STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Isogenie v kryptografii

Zdeněk Pezlar
Jihomoravský kraj

Brno 2020

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: ....

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
$\mathcal{D}(a,b)$	největší společný dělitel a,b
$a \sim b$	a je asociované s b
$\overline{a+b\sqrt{m}}$	konjugát $a+b\sqrt{m}$, neboli $a-b\sqrt{m}$
$\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$	množina přirozených, celých, racionálních, reálných, komplexních čísel
$\mathbb{Z}_d$	okruh zbytků modulo d
$R[x]$	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, t.j. dimenze vektorového prostoru $K:L$
$\mathcal{O}_K$	okruh celých algebraických čísel tělesa K
$Cl(\mathcal{O}_K)$	grupa tříd ideálů tělesa K
h_K	řád grupy tříd ideálů tělesa K
$\mathcal{U}(\mathcal{O}_K)$	grupa jednotek tělesa K
(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
$\mathcal{I} \mid \mathcal{J}$	ideál $\mathcal{I}$ dělí ideál $\mathcal{J}$
P_α	minimální polynom α nad K
G/H	faktorgrupa G podle H

Kapitola 1

Isogenie

1.1 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 (to zjistím, až to napíšu). Budeme postupovat vesměs dle ??, nicméně další vhodný úvodní materiál se nachází na ??.

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, 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. *Projektivní prostor $\mathbb{P}^n(\overline{K})$ definujeme jako množinu nenulových vektorů $(a_0, \dots, a_n) \in \overline{K}^{n+1}$ s ekvivalentní relací $(a_0, \dots, a_n) \sim (b_0, \dots, b_n)$, pokud existuje nenulové λ, že $(a_0, \dots, a_n) = \lambda(b_0, \dots, b_n)$. Tyto třídy ekvivalence budeme značit $(a_0 : \dots : a_n)$.*

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

Projektivní prostor $\mathbb{P}^2(\mathbb{R})$ je ????

Poznámka 1.1.2. *Je zajímavé uvážit spojitost 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 tedy o barycentrických souřadnicích přemýšlet jako o projektivním prostoru s jiným základem.*

?????? Přípomeňme si pak definici eliptické křivky:

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

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

Čtenář, jenž je již obeznámen s eliptickými křivkami, může protestovat, že eliptická křivka je množina bodů $x, y \in K$ splňující:

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

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

Podívejme se nyní na eliptickou křivku E geometricky. Je zjevné, že má graf symetrický podle osy x, definujme proto k $P \in E$ 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 právě $\mathcal{O}$.

OBrázky

Pokud řekneme, že tečna k E ji protíná ve dvou stejných bodech, pak každá přímka protíná E v právě třech bodech včetně multiplikativity. Speciálně tečna v bodě $y = 0$ tento bod protíná dvakrát a ten třetí je právě bod v nekonečnu E. Pak si sčítání $+$ 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 takto definovaný součet můžeme pro $P, Q \in E$ 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 sčítání můžeme s body na E pracovat jako s grupou. Samozřejmě součet dvou bodů dokážeme za pomocí analytické geometrie přímo spočíst:

Věta 1.1.4.

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

Definice 1.1.5. *Mějme bod $P \in E$. Pak pro n přirozené definujeme n-násobek:*

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

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

tu příklad, jak v Q tak v Z[n], hezky graficky

Všimneme si, že pro P s $y = 0$ je $[2]P = \mathcal{O}$. Na příkladu ?? též ale vidíme, že trojnásobek bodu ??? dává též $\mathcal{O}$. Obecně by nás mohlo zajímat, které body pošle násobení n do nekonečna.

Definice 1.1.6. *Buď n celé číslo. O množině všech $P \in E$, že $[n]P = \mathcal{O}$, řekneme, že tvoří n-torzi E a budeme ji značit $E[n]$.*

-¿ jak se chová E[n] ?

Multiplikace n patří mezi endomorfismy $E \mapsto E$. Se sčítáním endomorfismů $\phi, \psi : E \mapsto E, P \in E$:

$$(\phi + \psi)(P) := \phi(P) + \psi(P)$$

a skládáním $\psi \circ \phi = \phi(\psi)$, spolu s nulovou mapou $0 : P \mapsto \mathcal{O}$ tvoří endomorfismy E okruh, který budeme značit $End(E)$. ??

Mohly by nás nicméně též zajímat morfismy mezi dvěma různými eliptickými křivkami a jejich vlastnosti. Pokud je tato mapa dána racionální funkcí a má konečné jádro, což je množina bodů, které se zobrazí do nekonečna, nazveme ji *isogenií*. Jako stupeň isogenie pak bereme stupeň této racionální funkce.

1.2 Vlastnosti ??

Zde vlastnosti isogenií, jako existence duálu etc., v této či další už se dobrat s SIDH.

Kapitola 2

SIDH

Přes Caesarovu šifru po šifrování za pomocí Enigmy v období druhé světové války, po většinu lidské historie se užívaly kryptografické systémy založené na faktu, že obě komunikující partie si po domluvě vybraly způsob zamaskování zprávy a pro ostatní je skrytý. Například právě o kolik písmen v Caesarově šifře transponujeme. Tento způsob nutně závisí na faktu, že obě strany komunikují přes bezpečný kanál. S přibývajícím počtem účastníků a frekvencí komunikace, na příklad našeho každodenního interagování na internetu, je třeba vyšší počet klíčů a příbývá risk kompromitace.

Kvůli takovým obavám přišli *Whitfield Diffie* a *Martin Hellman* v roce 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 veřejného klíče tajně transformují svůj privátní klíč a výsledek publikují. Oba účastnící vezmou veřejný klíč toho druhého a provedou s ním ty samé tajné kroky závisící na jejich privátním kíčí. Podstatou takové výměny je, že na jejím konci získají obě původní strany netriviální informaci, t.j. 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. Nemůže tak útočník v rozumném čase všechny možná sdílená tajemství projít.

Pojďme se podívat na právě protokol, který Diffie a Hellman navrhli. Budeme o něm dále mluvit jako o *Diffie-Hellmanově výměně*. Je založen na problému *diskrétníhp logaritmu* prvku $a \in \mathbb{Z}_p \setminus \{0\}$. Tento prolém po nás ze znalosti primitivního kořene g modulo p žádá najít k, že $g^k = a$ v $\mathbb{Z}_p$.

-¿ tu nějak hezky typeset algoritmus

Závěr

zu ende

Literatura

[1] BENEŠ, Petr: *Zákony Reciprocity.* Diplomová práce. Brno: Masarykova univerzita, 2010.

[2] DECHENNE, Spencer. The Ramanujan-Nagell Theorem: Understanding the Proof. Dostupné z: http://buzzard.ups.edu/courses/2013spring/projects/spencer-ant-ups-434-2013.pdf

[3] DOLEŽÁLEK, Matěj. Pellova rovnice a kvadratické okruhy. In: PraSe, Organizátoři. PraSe Sborníček 2019 [online]. Sklené, 2019. Dostupné z: `https://prase.cz/soustredeni/sbornik.php?sous=47`.

[4] HRNČIAR, Maroš: *Řešení diofantických rovnic rozkladem v číselných tělesech.* Diplomová práce. Praha: 2015.

[5] HUDEC, Pavel. Odmocniny z jedničky. In: *i*KS, Organizátoři. *i*KS Sborníček 2019 [online]. Kunžak, 2019. Dostupné z: `http://iksko.org/files/sbornik8.pdf`.

[6] KUŘIL, Martin: *Základy teorie grup.*

[7] LENSTRA JR, Hendrik W.: *Solving the Pell Equation.* 2002.

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

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

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

[11] PUPÍK, Petr: *Užití grupy tříd ideálů při řešení některých diofantických rovnic.* Diplomová práce. Brno: Masarykova univerzita, 2009.

[12] RACLAVSKÝ, Marek. *Racionální body na eliptických křivkách.* Diplomová práce. Praha, 2014.

[13] ROSICKÝ, Jiří: *Algebra.* Brno: Masarykova univerzita, 2002.

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

[15] *i*KS - mezinárodní korespondenční seminář [online]. Dostupné z: `iksko.org`.