5718-1985-0777280-6.pdf.

[24] Shor, Peter W.: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* New York: Springer-Verlag, 1994. Dostupné z: https://arxiv.org/abs/quant-ph/9508027.

[25] Stein, William: *A Brief Introduction to Classical and Adelic Algebraic Number Theory.* 2004. Dostupné z: https://wstein.org/papers/ant/html/node93.html.

[26] SUCHÁNEK, Vojtěch. *Vulkány isogenií v kryptografii.* Brno, 2020. Available from: https://is.muni.cz/th/pxawb/. Master's thesis. Masaryk University, Faculty of Science. Thesis supervisor Marek Sýs.

[27] Sutherland, Andrew V.: *Elliptic Curves.* Massachusetts Institute of Technology, 2017. Dostupné z: https://math.mit.edu/classes/18.783/2017/lectures.html.

[28] Vélu, Jacques: *Isogénies entre courbes elliptiques*. Comptes Rendus de l'Académie des Sci-ences de Paris, 1971. Dostupné z: https://math.mit.edu/classes/18.783/2017/lectures.html.

[29] Washington, Lawrence C.: *Elliptic Curves: Number theory and cryptography*. Maryland, 2008.

[30] Weil, André: *L'arithmétique sur les courbes algébriques*. Acta Mathematica 52, 1929.