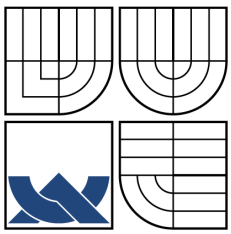


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV MATEMATIKY
FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF MATHEMATICS

TRANSFER ELIPTICKÝCH KŘIVEK NA TORUS

THE TRANSFER OF ELLIPTIC CURVES ONTO THE TORUS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
JAROSLAV BAJKO

VEDOUCÍ PRÁCE
SUPERVISOR
Doc. RNDr. MIROSLAV KUREŠ, Ph.D.

BRNO 2011

Abstrakt

Eliptické křivky jsou nedílnou součástí novodobé matematiky a nacházejí uplatnění zejména v kryptografii. Práce se věnuje vizualizaci eliptických křivek a grupové operace nad nimi v reálné rovině a následně na toru. V úvodní části se proto zaměříme na analýzu eliptických křivek nad polem reálných čísel a především nad poli prvočíselnými. Důraz je kladen na grafické znázornění probírané problematiky, stejně také na experimentální výsledky v oblasti diskrétních eliptických křivek. Předmětem zájmu v další části práce je topologie, průzkum zobrazení mezi topologickými prostory a následné zavedení pojmu hladké variety. Odvodíme vhodná zobrazení, která umožňují přenos geometrických objektů z reálné roviny na torus. Na základě zmíněných zobrazení pracuje software vyvinutý speciálně pro účely vizualizace eliptických křivek na toru.

Abstract

Elliptic curves are an essential part of modern mathematics and play an important role especially in cryptography. The bachelor work focuses on the visualization elliptic curves and group operation in real plane and torus. In the first chapter we will introduce elliptic curves over field of real numbers and above all over prime fields. In order to describe the problematics rigorously the graphical outputs and also the experimental results in the field of discrete elliptic curves will be mentioned. In the next section we will pay a particular attention to topology, functions between topological spaces and to the introduction of the concept of smooth manifold. We will search the suitable functions which can transfer geometrical objects from the real plane onto torus. A software specifically developed for transfering the elliptic curves onto the torus works on the basis of aforementioned functions.

klíčová slova

eliptická křivka, vizualizace, hladká varieta, torus

key words

elliptic curve, visualization, smooth manifold, torus

BAJKO, J.: *Transfer eliptických křivek na torus* , Brno, Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2011 (53 stran). Vedoucí bakalářské práce doc. RNDr. Miroslav Kureš, Ph.D.

Prohlašuji, že jsem bakalářskou práci *Transfer eliptických křivek na torus* zpracoval samostatně dle pokynů vedoucího bakalářské práce doc. RNDr. Miroslava Kureše, Ph.D. a s využitím uvedené literatury.

Jaroslav Bajko

Děkuji svému školiteli doc. RNDr. Miroslavu Kurešovi, Ph.D. za cenné rady a otevření nových obzorů při vedení mé bakalářské práce.

Jaroslav Bajko

Obsah

1 Úvod a metodika bakalářské práce

Úvodem bych se rád zmínil o motivacích a nápadech, které vedly ke vzniku práce s názvem Transfer eliptických křivek na torus. V první řadě stojí zájem o eliptické křivky, které jsou nejen hojně využívány v kryptosystémech, ale i důležitou součástí matematické teorie. Velká Fermátova věta dlouho odolávala pokusům o její důkaz. Až v roce 1994 přišel Andrew Wiles s velmi rozsáhlým důkazem, ve kterém využívá právě eliptické křivky. V rámci důkazu se mu podařilo dokázat Tanijamovu-Šimurovu-Weilovu domněnku[1], která ztotožňuje eliptické křivky a modulární formy.

Zaměříme se však na popsání eliptických křivek jak z hlediska geometrie, teorie grup, tak také uvedeme některé kryptografické souvislosti. Během zpracování eliptických křivek nad konečnými poli vzniká potřeba zavést nový, obecnější pojem semi-eliptické[2] křivky především z důvodů vizualizace a přesnějšího vyjadřování.

Za účelem prozkoumání množiny všech semi-eliptických křivek $\mathcal{M}(\mathbb{F}_p)$ vzniká program `ElCOFF`, který umožňuje znázorňení jednotlivých semi-eliptických křivek nad prvočíselnými poli $\mathbb{F}_p$, analýzu $\mathcal{M}(\mathbb{F}_p)$ nad $\mathbb{F}_p$ a další. Z experimentálních výsledků vzniká několik vět (4.1), (4.2), nejzajímavější je však hypotéza (4.1) o symetrii semi-eliptických křivek.

Značná část práce je věnována geometrii a topologii. Postupně rozvineme teorii topologických prostorů, včetně definice homeomorfismu a vlastností takového zobrazení. Pokračujeme teorií homotopií, neboli studia deformací oblouků v topologických prostorech a odvodíme pojem fundamentální grupy. Důležitou vlastností některých topologických prostorů je lokální podobnost s prostorem $\mathbb{R}^n$. Uvedeme přesnou formulaci této vlastnosti, čímž dostáváme pojem topologické variety (5.14). V této fázi odvozování již nechybí mnoho k pojmu hladké variety (5.18), kterými kapitola vrcholí. Příkladem dvourozměrné hladké variety je právě torus $\mathcal{T}$, jehož studiu se budeme nadále věnovat.

Motivaci pro vizualizaci eliptických křivek na toru nacházíme v konečných polích a modulární aritmetice, jež je snadno znázornitelná na kružnici. Uvažujeme-li bod eliptické křivky jako dvojici (x, y), kde x, y probíhají konečné pole, přirozeně tak získáváme možnost znázornit x na jedné kružnici a y na příslušné druhé kružnici. Topologicky kartézský součin 2 kružnic odpovídá toru, viz definice (5.19).

V další části práce se zaměříme na hledání vhodných zobrazení reálné roviny na torus, díky kterým můžeme provést transfer semi-eliptických křivek na torus. Rozlišíme zobrazení neomezené reálné roviny $\mathbb{R}^2$ a zobrazení omezené části reálné roviny na torus. Pro přenos semi-eliptických křivek definovaných nad $\mathbb{F}_p$ uvedeme definici diskrétního toru $\mathcal{DT}$ a souvislost s daným diskrétním zobrazením.

Pozornost bude věnována také dokumentaci programů `TrElC` a `ElCOFF`, z nichž první se obecně věnuje analýze semi-eliptických křivek nad polem reálných čísel $\mathbb{R}$ a druhý analýze opět semi-eliptických křivek, avšak nad prvočíslenými poli $\mathbb{F}_p$. Veškeré obrázky týkající se semi-eliptických křivek jsou pořízeny právě pomocí uvedeného softwaru.

[1] Také jinak Teorém modularity.

[2] Množina všech semi-eliptických křivek $\mathcal{M}(\mathbb{F}_p)$ obsahuje křivky jak eliptické, tak neeliptické. Nezáleží tedy na diskriminantu příslušných křivek.

2 Algebraický podtext

2.1 Základy teorie grup

Definice 2.1. Neprázdnou množinu $\mathcal{G}$ s binární operací $* : \mathcal{G} \times \mathcal{G} \to \mathcal{G}$, tj. dvojici $(\mathcal{G}, *)$, nazýváme *grupa*, jestliže jsou splněny následující axiomy

($\mathcal{G}1$) Pro $a, b, c \in \mathcal{G}$ platí

$$a * (b * c) = (a * b) * c \qquad \text{(asociativní zákon)}.$$

($\mathcal{G}2$) Existuje prvek $e \in \mathcal{G}$ takový, že pro každý prvek $g \in \mathcal{G}$ platí

$$g * e = e * g = g \qquad \text{(existence neutrálního prvku)}.$$

($\mathcal{G}3$) Pro každý prvek $g \in \mathcal{G}$ existuje takový prvek $g^{-1} \in \mathcal{G}$, že platí

$$g * g^{-1} = g^{-1} * g = e \qquad \text{(existence inverzního prvku)}.$$

Jestliže za operaci $*$ volíme sčítání $+$ (resp. násobení $\cdot$), mluvíme o aditivním (multiplikativním) označení operace grupy a píšeme $(\mathcal{G}, +)$ ($(\mathcal{G}, \cdot)$). V případech, kdy je zřejmé o jakou operaci se jedná nebo při multiplikativním označení, budeme grupu $(\mathcal{G}, *)$ značit jen $\mathcal{G}$. Při multiplikativním označení operace $x \cdot y$ využijeme stručnější xy. Neutrální prvek e se při aditivním zápisu nazývá *nula* a označujeme jej $0_{\mathcal{G}}$. Při multiplikativním zápisu se nazývá *jednička* a značíme jej $1_{\mathcal{G}}$. Inverzní prvek při aditivním zápisu označujeme $-g$ a mluvíme o *opačném prvku*.

Definice 2.2. Nechť $(\mathcal{G}, *)$ je grupa a $\mathcal{G}$ konečná množina. Pak se číslo $\texttt{card}(\mathcal{G})$ nazývá *řád grupy* $\mathcal{G}$. Jestliže $\mathcal{G}$ je nekonečná množina, říkáme, že grupa $\mathcal{G}$ má *nekonečný řád*.

Jestliže pro každé x, y grupy $\mathcal{G}$ platí $xy = yx$ (komutativní zákon), nazýváme grupu $\mathcal{G}$ *komutativní* nebo *abelovskou*.

Příklad 2.1. Příklady komutativních grup nekonečného řádu jsou číselné množiny s operací součtu $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$. Označme $\mathbb{Q}^*$ množinu $\mathbb{Q} \setminus \{0\}$ a podobně pro další číselné množiny. Potom $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ tvoří komutativní grupu. Nulu vypouštíme, jelikož nemá inverzní prvek při operaci součinu.

Příkladem grupy konečného řádu je grupa $(\mathbb{Z}_n, +)$ zbytkových tříd modulo $n \in \mathbb{N}$ s operací součtu v modulární aritmetice. Grupu obsahující jediný prvek nazýváme *triviální*. Pro $n = 1$ dostáváme triviální grupu $(\mathbb{Z}_1, +) = (\{0\}, +)$.

Uvažujeme-li množinu zbytkových tříd modulo p s operací součinu, kde p je prvočíslo, potom $(\mathbb{Z}_p^*, \cdot)$ tvoří strukturu komutativní grupy.

Definice 2.3. Nechť $(\mathcal{G}, *)$ je grupa. Neprázdnou podmnožinu $\mathcal{H} \subseteq \mathcal{G}$ nazýváme *podgrupa* grupy $(\mathcal{G}, *)$, jestliže prvky z $\mathcal{H}$ tvoří vzhledem k operaci $*$ opět grupu.

Více o vlastnostech grup a podgrup např. ve skriptu [7].

2.2 Faktorové grupy

Definice 2.4. Nechť $(\mathcal{H}, \cdot)$ je podgrupa grupy $\mathcal{G}$ a $g \in \mathcal{G}$. *Levá třída $g\mathcal{H}$ podgrupy $\mathcal{H}$ vzhledem k prvku g grupy $\mathcal{G}$* je definována následovně

$$g\mathcal{H} = \{g \cdot h;\ h \in \mathcal{H}\}\,.$$

Pravá třída $\mathcal{H}g$ podgrupy $\mathcal{H}$ vzhledem k prvku g grupy $\mathcal{G}$ je definována

$$\mathcal{H}g = \{h \cdot g;\ h \in \mathcal{H}\}\,.$$

Řekneme, že podgrupa $\mathcal{H}$ grupy $\mathcal{G}$ je *normální*, právě když systém všech levých tříd $\{g\mathcal{H};\ g \in \mathcal{G}\}$ splývá se systémem všech pravých tříd $\{\mathcal{H}g;\ g \in \mathcal{G}\}$. Tato situace nastává vždy pro komutativní grupu $\mathcal{G}$. Ekvivalentní definice normální podgrupy viz [11].

Definice 2.5. Nechť $\mathcal{H}$ je normální podgrupa grupy $\mathcal{G}$. Definujme množinu $\mathcal{G}/\mathcal{H}$ takto

$$\mathcal{G}/\mathcal{H} = \{g\mathcal{H};\ g \in \mathcal{G}\ \}\,.$$

Množina $\mathcal{G}/\mathcal{H}$ spolu s operací $\circ : (\mathcal{G}/\mathcal{H})^2 \to \mathcal{G}/\mathcal{H}$ definovanou pro libovolná $a\mathcal{H}, b\mathcal{H} \in \mathcal{G}/\mathcal{H}$ následovně

$$(a\mathcal{H}) \circ (b\mathcal{H}) = (ab)\mathcal{H},$$

tvoří opět grupu, jež se nazývá *faktorová grupa*.

Pro označení faktorové grupy budeme využívat kratší zápis $\mathcal{G}/\mathcal{H}$ místo $(\mathcal{G}/\mathcal{H}, \circ)$.

Příklad 2.2. (Válec v $\mathbb{Z}_3^2$)
Uvažujme grupu $\mathcal{G} = (\mathbb{Z}_3^2, +)$, kde $+$ je sčítání po složkách a podgrupu vertikálních posunutí[3] $\Gamma = \{p_{0+ni};\ n \in \mathbb{Z}_3\} = \{(0,0),(0,1),(0,2)\}$. Potom $\mathbb{Z}_3^2/\Gamma = \{a + \Gamma;\ a \in \mathbb{Z}_3^2\}$.

$$\begin{aligned}
(0,0)+\Gamma = (0,1)+\Gamma = (0,2)+\Gamma &= \{(0,0),(0,1),(0,2)\}\\
(1,0)+\Gamma = (1,1)+\Gamma = (1,2)+\Gamma &= \{(1,0),(1,1),(1,2)\}\\
(2,0)+\Gamma = (2,1)+\Gamma = (2,2)+\Gamma &= \{(2,0),(2,1),(2,2)\}\,.
\end{aligned}$$

Tedy rozklad podle podgrupy Γ je

$$\mathbb{Z}_3^2/\Gamma = \{\{(0,0),(0,1),(0,2)\}\,,\{(1,0),(1,1),(1,2)\}\,,\{(2,0),(2,1),(2,2)\}\}\,.$$

Definice 2.6 (Přímý součet grup)**.** Uvažujme grupy $(\mathcal{G}, *)$ a $(\mathcal{H}, \circ)$. Přímý součet grup $(\mathcal{G}, *) \oplus (\mathcal{H}, \circ)$ je množina $\mathcal{G} \times \mathcal{H}$ spolu s operací $\bullet$ definovanou pro prvky $(g_1, h_1), (g_2, h_2) \in \mathcal{G} \times \mathcal{H}$ po složkách takto

$$(g_1, h_1) \bullet (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2).$$

Množina $\mathcal{G} \times \mathcal{H}$ s takto zavedenou operací $\bullet$ tvoří opět grupu.

[3] Zavedení grup izometrií je provedeno v kapitole 6.

2.3 Izomorfismus grup

Definice 2.7. Uvažujme grupy $(\mathcal{G}, *)$ a $(\mathcal{H}, \circ)$ a bijektivní zobrazení $f : \mathcal{G} \to \mathcal{H}$. Potom f se nazývá *izomorfismus grupy* $(\mathcal{G}, *)$ *na grupu* $(\mathcal{H}, \circ)$, jestliže pro libovolné prvky $a, b \in \mathcal{G}$ platí

$$f(a * b) = f(a) \circ f(b).$$

Platí také, že $f^{-1} : \mathcal{H} \to \mathcal{G}$ je izomorfismus grupy $(\mathcal{H}, \circ)$ na grupu $(\mathcal{G}, *)$. Říkáme, že tyto grupy jsou *izomorfní* a píšeme $(\mathcal{G}, *) \approx (\mathcal{H}, \circ)$.

Definice 2.8. (Celočíselná mocnina) Uvažujme grupu $(\mathcal{G}, \cdot)$, prvek $a \in \mathcal{G}$ a $n \in \mathbb{Z}$. Pro různá n klademe

$n > 0$	$n = 0$	$n < 0$
$a^n = \underbrace{a \cdot \ldots \cdot a}_{n\text{-krát}}$	e	$a^n = \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{\lvert n\rvert\text{-krát}}$

Definice 2.9. Grupa $\mathcal{G}$ se nazývá *cyklická*, jestliže existuje prvek $g \in \mathcal{G}$ takový, že každý prvek grupy $\mathcal{G}$ je nějakou celočíselnou mocninou prvku g. Prvek g se pak nazývá *generátor grupy* $\mathcal{G}$ a píšeme $\mathcal{G} = \langle g \rangle$.

Věta 2.1. Nechť $\mathcal{G}$ je cyklická grupa řádu n, kde $n \in \mathbb{N}$. Potom $\mathcal{G}$ je izomorfní s grupou $(\mathbb{Z}_n, +)$.

Důkaz 2.1. Důkaz proveden v [7].

Příklad 2.3. Uvažujme množinu $\mathcal{E}_\infty = \{[1,1], [1,-1], [2,1], [2,-1], \infty\}$ a operaci $\oplus$ definovanou tabulkou.

$\oplus$	∞	$[1,1]$	$[1,-1]$	$[2,1]$	$[2,-1]$
∞	∞	$[1,1]$	$[1,-1]$	$[2,1]$	$[2,-1]$
$[1,1]$	$[1,1]$	$[2,1]$	∞	$[2,-1]$	$[1,-1]$
$[1,-1]$	$[1,-1]$	∞	$[2,-1]$	$[1,1]$	$[2,1]$
$[2,1]$	$[2,1]$	$[2,-1]$	$[1,1]$	$[1,-1]$	∞
$[2,-1]$	$[2,-1]$	$[1,-1]$	$[2,1]$	∞	$[1,1]$

V kapitole 4 (příklad (4.3)) ukážeme, že $(\mathcal{E}_\infty, \oplus)$ je cyklická grupa s neutrálním prvkem ∞. Nyní však sestrojíme izomorfismus dané grupy s $(\mathbb{Z}_5, +)$ podle věty 2.1. Izomorfismus $f : \mathcal{E}_\infty \to \mathbb{Z}_5$ a upravená aditivní tabulka grupy $(\mathbb{Z}_5, +)$ jsou dány následujícími tabulkami

∞	$\to$	0
$[2,1]$	$\to$	1
$[2,-1]$	$\to$	4
$[1,1]$	$\to$	3
$[1,-1]$	$\to$	2

Tabulka 1: $f : \mathcal{E}_\infty \to \mathbb{Z}_5$

$+$	0	3	2	1	4
0	0	3	2	1	4
3	3	1	0	4	2
2	2	0	4	3	1
1	1	4	3	2	0
4	4	2	1	0	3

Tabulka 2: Aditivní tabulka grupy $(\mathbb{Z}_5, +)$

2.4 Pole

Definice 2.10. Množinu $\mathcal{F}$, která má alespoň 2 prvky, spolu s operacemi + a · nazýváme *pole*, jestliže jsou splněny následující axiomy

($\mathcal{F}1$) $(\mathcal{F}, +)$ je komutativní grupa.

($\mathcal{F}2$) Pro všechna $a, b, c \in \mathcal{F}$ platí: $(a.b).c = a.(b.c)$

($\mathcal{F}3$) Existuje $1_{\mathcal{F}} \in \mathcal{F}$ tak, že $\forall a \in \mathcal{F}$ platí: $1_{\mathcal{F}}.a = a.1_{\mathcal{F}} = a$

($\mathcal{F}4$) Pro všechna $a \in \mathcal{F}$, $a \neq 0_{\mathcal{F}}$ existuje $a^{-1} \in \mathcal{F}$ tak, že $a.a^{-1} = a^{-1}.a = 1_{\mathcal{F}}$

($\mathcal{F}5$) Platí *distributivní zákony*, tj. pro $a, b, c \in \mathcal{F}$ platí

$$a.(b + c) = a.b + a.c \quad \wedge \quad (b + c).a = b.a + c.a$$

Pole budeme označovat $(\mathcal{F}, +, \cdot)$ nebo jen zkráceně $\mathcal{F}$.

Příklad 2.4. Základními příklady nekonečných polí jsou číselné množiny s operacemi sčítání a násobení v jednotlivých aritmetikách $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$.

Množina racionálních funkcí $f(x) = \frac{p(x)}{q(x)}$, kde $p(x), q(x) \in \mathcal{F}[x]$ jsou polynomy jedné neurčité s koeficienty z pole $\mathcal{F}$, spolu s operací součtu a součinu polynomů tvoří pole, které označujeme pole racionálních funkcí $(\mathcal{F}(x), +, \cdot)$.

Dalším příkladem polí jsou pole konečná, která zavedl francouzský matematik Évariste Galois. Konečná pole existují pouze pro p^n prvků, kde p je prvočíslo. Takové pole je až na izomorfismus jediné.

Pole $(\mathbb{Z}_p, +, \cdot)$, kde $\mathbb{Z}_p$ je množina zbytkových tříd modulo p a operace jsou sčítání a násobení v modulární aritmetice, je příkladem konečného pole. Pro pole $(\mathbb{Z}_p, +, \cdot)$ však využíváme označení $(\mathbb{F}_p, +, \cdot)$ a nazýváme jej polem *prvočíselným*.

V případě $n > 1$ se pole nazývají *neprvočíselná* a značíme je $(\mathbb{F}_{p^n}, +, \cdot)$.
Operace + a · se zavádějí speciálně (viz např. [12]).

Definice 2.11. Uvažujme pole $\mathcal{F}$, nulový prvek $0_{\mathcal{F}}$ a jedničku $1_{\mathcal{F}}$. *Charakteristikou pole* $\mathcal{F}$ nazýváme takové nejmenší číslo $n \in \mathbb{N}$, pro které platí

$$\underbrace{1_{\mathcal{F}} + 1_{\mathcal{F}} + \cdots + 1_{\mathcal{F}}}_{\text{n-krát}} = 0_{\mathcal{F}}$$

a píšeme $char(\mathcal{F}) = n$.

V případě, že takové přirozené číslo n neexistuje, říkáme, že pole $\mathcal{F}$ má charakteristiku 0 a píšeme $char(\mathcal{F}) = 0$.

Věta 2.2. Uvažujme pole $\mathcal{F}$ charakteristiky $n \in \mathbb{N}$. Potom n je prvočíslo.

Důkaz 2.2. Důkaz proveden v [7].

3 Kvadratická rezidua

Definice 3.1. Uvažujme $a \in \mathbb{N}$ a prvočíslo $p > 2$, kde a, p jsou nesoudělná. Řekneme, že číslo a je *kvadratickým reziduem* $(\mathrm{mod}\, p)$, jestliže kongruence

$$y^2 - a \equiv 0 \,(\mathrm{mod}\, p)$$

má řešení.
V opačném případě říkáme, že a je *kvadratickým nereziduem* $(\mathrm{mod}\, p)$.

Všechna kvadratická rezidua dostaneme, pokud budeme čísla $1^2, 2^2, \ldots, (p-1)^2$ redukovat podle modulu p. Dalším důležitým poznatkem v teorii je, že existuje právě $\frac{p-1}{2}$ kvadratických reziduí a stejný počet nereziduí.[4]

Úlohu určit, zda dané číslo a je, či není kvadratickým reziduem je možné řešit také pomocí následujícího teorému.

Teorém 3.1. (Eulerovo kritérium)

$$a^{\frac{1}{2}(p-1)} \equiv 1 \Longleftrightarrow a \text{ je kvadratickým reziduem}$$

$$a^{\frac{1}{2}(p-1)} \equiv -1 \Longleftrightarrow a \text{ je kvadratickým nereziduem}$$

Důkaz Teorému 3.1. Důkaz proveden v [6].

Zavedeme nyní symbol, vyjadřující vztah a k p v teorii kvadratických reziduí.

Definice 3.2. Nechť $p > 2$ a $(a, p) = 1$. *Legendrův symbol* $\left(\frac{a}{p}\right)$ nyní definujeme následovně

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{, pokud } a \text{ je kvadratické reziduum } (\mathrm{mod}\, p) \\ 0 & \text{, pokud } a \equiv 0 \,(\mathrm{mod}\, p) \\ -1 & \text{, pokud } a \text{ je kvadratické nereziduum } (\mathrm{mod}\, p) \end{cases}$$

Originální definici je možné nalézt na str. 42 knihy [6]. Definujeme zde stejně jako v [9] pro Legendrův symbol navíc hodnotu 0 z důvodu výpočtu počtu bodů semi-eliptických křivek.

Věta 3.1. Nechť $a, b \in \mathbb{N}$ a $p > 2$. Potom platí

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

Důkaz 3.1. Za předpokladu $p > 2$ lze psát přímo

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{1}{2}(p-1)} = a^{\frac{1}{2}(p-1)} \cdot b^{\frac{1}{2}(p-1)} = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

[4] Tabulka kvadratických reziduí pro $p \leq 61$ je uvedena v příloze B.

4 Úvod k eliptickým křivkám

V následující kapitole prostudujeme vlastnosti speciálních kubických křivek. Nejdříve uvedeme pojem obecnější semi-eliptické křivky a dále zúžení na křivky eliptické. K našim účelům bude postačující, když se omezíme na jeden tvar eliptických křivek, zobecnění je možné najít v [1].

Definice 4.1. *Semi-eliptickou křivkou definovanou nad polem* $\mathcal{F}$ rozumíme množinu všech bodů $(x, y) \in \mathcal{F} \times \mathcal{F}$, která je určena rovnicí

$$\mathcal{E} : y^2 = x^3 + ax + b, \tag{4.1}$$

kde koeficienty a, b jsou prvky pole $\mathcal{F}$.

Semi-eliptickou křivku s pevnými koeficienty $a, b \in \mathcal{F}$ označme $\mathcal{E}(\mathcal{F}, a, b)$, čili

$$\mathcal{E}(\mathcal{F}, a, b) = \left\{(x, y) \in \mathcal{F} \times \mathcal{F} : y^2 = x^3 + ax + b\right\}. \tag{4.2}$$

Dále symbolem Δ označme *diskriminant* této křivky, jenž je definován

$$\Delta = -16(4a^3 + 27b^2). \tag{4.3}$$

Z důvodu zjednodušení můžeme místo $\mathcal{E}(\mathcal{F}, a, b)$ psát také $\mathcal{E}(\mathcal{F})$ nebo jen $\mathcal{E}$.

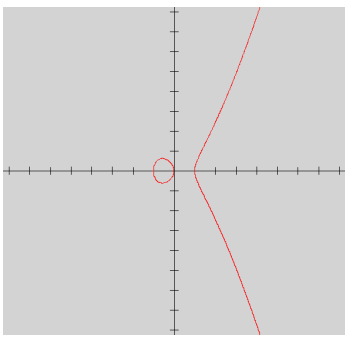
Poznámka 4.1.

(i) V literatuře [1] je možné dohledat obecnější (tzv. *Weierstrassovu*) rovnici ve tvaru $\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, kde $a_1, a_2, a_3, a_4, a_6 \in \mathcal{F}$. Zjednodušení na tvar (4.1) se provádí pomocí transformace souřadnic.

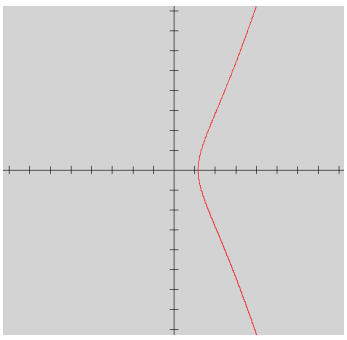
(ii) S výhodou využijeme zápisu $\mathcal{E}(\mathcal{F})$ při zdůraznění, že $\mathcal{E}$ je definována nad polem $\mathcal{F}$.

(iii) Determinant semi-eliptické křivky určuje její regularitu. Pokud $\Delta = 0$, potom semi-eliptická křivka obsahuje nějaký typ singulárního bodu.

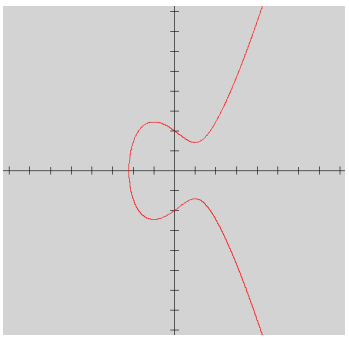
Příklad 4.1. (Semi-eliptické křivky nad polem $\mathbb{R}$ s $\Delta \neq 0$)



Obrázek 1: $\mathcal{E}(\mathbb{R}, -1, 0)$
$\Delta = 64$

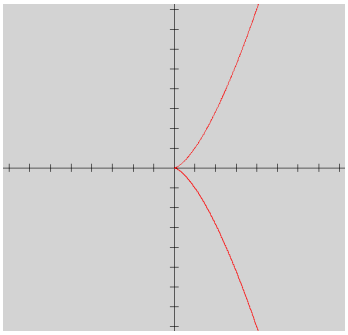


Obrázek 2: $\mathcal{E}(\mathbb{R}, 2, -4)$
$\Delta = -7424$

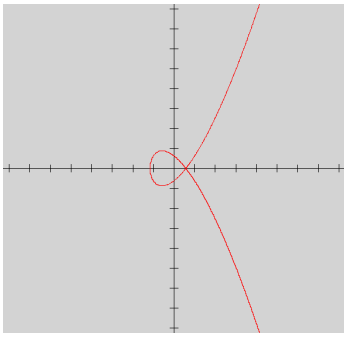


Obrázek 3: $\mathcal{E}(\mathbb{R}, -3, -4)$
$\Delta = -5184$

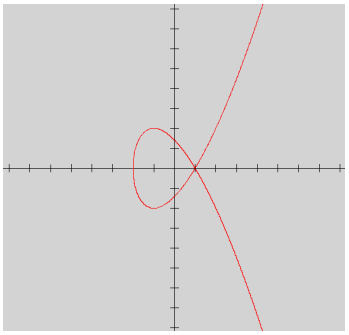
Semi-eliptické křivky nad polem $\mathbb{R}$ s $\Delta = 0$.



Obrázek 4: $\mathcal{E}(\mathbb{R}, 0, 0)$



Obrázek 5: $\mathcal{E}(\mathbb{R}, -1, \frac{2\sqrt{3}}{9})$



Obrázek 6: $\mathcal{E}(\mathbb{R}, -3, -2)$

Jak můžeme pozorovat z obrázků výše, pokud $\Delta = 0$ a $a = 0$, potom křivka obsahuje *bod vratu*. Dále, pokud $\Delta = 0$ a $a \neq 0$, potom křivka obsahuje *uzel*.

V následujícím odstavci zavedeme pojem eliptické křivky. Zaměříme se specielně na eliptické křivky tvaru $\mathcal{E} : y^2 = x^3 + ax + b$ nad polem $\mathcal{F}$ charakteristiky různé od 2 nebo 3.

4.1 Eliptické křivky

Definice 4.2. *Eliptickou křivkou definovanou nad polem* $\mathcal{F}$, kde $char(\mathcal{F}) \neq 2, 3$ rozumíme takovou semi-eliptickou křivku $\mathcal{E}$, že platí $\Delta \neq 0$.

Eliptickou křivkou $\mathcal{E}$ tedy rozumíme opět množinu $\mathcal{E}(\mathcal{F}, a, b)$ danou vztahem

$$\mathcal{E}(\mathcal{F}, a, b) = \left\{(x, y) \in \mathcal{F} \times \mathcal{F} : y^2 = x^3 + ax + b\right\}, \tag{4.4}$$

avšak při nenulovém diskriminantu.

Eliptickou křivkou $\mathcal{E}_\infty$ *s bodem* ∞ rozumíme množinu $\mathcal{E}_\infty(\mathcal{F}, a, b)$ danou vztahem

$$\mathcal{E}_\infty(\mathcal{F}, a, b) = \mathcal{E}(\mathcal{F}, a, b) \cup \{\infty\} = \left\{(x, y) \in \mathcal{F} \times \mathcal{F} : y^2 = x^3 + ax + b\right\} \cup \{\infty\}. \tag{4.5}$$

Eliptickou křivku $\mathcal{E}_\infty(\mathcal{F}, a, b)$ s bodem ∞ často označujeme jen jako eliptickou křivku a využíváme opět kratšího označení $\mathcal{E}_\infty(\mathcal{F})$ nebo $\mathcal{E}_\infty$.

Poznámka 4.2.

(i) Podmínka $\Delta \neq 0$ nyní již zaručuje regularitu eliptické křivky.

(ii) Je nutné rozlišovat mezi množinami $\mathcal{E}_\infty(\mathcal{F}, a, b)$ a $\mathcal{E}(\mathcal{F}, a, b)$. Na první z nich lze zavést grupovou operaci $\oplus$, jak bude ukázáno později.

(iii) V literatuře se často přímo zavádí eliptická křivka $\mathcal{E}(\mathcal{F})$ jako množina vlastních bodů spolu s bodem ∞. Z důvodu lepšího popisu při vizualizaci křivek však nejdříve zavádíme (4.4) a následně (4.5).

4.2 Struktura grupy

Uvažujme eliptickou křivku $\mathcal{E}_\infty(\mathcal{F})$ definovanou nad polem $\mathcal{F}$. Po dodání dalšího prvku, který označíme ∞, k množině všech vlastních bodů eliptické křivky je nyní možné postupně vytvořit strukturu grupy. Nechť $\mathcal{E}_\infty(\mathcal{F})$ je množinou všech bodů eliptické křivky $\mathcal{E}$ s bodem ∞. Operaci $\oplus : \mathcal{E}^2_\infty(\mathcal{F}) \mapsto \mathcal{E}_\infty(\mathcal{F})$ nyní zavedeme následovně.

(1) *Neutrální prvek.* Nechť $P \in \mathcal{E}_\infty(\mathcal{F})$, potom $P \oplus \infty = \infty \oplus P = P$.

(2) *Opačný prvek.* Uvažujme bod $P = (x, y) \in \mathcal{E}_\infty(\mathcal{F})$, potom bod $-P = (x, -y) \in \mathcal{E}_\infty(\mathcal{F})$ se nazývá *opačný* k P a platí $P \oplus -P = (x, y) \oplus (x, -y) = \infty$. Také $-\infty = \infty$.

(3) *Součet bodů.* Nechť $P = (x_1, y_1) \in \mathcal{E}_\infty(\mathcal{F})$ a $Q = (x_2, y_2) \in \mathcal{E}_\infty(\mathcal{F})$, kde $P \neq \pm Q$. Potom $R = P \oplus Q = (x_3, y_3)$, kde

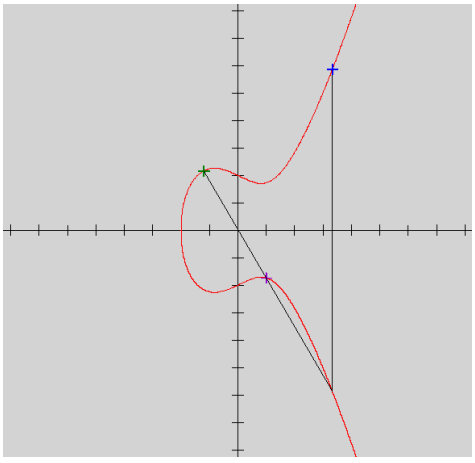
$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \quad a \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1. \tag{4.6}$$

(4) *Zdvojení bodu.* Nechť $P = (x_1, y_1) \in \mathcal{E}_\infty(\mathcal{F})$, kde $P \neq -P$. Potom $R = P \oplus P = (x_3, y_3)$, kde

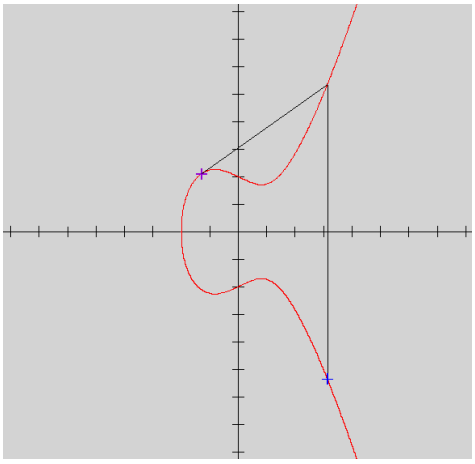
$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \quad a \quad y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1. \tag{4.7}$$

Množina s operací $(\mathcal{E}_\infty(\mathcal{F}), \oplus)$ tvoří grupu, která určuje aritmetiku bodů na eliptických křivkách. Velice názorně lze vysvětlit operaci součtu, pokud si představíme eliptickou křivku v reálné rovině. Sčítáme-li dva různé body, nejdříve vedeme přímku těmito body a bod, kde se tato přímka protne opět s eliptickou křivkou, symetricky promítneme podle osy x zase na bod eliptické křivky, který je výsledkem. V případě, když se pokusíme sečíst bod sám se sebou, vedeme tečnu k eliptické křivce v tomto bodě a místo, kde se tečna protne s eliptickou křivkou opět promítneme dle osy x, čímž získáme výsledek součtu.

Příklad 4.2. Součtu a zdvojení bodů na eliptické křivce $\mathcal{E}_\infty(\mathbb{R}, -2, 4)$.



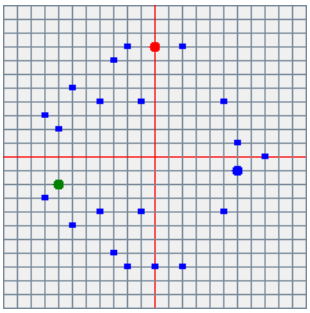
Obrázek 7: Součet bodů



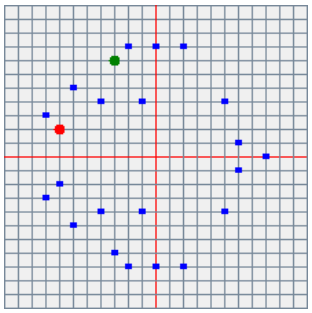
Obrázek 8: Zdvojení bodu

Poslední možností je součet bodů tvaru $P = (x, y)$ a $Q = (x, -y)$, neboli bodů opačných. Výsledkem součtu je pak právě bod ∞. Interpretací bodu ∞ v reálné rovině tedy může být rovnoběžka s osou y.

Uvádíme dále příklad součtu bodů $P = (-7, -2)$ a $Q = (6, -1)$ a zdvojení bodu $R = (-3, 7)$ na eliptické křivce $\mathcal{E}_\infty(\mathbb{F}_{17}, 13, 13)$.



Obrázek 9: $P \oplus Q = (0, 8)$



Obrázek 10: $R \oplus R = (-7, 2)$

O grupu $(\mathcal{E}_\infty(\mathcal{F}), \oplus)$ se opírají kryptosystémy založené na eliptických křivkách. Pole, nad kterými jsou výpočty prováděny, jsou z velké míry pole prvočíselná $\mathbb{F}_p$ a binární $\mathbb{F}_{2^n}$. Budeme se však zabývat jen poli prvočíselnými. Pro praktickou kryptografii se vyžaduje velice dobrá implementace grupové operace nad těmito poli a dále rychlé určení řádu eliptické křivky. Věnujme se nyní zavedení tohoto pojmu.

4.3 Počet bodů křivky a řád grupy

Definice 4.3. Uvažujme semi-eliptickou křivku $\mathcal{E}$ definovanou nad prvočíselným polem $\mathbb{F}_p$, kde $p > 3$. Počet bodů křivky, neboli mohutnost konečné množiny $\mathcal{E}(\mathbb{F}_p, a, b)$ označme

$$\texttt{card}(\mathcal{E}(\mathbb{F}_p, a, b)).$$

Jelikož z rovnice $y^2 = x^3 + ax + b$ pro pevné x dostáváme dvě, jedno nebo žádné řešení, můžeme počet bodů dané semi-eliptické křivky $\mathcal{E}(\mathbb{F}_p, a, b)$ spočíst s využitím Legendrova symbolu $\left(\frac{\cdot}{p}\right)$ následovně

$$\texttt{card}(\mathcal{E}(\mathbb{F}_p, a, b)) = \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right) = p + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right).$$

Uvedený přístup k výpočtu bodů semi-eliptických křivek se nazývá *naivní algoritmus*. V programu `ElCOFF` je implementován pro malá p přímý výpočet bodů, takže počet bodů dostáváme jako vedlejší produkt. Existují však mnohem efektivnější algoritmy, viz například [9].

Definice 4.4. Nechť $\mathcal{E}_\infty$ je eliptická křivka definovaná nad prvočíselným polem $\mathbb{F}_p$, kde $p > 3$. *Řádem* eliptické křivky rozumíme řád $\mathcal{E}_\infty$ jako grupy, který označíme $\#\mathcal{E}_\infty(\mathbb{F}_p, a, b)$ a platí

$$\#\mathcal{E}_\infty(\mathbb{F}_p, a, b) = \texttt{card}(\mathcal{E}_\infty(\mathbb{F}_p, a, b)) = \texttt{card}(\mathcal{E}(\mathbb{F}_p, a, b)) + 1.$$

Nyní uvedeme teorém, jež nám poskytne odhad řádu eliptické křivky.

Teorém 4.1 (Hasse)**.** Nechť $\mathcal{E}_\infty$ je eliptická křivka definovaná nad $\mathbb{F}_p$. Potom

$$p + 1 - 2\sqrt{p} \leq \#\mathcal{E}_\infty(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

Interval $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ se nazývá *Hasseho interval*.

Důkaz Teorému 4.1. V příloze A.

Teorém 4.2. (Struktura grupy eliptických křivek) Uvažujme eliptickou křivku $\mathcal{E}_\infty(\mathbb{F}_p)$. Potom $\mathcal{E}_\infty(\mathbb{F}_p)$ je izomorfní s $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ ($\oplus$ značí přímý součet grup), kde $n_1, n_2 \in \mathbb{N}$ jsou jednoznačně určena a platí

$$n_2|(p-1) \ \wedge \ n_2|n_1.$$

Platí, že $\#\mathcal{E}_\infty(\mathbb{F}_p) = n_1 n_2$. Jestliže $n_2 = 1$, potom $\mathcal{E}_\infty(\mathbb{F}_p)$ je cyklická grupa. Zobecnění teorému viz [1].

Příklad 4.3. Uvažujme eliptickou křivku $\mathcal{E}_\infty(\mathbb{F}_5, 3, 2) = \{[1,1], [1,-1], [2,1], [2,-1], \infty\}$. Tabulka grupové operace je uvedena v příkladu (2.3). Jelikož $\#\mathcal{E}_\infty = 5$, $n_1 = 5$ a $n_2 = 1$. Eliptická křivka $\mathcal{E}_\infty(\mathbb{F}_5, 3, 2)$ je tedy cyklická grupa řádu 5 s libovolným generátorem různým od neutrálního prvku ∞. Označme $P = [1,1]$, potom $\mathcal{E}_\infty(\mathbb{F}_5, 3, 2) = \langle P \rangle$.

$0P = \infty$	$1P = [1,1]$	$2P = [2,1]$	$3P = [2,-1]$	$4P = [1,-1]$

Dalším z důležitých invariantů v teorii eliptických křivek je kromě diskriminantu Δ také j-invariant, který uvedeme v následující definici.

Definice 4.5. Nechť $\mathcal{E}_\infty(\mathbb{F}_p, a, b)$ je eliptická křivka definovaná nad prvočíselným polem $\mathbb{F}_p$. Pak *j-invariantem* nazveme číslo $j(\mathcal{E}_\infty)$, kde

$$j(\mathcal{E}_\infty) = 1728\frac{4a^3}{4a^3 + 27b^2} \in \mathbb{F}_p.$$

Definice 4.6. Uvažujme eliptické křivky $\mathcal{E}_\infty(\mathbb{F}_p, a, b)$ a $\mathcal{E}'_\infty(\mathbb{F}_p, a', b')$ definované nad prvočíselným polem $\mathbb{F}_p$ a dále $0 \neq d \in \mathbb{F}_p$ kvadratické nereziduum. Řekneme, že eliptická křivka $\mathcal{E}'_\infty$ je *kvadratickým twistem* křivky $\mathcal{E}_\infty$, jestliže platí

$$a' = ad^2 \quad \wedge \quad b' = bd^3.$$

Kvadratický twist dané křivky $\mathcal{E}_\infty$ je tedy tvaru $\mathcal{E}'_\infty : y^2 = x^3 + ad^2x + bd^3$. Z definice (4.5) vyplývá, že eliptické křivky $\mathcal{E}_\infty$ i $\mathcal{E}'_\infty$ mají shodný j-invariant.

Teorém 4.3. (Mestre) Nechť $\mathcal{E}_\infty$ je eliptická křivka definovaná nad prvočíselným polem $\mathbb{F}_p$ a $\#\mathcal{E}_\infty(\mathbb{F}_p, a, b) = p + 1 - t$, $t \in \mathbb{Z}$. Označme $\mathcal{E}'_\infty(\mathbb{F}_p, ad^2, bd^3)$ eliptickou křivku, která je kvadratickým twistem křivky $\mathcal{E}_\infty$. Pak pro $\#\mathcal{E}'_\infty(\mathbb{F}_p, ad^2, bd^3)$ platí

$$\#\mathcal{E}'_\infty(\mathbb{F}_p, ad^2, bd^3) = p + 1 + t.$$

Ekvivalentně můžeme Mestreho výsledek interpretovat jako skutečnost, že součet bodů $\mathcal{E}_\infty$ a $\mathcal{E}'_\infty$ je konstantní a platí

$$\#\mathcal{E}_\infty(\mathbb{F}_p, a, b) + \#\mathcal{E}'_\infty(\mathbb{F}_p, ad^2, bd^3) = 2p + 2$$

Poznámka 4.3. V generovaných tabulkách programem `ElCOFF` je uveden vždy počet bodů semi-eliptických křivek, tedy součet bodů $\mathcal{E}$ a $\mathcal{E}'$ je roven $2p$, neboť sčítáme jen vlastní body (vynecháváme u $\mathcal{E}$ i $\mathcal{E}'$ bod ∞).

4.4 Experimentální výsledky

Vraťme se nazpět k obecnějšímu pojmu semi-eliptické křivky, nerozlišujeme tedy regularitu křivek. Motivací ke studiu semi-eliptických křivek a vůbec zavedení tohoto pojmu bylo softwarové zpracování a následná analýza množiny všech semi-eliptických křivek nad prvočíselnými poli.

V následujícím textu se budeme zabývat touto množinou, kterou budeme označovat $\mathcal{M}(\mathbb{F}_p)$. Zaměříme se na její strukturu a vlastnosti. Pokud již z kontextu bude zřejmé, že daná semi-eliptická křivka je definována nad $\mathbb{F}_p$, pak z důvodu zjednodušení zápisu budeme psát $\mathcal{E}(a,b)$ místo $\mathcal{E}(\mathbb{F}_p,a,b)$, případně pro systém $\mathcal{M}(\mathbb{F}_p)$ využijeme jen zápisu $\mathcal{M}$.

Nejjednošším případem je množina $\mathcal{M}(\mathbb{F}_5)$, která obsahuje všechny semi-eliptické křivky nad polem $\mathbb{F}_5$. Z tabulky vidíme, že pro eliptické křivky $\mathcal{E}_\infty$ je číslo $\texttt{card}(\mathcal{E})+1$ zároveň jejich řádem. Výraz „NaN“ pro j-invariant je uveden právě u semi-eliptických křivek, které nejsou eliptickými.

(a,b)	Δ	$j(\mathcal{E})$	$\texttt{card}(\mathcal{E})$	$\mathcal{E}(\mathbb{F}_5,a,b)$
(0,0)	0	NaN	5	[0,0][1,1][1,-1][-1,2][-1,-2]
(0,1)	-2	0	5	[0,1][0,-1][2,2][2,-2][-1,0]
(0,2)	-3	0	5	[2,0][-2,2][-2,-2][-1,1][-1,-1]
(0,3)	-3	0	5	[1,2][1,-2][2,1][2,-1][-2,0]
(0,4)	-2	0	5	[0,2][0,-2][1,0][-2,1][-2,-1]
(1,0)	-4	3	3	[0,0][2,0][-2,0]
(1,1)	-1	2	8	[0,1][0,-1][2,1][2,-1][-2,1][-2,-1][-1,2][-1,-2]
(1,2)	-2	1	3	[1,2][1,-2][-1,0]
(1,3)	-2	1	3	[1,0][-1,1][-1,-1]
(1,4)	-1	2	8	[0,2][0,-2][1,1][1,-1][2,2][2,-2][-2,2][-2,-2]
(2,0)	-2	3	1	[0,0]
(2,1)	-4	4	6	[0,1][0,-1][1,2][1,-2][-2,2][-2,-2]
(2,2)	0	NaN	6	[1,0][2,2][2,-2][-2,0][-1,2][-1,-2]
(2,3)	0	NaN	6	[1,1][1,-1][2,0][-2,1][-2,-1][-1,0]
(2,4)	-4	4	6	[0,2][0,-2][2,1][2,-1][-1,1][-1,-1]
(3,0)	-3	3	9	[0,0][1,2][1,-2][2,2][2,-2][-2,1][-2,-1][-1,1][-1,-1]
(3,1)	0	NaN	4	[0,1][0,-1][1,0][2,0]
(3,2)	-1	4	4	[1,1][1,-1][2,1][2,-1]
(3,3)	-1	4	4	[-2,2][-2,-2][-1,2][-1,-2]
(3,4)	0	NaN	4	[0,2][0,-2][-2,0][-1,0]
(4,0)	-1	3	7	[0,0][1,0][2,1][2,-1][-2,2][-2,-2][-1,0]
(4,1)	-3	1	7	[0,1][0,-1][1,1][1,-1][-2,0][-1,1][-1,-1]
(4,2)	-4	2	2	[-2,1][-2,-1]
(4,3)	-4	2	2	[2,2][2,-2]
(4,4)	-3	1	7	[0,2][0,-2][1,2][1,-2][2,0][-1,2][-1,-2]

Tabulka 3: Výpis všech semi-eliptických křivek nad $\mathbb{F}_5$

Příklad 4.4. Prozkoumejme vlastnosti semi-eliptické křivky $\mathcal{E}(\mathbb{F}_{31}, 3, 18)$. Diskriminant této křivky je

$$\Delta = -16(4.3^3 + 27.18^2) = -141696,$$

platí tedy $-141696 \equiv -26 (\mathrm{mod}\, 31) \Longrightarrow$ křivka je regulární (eliptická).
Spočtěme ještě j-invariant

$$j(\mathcal{E}) = 1728 \frac{4.3^3}{4.3^3 + 27.18^2} = \frac{864}{41},$$

dostáváme $\frac{864}{41} \equiv 12 (\mathrm{mod}\, 31)$.

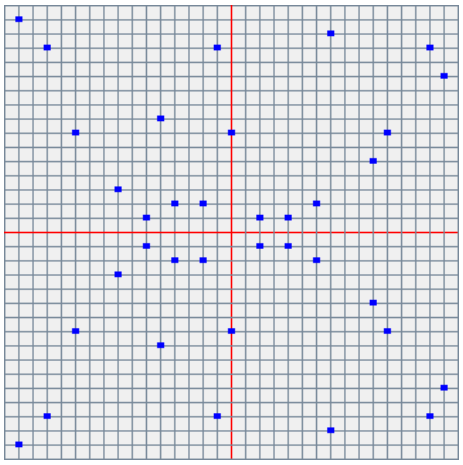
Řád křivky zjistíme z tabulky nebo grafu vygenerované programem `ElCOFF`. Řádek příslušné tabulky vypadá následovně

(a, b)	Δ	$j(\mathcal{E})$	`card`$(\mathcal{E})$	$\mathcal{E}(\mathbb{F}_{31}, a, b)$
(3,18)	-26	12	36	[0,7][0,-7][2,1][2,-1][4,1][4,-1][6,2][6,-2] [7,14][7,-14][10,5][10,-5][11,7][11,-7][14,13][14,-13] [15,11][15,-11][-15,15][-15,-15][-13,13][-13,-13][-11,7] [-11,-7][-8,3][-8,-3][-6,1][-6,-1][-5,8][-5,-8][-4,2] [-4,-2][-2,2][-2,-2][-1,13][-1,-13]

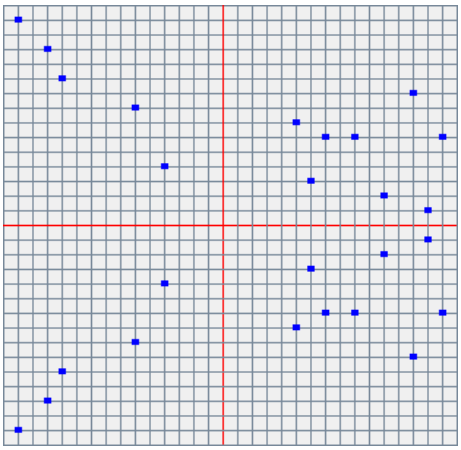
Tabulka 4: Semi-eliptická křivka $\mathcal{E}(\mathbb{F}_{31}, 3, 8)$

Spočtěme dále kvadratický twist eliptické křivky $\mathcal{E}(\mathbb{F}_{31}, 3, 18)$ pro kvadratické nerezidduum $d = 15$. Víme, že počet bodů je `card`$(\mathcal{E}(3, 18)) = 36 = 31 - (-5)$ a kvadratický twist této křivky $\mathcal{E}'(\mathbb{F}_{31}, a', b')$, bude mít počet bodů `card`$(\mathcal{E}(a', b')) = 31 + (-5) = 26$. Pomocí vztahů $a' = ad^2$ a $b' = bd^3$ dostáváme $a' = 24$ a $b' = 21$. Ověříme nyní počet bodů křivky $\mathcal{E}'(\mathbb{F}_{31}, 24, 21)$ pomocí výstupu z programu.

Eliptická křivka $\mathcal{E}(\mathbb{F}_{31}, 3, 18)$ a její kvadratický twist $\mathcal{E}'(\mathbb{F}_{31}, 24, 21)$.



Obrázek 11: $\mathcal{E}(\mathbb{F}_{31}, 3, 18)$



Obrázek 12: $\mathcal{E}'(\mathbb{F}_{31}, 24, 21)$

4.4.1 Třídění semi-eliptických křivek

Hasseho interval bez připočtení bodu ∞ je postupně pro pole $\mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_{11}$ dán a zaokrouhlen $\langle 1, 9\rangle$, $\langle 2, 12\rangle$, $\langle 5, 17\rangle$. Roztřídění semi-eliptických křivek nad zmíněnými poli uvádíme v následujících tabulkách, případně v grafu (obrázek 13).

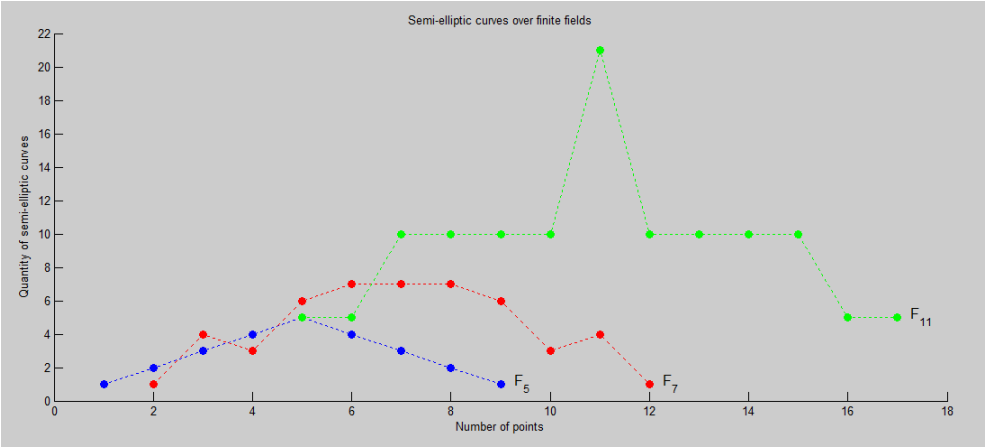
$\texttt{card}(\mathcal{E}(\mathbb{F}_5))$	Počet semi-el. křivek
1	1
2	2
3	3
4	4
5	5
6	4
7	3
8	2
9	1

Tabulka 5: Semi-el. křivky nad $\mathbb{F}_5$

$\texttt{card}(\mathcal{E}(\mathbb{F}_7))$	Počet semi-el. křivek
2	1
3	4
4	3
5	6
6	7
7	7
8	7
9	6
10	3
11	4
12	1

Tabulka 6: Semi-el. křivky nad $\mathbb{F}_7$

Další obrázek zachycuje, jak se vyvíjí počet semi-eliptických křivek v závislosti na hodnotách počtu bodů z Hasseho intervalu pro tři prvočíselná pole.



Obrázek 13: Roztřídění semi-eliptických křivek nad poli $\mathbb{F}_5$, $\mathbb{F}_7$ a $\mathbb{F}_{11}$

Z analýzy uvedených dat a dalšího studia množin $\mathcal{M}(\mathbb{F}_p)$ všech semi-eliptických křivek nad různými prvočíselnými poli byly získány následující poznatky.

Věta 4.1. Uvažujme množinu $\mathcal{M}(\mathbb{F}_p)$ všech semi-eliptických křivek tvaru

$$\mathcal{E} : y^2 = x^3 + ax + b$$

definovaných nad $\mathbb{F}_p$. Přesněji $\mathcal{M}(\mathbb{F}_p) = \{\mathcal{E}(a,b) : a,b \in \mathbb{F}_p\}$. Označme $\mathcal{M}_a = \{\mathcal{E}(a,b) : b \in \mathbb{F}_p\}$ jednoparametrický systém, kde $a \in \mathbb{F}_p$ je pevně zvoleno.

Pak pro $\mathcal{E}(a,i) \in \mathcal{M}_a, i \in \mathbb{F}_p$ platí

$$\mathcal{E}(a,0) \cup \mathcal{E}(a,1) \cup \cdots \cup \mathcal{E}(a,p-1) = \bigcup_{i=0}^{p-1} \mathcal{E}(a,i) = \{(x,y) : x,y \in \mathbb{F}_p\} = \mathbb{F}_p \times \mathbb{F}_p$$

Pokud tedy vezmeme všechny křivky s pevným parametrem a a spočteme všechny body takových semi-eliptických křivek nad $\mathbb{F}_p$, dostaneme všechny body množiny $\mathbb{F}_p \times \mathbb{F}_p$.

Důkaz 4.1. Předpokládejme množinu $\mathcal{M}(\mathbb{F}_p)$ a systém množin $\mathcal{M}_a$, $a \in \mathbb{F}_p$.

$$\mathcal{M}_a = \{\mathcal{E}(a,b) : b \in \mathbb{F}_p\}.$$

Pro každé pevné a a libovolné $x \in \mathbb{F}_p$ můžeme psát $x^3 + ax = c$, kde $c \in \mathbb{F}_p$. Dostáváme tedy

$$\left\{x^3 + ax + b : b \in \mathbb{F}_p\right\} = \{c + b : b \in \mathbb{F}_p\} = \mathbb{F}_p.$$

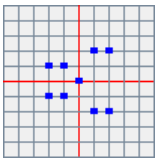
Jelikož platí, že počet kvadratických reziduí v $\mathbb{F}_p$ je $\frac{p-1}{2}$, dostáváme pro kongruenci

$$y^2 \equiv m (\mathrm{mod}\, p),$$

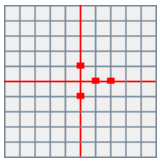
kde m je kvadratické reziduum, $2\frac{p-1}{2} + 1 = p$ různých řešení pro y, kde $p-1$ je dvojic řešení pro různá kvadratická rezidua a jedno triviální řešení $y = 0$. Tím je věta dokázána. □

Poznámka 4.4. Systém množin $\mathcal{M}_a, a \in \mathbb{F}_p$ tvoří pokrytí množiny $\mathcal{M}(\mathbb{F}_p)$.

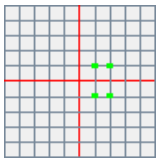
Příklad 4.5. Množina $\mathcal{M}_3$ nad $\mathbb{F}_5$.



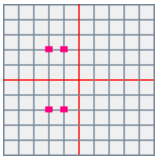
Obrázek 14: $\mathcal{E}(\mathbb{F}_5, 3, 0)$



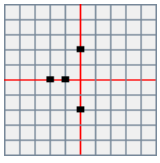
Obrázek 15: $\mathcal{E}(\mathbb{F}_5, 3, 1)$



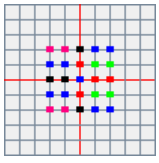
Obrázek 16: $\mathcal{E}(\mathbb{F}_5, 3, 2)$



Obrázek 17: $\mathcal{E}(\mathbb{F}_5, 3, 3)$



Obrázek 18: $\mathcal{E}(\mathbb{F}_5, 3, 4)$



Obrázek 19: $\mathcal{M}_3$

Věta 4.2. Uvažujme množinu $\mathcal{M}(\mathbb{F}_p)$ všech semi-eliptických křivek tvaru

$$\mathcal{E} : y^2 = x^3 + ax + b$$

definovaných nad prvočíselným polem $\mathbb{F}_p$.

Pak platí: Počet semi-eliptických křivek z množiny $\mathcal{M}(\mathbb{F}_p)$, které mají diskriminant $\Delta = 0$, je p.

Důkaz 4.2. Diskriminant je definován $\Delta = -16(4a^3 + 27b^2) = 0 \Rightarrow 4a^3 + 27b^2 = 0$. Označme $n = -\frac{4}{27}$. Dostáváme tedy rovnici

$$b^2 = na^3;\ a, b, n \in \mathbb{F}_p$$

Zřejmým řešením je dvojice $(0, 0)$. Vidíme, že se jedná o rovnici, která má buď 2 různé kořeny pro $na^3 \in \mathbb{F}_p, (na^3, p) = 1, a \neq 0$ nebo žádný. Stačí tedy ukázat, že posloupnost $(na^3)_{a=1}^{p-1}$ obsahuje $\frac{p-1}{2}$ (ne nutně různých) kvadratických reziduí.

Vyjdeme dále z věty

$$\left(\frac{cd}{p}\right) = \left(\frac{c}{p}\right)\left(\frac{d}{p}\right),$$

kde $\left(\frac{\div}{p}\right)$ je Legendrův symbol a $c, d \in \mathbb{F}_p$.

Podívejme se nejdříve na posloupnost čísel $(a^2)_{a=1}^{p-1}$, které redukujeme podle modulu p. Všechna tato čísla jsou kvadratickými rezidui, viz [6], str. 43. Pokud dále vezmeme posloupnost čísel $(a^3)_{a=1}^{p-1}$ a skutečnost, že v množině $\mathbb{F}_p$ je právě $\frac{p-1}{2}$ kvadratických reziduí, dostáváme podle věty výše v posloupnosti čísel $(a^3)_{a=1}^{p-1}$ právě $\frac{p-1}{2}$ kvadratických reziduí. Opětovným užitím věty výše dostáváme také v posloupnosti $(na^3)_{a=1}^{p-1}$ právě $\frac{p-1}{2}$ kvadratických reziduí, čímž je věta dokázána. □

Hypotéza 4.1. (Symetrie semi-eliptických křivek) Uvažujme množinu $\mathcal{M}(\mathbb{F}_p)$ všech semi-eliptických křivek tvaru $\mathcal{E} : y^2 = x^3 + ax + b$ definovaných nad $\mathbb{F}_p$. Označme c nejmenší počet bodů křivky, C největší počet bodů křivky $\mathcal{E}(\mathbb{F}_p) \in \mathcal{M}(\mathbb{F}_p)$ a Ψ_i počet křivek řádu i. Pak pro $j = 0, 1, \ldots, \frac{C-c}{2} - 1$ platí

$$\Psi_{c+j} = \Psi_{C-j}$$

Podpora hypotézy 4.1. Uvažujme množinu všech semi-eliptických křivek $\mathcal{M}(\mathbb{F}_p)$. Provedeme rozklad množiny $\mathcal{M}(\mathbb{F}_p)$ na množinu všech eliptických křivek $\mathcal{M}_{\Delta\neq 0}(\mathbb{F}_p)$ nad polem $\mathbb{F}_p$ a množinu všech neeliptických křivek $\mathcal{M}_{\Delta=0}(\mathbb{F}_p)$ nad polem $\mathbb{F}_p$.

K důkazu hypotézy pro $\mathcal{M}_{\Delta\neq 0}(\mathbb{F}_p)$ můžeme využít Mestreho teorém. Zvolíme libovolné kvadratické nereziduum d a postupně pro $\mathcal{E}_\infty(a, b) \in M_{\Delta\neq 0}(\mathbb{F}_p)$ počítáme kvadratický twist $\mathcal{E}_\infty(a', b')$. Podle upraveného Mestreho teorému (poznámka 4.3) platí

$$\texttt{card}\left(\mathcal{E}_\infty(a, b)\right) + \texttt{card}\left(\mathcal{E}_\infty(a', b')\right) = 2p.$$

Ekvivalentně také platí, pokud $\texttt{card}(\mathcal{E}_\infty(a, b)) = p-t, t \in \mathbb{Z} \Rightarrow \texttt{card}(\mathcal{E}_\infty(a', b')) = p+t$. Čili vidíme, že „středem symetrie“ je číslo p. Eliptické křivky $\mathcal{E}_\infty(a, b)$ a $\mathcal{E}_\infty(a', b')$ tvoří jednu dvojici, která „symetrii“ neporuší.

V dalším kroku odečteme dvouprvkovou množinu $\{\mathcal{E}_\infty(a,b), \mathcal{E}_\infty(a',b')\}$ od $\mathcal{M}_{\Delta\neq 0}(\mathbb{F}_p)$ a dostáváme

$$\mathcal{M}^1_{\Delta\neq 0}(\mathbb{F}_p) = \mathcal{M}_{\Delta\neq 0}(\mathbb{F}_p) \setminus \{\mathcal{E}_\infty(a,b), \mathcal{E}_\infty(a',b')\},$$

z které vybereme další eliptickou křivku $\mathcal{E}_\infty(a_1,b_1)$ a dopočítáme kvadratický twist $\mathcal{E}_\infty(a_1',b_1')$, čímž dostáváme další dvojici, která „symetrii“ neporuší.

Pokračujeme dále, až do k-té iterace. Nyní již $\mathcal{M}^k_{\Delta\neq 0}(\mathbb{F}_p) = \emptyset$.

Poznámka 4.5. Počet semi-eliptických křivek v množině $\mathcal{M}(\mathbb{F}_p)$ je p^2. Podle věty (4.2) platí $\texttt{card}(\mathcal{M}_{\Delta=0}(\mathbb{F}_p)) = p$, neboli počet eliptických křivek v množině $\mathcal{M}(\mathbb{F}_p)$ je

$$\texttt{card}(\mathcal{M}_{\Delta\neq 0}(\mathbb{F}_p)) = p^2 - p,$$

což je číslo sudé.

Zabývejme se nyní množinou $\mathcal{M}_{\Delta=0}(\mathbb{F}_p)$. Víme, že $\texttt{card}(\mathcal{M}_{\Delta=0}(\mathbb{F}_p)) = p$ a jistě platí $\mathcal{E}(\mathbb{F}_p,0,0) \in \mathcal{M}_{\Delta=0}(\mathbb{F}_p)$, tedy zbývajících neeliptických křivek je $p-1$.

Hypotéza zůstává otevřená, nepodařilo se prozatím prokázat symetrii i pro zbývajících $p-1$ neeliptických křivek.

5 Úvod do topologie

Definice 5.1. Množinu T spolu se systémem podmnožin τ, neboli dvojici (T, τ) nazýváme *topologický prostor*, právě když τ splňuje následující axiomy

(i) $\emptyset, T \in \tau$.

(ii) Sjednocení libovolných množin z τ patří do τ.

(iii) Průnik jakéhokoli konečného systému množin z τ je také v τ.

Systém podmnožin τ se nazývá *topologií* na množině T. Dále množiny v τ nazýváme *otevřené množiny* a jejich doplňky v T nazýváme *uzavřené množiny*.

Prvním příkladem topologického prostoru může být libovolná množina T spolu s nejmenším možným systémem $\tau = \{\emptyset, T\}$, který nazýváme *triviální* topologií. Pokud naopak zvolíme největší možný systém, tj. $\tau = 2^T$, kde 2^T označuje potenční množinu množiny T, dostáváme *diskrétní* topologii.

Místo zápisu dvojice (T, τ) budeme v textu využívat i kratšího označení T. Vždy však uvedeme, že zápisem T je myšlen topologický prostor.

Definice 5.2. Nechť (T, τ) je topologický prostor. *Bází* $\mathcal{B}$ nazýváme takový podsystém topologie τ, jestliže každá množina z τ je sjednocením nějakých množin z $\mathcal{B}$. Topologie τ se pak nazývá *generovaná* bází $\mathcal{B}$. Každá báze ovšem generuje pouze jedinou topologii. Zdroj viz skriptum [**?**].

Definice 5.3. Nechť (T, τ), (S, σ) jsou topologické prostory. *Součinovou topologií* $\tau \times \sigma$ na $T \times S$ rozumíme topologii generovanou bází

$$\mathcal{B} = \{U \times V;\ U \in \tau, V \in \sigma\}$$

Definice 5.4. Nechť (T, τ), (S, σ) jsou topologické prostory. *Součinem topologických prostorů* $(T, \tau) \times (S, \sigma)$ rozumíme kartézský součin $T \times S$ vybavený součinovou topologií $\tau \times \sigma$.

Obecnější formulace uvedena v [13].

Definice 5.5. Topologický prostor (T, τ) nazýváme *souvislý*, jestliže T nemůže být vyjádřeno jako sjednocení dvou disjunktních otevřených množin v dané topologii τ. Pokud platí opačné tvrzení, nazýváme prostor *nesouvislý*.

Definice 5.6. Uvažujme topologický prostor (T, τ). Množinu $S \subseteq T$ nazýváme *kompaktní*, jestliže každé otevřené pokrytí obsahuje konečné podpokrytí.

Poznámka 5.1. Definice otevřeného pokrytí a podpokrytí čtenář snadno vyhledá v publikacích o topologii, či na internetu.

Definice 5.7. Topologický prostor (T, τ) nazýváme *Hausdorffův* nebo s *Hausdorffovou strukturou*, jestliže pro dva různé prvky $t_1, t_2 \in T$ existují disjunktní otevřené množiny $U_1, U_2 \in \tau$ takové, že $t_1 \in U_1$ a $t_2 \in U_2$.

Definice 5.8. Nechť (T, τ) je topologický prostor a dále $\sim$ je relací ekvivalence na T. *Faktorovým prostorem* $T/\sim$ rozumíme množinu všech tříd ekvivalence T danou $\sim$.

Na faktorovém prostoru $T/\sim$ lze zavést *faktorovou topologii* jako topologii, tvořenou množinami $U \subseteq T/\sim$ takovými, že jejich sjednocení je otevřená množina v T (viz [14]).

Zápisem T/Γ, kde $\Gamma \subseteq T$, rozumíme faktorový prostor tvořený třídami, v kterých ztotožníme všechny prvky množiny Γ.

5.1 Homeomorfismus

Definice 5.9. Zobrazení $f : T \to S$ mezi dvěma topologickými prostory (T, τ) a (S, σ) se nazývá *homeomorfismus*, jestliže má následující vlastnosti

(i) f je bijekce.

(ii) f je spojité.

(iii) f^{-1} je spojité.

Zobrazení f s těmito vlastnostmi se často označuje jako *bi-spojité* nebo také jako *topologický izomorfismus*. Dále řekneme, že dva topologické prostory jsou *homeomorfní*, jestliže mezi nimi existuje homeomorfismus.

Zkoumáme-li vztahy mezi topologickými prostory, zjišťujeme, že homeomorfismus zachovává topologické vlastnosti stejně jako izomorfismus grup zachovává algebraickou strukturu a vlastnosti grupy. Můžeme tedy říci, že dva homeomorfní prostory jsou topologicky ekvivalentní. Věnujme se nyní precizněji vlastnostem homeomorfismu.
Uvažujme homeomorfismus $f : S \to T$ mezi topologickými prostory (S, τ_S) a (T, τ_T), potom f zachovává

(a) kompaktnost,

(b) souvislost,

(c) Hausdorffovu strukturu,

(d) fundamentální grupu.

Příklad 5.1. (Homeomorfismus)

- Otevřený interval $(-1, 1)$ je homeomorfní s $\mathbb{R}$. Bi-spojitá funkce je dána vztahem

$$f(x) = \operatorname{tg}\left(\frac{\pi}{2}x\right).$$

- Jednotková kružnice a jednotkový čtverec v rovině jsou homeomorfní.

- Sféra $\mathbb{S}^n$ s jedním vyjmutým bodem je homeomorfní s $\mathbb{R}^n$.
  Homeomorfismus je dán jako stereografická projekce, viz příklad (5.4).

- $\mathbb{R}^m$ a $\mathbb{R}^n$ jsou homeomorfní jen pro $m = n$.
  Jako příklad si nejdříve vezměme funkci $f : \mathbb{R} \to \mathbb{R}^2$ a předpokládejme opak. Tedy, že prostory $\mathbb{R}$ a $\mathbb{R}^2$ jsou homeomorfní. Definujme, že bod $0 \in \mathbb{R}$ se zobrazí na počátek soustavy souřadnic $(0, 0) \in \mathbb{R}^2$. Nyní bychom museli nesouvislou množinu $\mathbb{R} \setminus \{0\}$ zobrazit na $\mathbb{R}^2 \setminus \{(0, 0)\}$, která ovšem souvislá je. Z poznatku, že homeomorfismus zachovává souvislost, dostáváme rozpor a tedy $\mathbb{R}$ a $\mathbb{R}^2$ nemohou být homeomorfní.
  Podobně můžeme obecně dokázat, že prostory $\mathbb{R}^m$ a $\mathbb{R}^n$ nejsou homeomorfní pro $m \neq n$.

5.2 Homotopie

Možným způsobem jak zkoumat topologické prostory je sledovat jak se mohou deformovat jednotlivé oblouky v prostoru do jiných. Disciplínou zabývající se touto problematikou je teorie homotopií (viz [3]), která umožňuje zkoumat souvislost topologických prostorů v jiném pojetí. Přistupme nejdříve k definici oblouku.

Definice 5.10. Uvažujme topologický prostor (T, τ). *Obloukem* $\gamma(s)$ s počátkem v bodě $x_0 \in T$ a koncem v bodě $x_1 \in T$ rozumíme spojité zobrazení

$$\gamma : \langle 0, 1\rangle \to T$$

takové, že

$$\gamma(0) = x_0 \quad \wedge \quad \gamma(1) = x_1$$

Se zavedením pojmu oblouku můžeme definovat nové pojetí souvislosti prostoru.

Řekneme, že topologický prostor T je *obloukově souvislý*, jestliže vždy existuje oblouk $\gamma(s)$ mezi libolnými body $x_0, x_1 \in T$. Platí věta, že každý obloukově souvislý topologický prostor je souvislý, avšak neplatí obrácená implikace. Protipříkladem může být tzv. topologický sinus, neboli prostor T s topologií τ indukovanou $\mathbb{R}^2$, kde T je definovaný jako graf funkce $f(x) = \sin(\frac{1}{x})$ spolu s bodem $(0, 0) \in \mathbb{R}^2$. Není totiž možné vytvořit oblouk z bodu $(0, 0)$ do bodu funkce $f(x)$.

Definujme dále skládání oblouků následovně.

Definice 5.11. Uvažujme dva oblouky α, β takové, že $\alpha(1) = \beta(0)$. *Složením* oblouků α, β nazveme oblouk $\gamma(s)$ takový, že

$$\gamma(s) = \alpha(s) \circ \beta(s) = \begin{cases} \alpha(2s), & 0 \leq s \leq \frac{1}{2} \\ \beta(2s - 1), & \frac{1}{2} \leq s \leq 1 \end{cases}$$

Složení oblouků jako operace není asociativní, avšak pomocí reparametrizace lze asociativity dosáhnout. Dostáváme se tak již k aparátu, jak popsat spojité deformace jednoho oblouku na druhý.

Pokud nyní vezmeme speciální oblouky α, β takové, že $\alpha(0) = \beta(0)$ a $\alpha(1) = \beta(1)$, tj. oblouky se splývajícími krajními body, můžeme již zavést speciální relaci mezi oblouky.

Definice 5.12. Uvažujme topologický prostor T a definujme relaci $\alpha \sim \beta$ (α *je homotopický s* β), pokud se α dá spojitě deformovat do β při pevných koncích, tj. existuje-li zobrazení $\Phi : \langle 0,1\rangle \times \langle 0,1\rangle \to T$ takové, že

$$\begin{aligned} \Phi(s,0) = \alpha(s) \quad &\wedge \quad \Phi(s,1) = \beta(s) \\ \Phi(0,t) = \alpha(0) = \beta(0) \quad &\wedge \quad \Phi(1,t) = \alpha(1) = \beta(1) \end{aligned}$$

Takovou spojitou deformaci z oblouku α do β nazýváme *homotopií*.

5.2.1 Fundamentální grupa

Zabývejme se nyní důležitou skupinou oblouků, které nazýváme *smyčky*. Uvažujeme tedy takové oblouky γ, pro které platí $\gamma(0) = \gamma(1) = P \in T$. Bod P pak nazveme *bázovým bodem* smyčky γ.

Homotopie je relace ekvivalence na množině všech smyček z topologického prostoru T a tedy indukuje rozpad do tříd ekvivalence, které označíme $[\gamma]$. V každé třídě $[\gamma]$ jsou tedy všechny smyčky $\gamma(t)$, které jsou navzájem homotopické. Na množině všech homotopických tříd smyček lze zavést operaci skládání $\circ$ stejně, jako skládání smyček. Nechť $[\alpha], [\beta]$ jsou třídy smyček s bázovým bodem P, pak

$$[\alpha] \circ [\beta] = [\alpha \circ \beta]$$

Definice 5.13. Uvažujme topologický prostor (T, τ). Množina všech tříd ekvivalence homotopie smyček s bázovým bodem P spolu s operací skládání $\circ$ tvoří grupu, kterou nazýváme *fundamentální grupa* a značíme ji

$$(\pi_1(T,P), \circ) = (\{[\gamma];\ \gamma(s) \text{ je smyčka v } T \text{ s bázovým bodem } P\}, \circ)$$

Poznámka 5.2. K důkazu. K ověření asociativity využijeme vlastnosti, že reparametrizace oblouku (smyčky) je speciálním případem homotopie. Neutrálním prvkem je třída smyček $[\epsilon]$, kde $\epsilon(s) = P$, $0 \leq s \leq 1$, což je smyčka stažená do jednoho bodu. Dále inverzním prvkem ke každé třídě smyček $[\gamma]$ je třída $[\gamma^{-1}]$, kde γ^{-1} je smyčka parametrizovaná v opačném směru.

Dá se ukázat, že na volbě bázového bodu P nezáleží. Důvodem je fakt, že pokud vezmeme dvě fundamentální grupy $\pi_1(T,P)$ a $\pi_1(T,Q)$, kde P, Q jsou různé bázové body, potom grupy $\pi_1(T,P)$ a $\pi_1(T,Q)$ jsou izomorfní. Stačí tedy označovat fundamentální grupu [5] jako $\pi_1(T)$.

[5] Fundamentální grupa je označována také jako *první homotopická grupa*, z čehož plyne index 1 u označení π_1. Zobecnění je možné nalézt např. v [3].

Příklad 5.2.

- Již intuitivně je jasné, že každou smyčku v eukleidovských prostorech $\mathbb{R}^n$ můžeme stáhnout do jednoho bodu, tudíž jsou $\mathbb{R}^n$ homotopicky triviální, tj. $\pi_1(\mathbb{R}^n) = [\epsilon]$.
- Za prostor T zvolme kružnici $\mathbb{S}^1$. Označme $\gamma_n(s), n \in \mathbb{Z}$ smyčku, která se pro $n > 0$ obtočí n krát doleva okolo kružnice $\mathbb{S}^1$ a pro $n < 0$ se obtočí $|n|$ krát doprava. Pro $n = 0$ je $\gamma_n(s) = \epsilon$. Dostáváme tedy systém tříd $[\gamma_n], n \in \mathbb{Z}$ a pro kompozici tříd smyček $\circ$ platí
$$[\gamma_n] \circ [\gamma_m] = [\gamma_{n+m}].$$
Tedy $\pi_1(\mathbb{S}^1) = (\{[\gamma_n], n \in \mathbb{Z}\}, \circ)$. S využitím izomorfismu $[\gamma_n] \in \pi_1(\mathbb{S}^1) \to n \in \mathbb{Z}$ můžeme psát přímo $\pi_1(\mathbb{S}^1) = \mathbb{Z}$.

Věta 5.1. Nechť (T, τ) a (S, σ) jsou topologické prostory a $\pi_1(T)$, $\pi_1(S)$ příslušné fundamentální grupy. Potom platí
$$\pi_1(T \times S) = \pi_1(T) \oplus \pi_1(S)$$

Důkaz 5.1. Počítáme $\pi_1(T \times S) = \pi_1(\{[\gamma];\ \gamma(t,s), t \in T, s \in S\})$ a díky homotopii můžeme popisovat smyčky jen jako zobrazení buď proměnné t nebo s a tedy můžeme psát
$$\pi_1(\{[\gamma];\ \gamma(t,s), t \in T, s \in S\}) = \{([\gamma_1], [\gamma_2]);\ [\gamma_1] \in \pi_1(T), [\gamma_2] \in \pi_1(S)\} = \pi_1(T) \oplus \pi_1(S)$$
Přímý součet grup zde splývá s kartézským součinem množin.

Přistupme k výpočtu fundamentální grupy toru[6] $\mathcal{T}^2$. S využitím znalosti $\pi_1(\mathbb{S}^1) = \mathbb{Z}$ můžeme fundamentální grupu prostoru $\mathcal{T}^2$ spočíst podle věty (5.1) následovně
$$\pi_1(\mathcal{T}^2) = \pi_1(\mathbb{S}^1 \times \mathbb{S}^1) = \mathbb{Z} \times \mathbb{Z}$$
Množina tříd homotopií smyček na toru je tedy izomorfní s $\mathbb{Z} \times \mathbb{Z}$ a tedy každou smyčku na toru můžeme popisovat pomocí dvojice celých čísel, kde první (druhé) celé číslo udává počet obtočení smyčky okolo první (druhé) kružnice $\mathbb{S}^1$ a znaménko určuje smysl otáčení.

5.3 Hladké variety

Objektem zájmu této podkapitoly bude zavedení nových struktur k topologickým prostorům. Zaměříme se nejdříve na topologické variety, jejichž vlastností je „lokální podobnost“ s prostorem $\mathbb{R}^n$, kterou přesněji vymezíme v následující definici.

Definice 5.14. *Topologickou varietou dimenze n* nazýváme takový Hausdorffův topologický prostor (T, τ) se spočetnou bází, jestliže ke každému bodu $t \in T$ existuje jeho okolí $O(t)$, které je homeomorfní s $\mathbb{R}^n$.

Ekvivalentně také pro každé $t \in T$ můžeme najít otevřenou množinu $U \subseteq T$ obsahující t, dále otevřenou množinu $\bar{U} \subseteq \mathbb{R}^n$ a homeomorfismus $f : U \to \bar{U}$.

[6] Zavedení toru viz definice (5.19).

Poznámka 5.3. V textu budeme často využívat označení *topologická varieta* místo topologická varieta dimenze n.

Ke studiu funkcí na topologikých varietách je třeba přidat navíc, tzv. C^∞-strukturu k jejich topologii.

Definice 5.15. Nechť (T, τ) je topologická varieta dimenze n. *Mapou* $\mathcal{C}$ na topologické varietě (T, τ) nazýváme dvojici (U, ϕ) splňující

(i) $U \in \tau$, $\quad$ (U je otevřená množina v T)

(ii) $\phi : T \to \mathbb{R}^n$ je homeomorfismus, $\quad$ ($\phi(U)$ je otevřená množina v $\mathbb{R}^n$)

Při zadané mapě $\mathcal{C} = (U, \phi)$ definujme *souřadnice* bodu $P \in U \subset T$ jako kartézské souřadnice bodu $\phi(P) \in \phi(U) \subset \mathbb{R}^n$. Složky $\phi(P)$, kde $P \in U$ definují množinu n reálných funkcí na otevřené množině U, které nazýváme *funkce souřadnic*.

Nyní jsme schopni přenášet části topologických prostorů do známého prostoru $\mathbb{R}^n$. Chtěli bychom však pomocí map pokrýt celý prostor T. Je zřejmé, že pokud systém otevřených množin U má být pokrytím T, budou se množiny U map $\mathcal{C}$ překrývat. Tímto jsme vedeni k následující definici.

Definice 5.16. Nechť $\mathcal{C}_1 = (U_1, \phi_1)$ a $\mathcal{C}_2 = (U_2, \phi_2)$ jsou mapy na topologické varietě (T, τ). Potom $\mathcal{C}_1$ a $\mathcal{C}_2$ nazveme C^∞*-slučitelné*, jestliže

(i) U_1 a U_2 jsou disjunktní nebo platí

(ii) zobrazení $\phi_1 \circ \phi_2^{-1} : \phi_2(U_1 \cap U_2) \to \phi_1(U_1 \cap U_2)$ a $\phi_2 \circ \phi_1^{-1} : \phi_1(U_1 \cap U_2) \to \phi_2(U_1 \cap U_2)$ jsou libovolně hladké funkce, čili třídy C^∞.

Obrazy funkcí $\phi_1(U_1)$ i $\phi_2(U_2)$ jsou části prostoru $\mathbb{R}^n$ a funkce $\phi_1 \circ \phi_2^{-1}$ a $\phi_2 \circ \phi_1^{-1}$ nazýváme *přechodové funkce*, což jsou reálné funkce n proměnných.

Již je vše přichystáno k vytvoření systému map, které pokryjí celý prostor T.

Definice 5.17. C^∞*-atlasem* $\mathcal{A}$ topologické varietě (T, τ) rozumíme systém map $\mathcal{C}_i = (U_i, \phi_i)$, kde i probíhá nějakou indexovou množinu I a platí, že systém U_i tvoří pokrytí T a všechny mapy $\mathcal{C}_i$ jsou vzájemně C^∞-slučitelné.

Mapu $\mathcal{C} = (U, \phi)$ na topologické varietě (T, τ) nazýváme *kompatibilní s* C^∞*-atlasem* $\mathcal{A}$, jestliže po přidání mapy $\mathcal{C}$ k atlasu $\mathcal{A}$ vzniká opět C^∞-atlas. *Maximálním* C^∞*-atlasem* $\mathcal{A}_{\max}$ nebo také *hladkou* C^∞*-strukturou na* T pak rozumíme takový C^∞-atlas, který obsahuje všechny mapy s ním kompatibilní.

Vyvrcholením této kapitoly je zavedení pojmu hladké variety pomocí topologické variety a systému map na ní zavedených.

Definice 5.18. *Hladkou varietou* nebo jen *varietou* rozumíme dvojici $(T, \mathcal{A}_{\max})$, kde (T, τ) je topologická varieta a $\mathcal{A}_{\max}$ je maximální C^∞-atlas.

Věta 5.2. Nechť (T, τ) je topologická varieta, potom platí následující tvrzení. Každý C^∞-atlas $\mathcal{A}$ na (T, τ) je obsažen v jediném maximálním C^∞-atlasu $\mathcal{A}_{\max}$.

Důkaz 5.2. Důkaz je uveden v [5].

Poznámka 5.4. Využijeme-li k zavedení hladké variety map, které jsou C^r-slučitelné, kde $r \in \mathbb{R}$, neboli přechodové funkce jsou třídy C^r, dostáváme tak širší skupinu vhodných map a zavedení hladké variety proběhne stejným způsobem od definice 5.15 do 5.18.

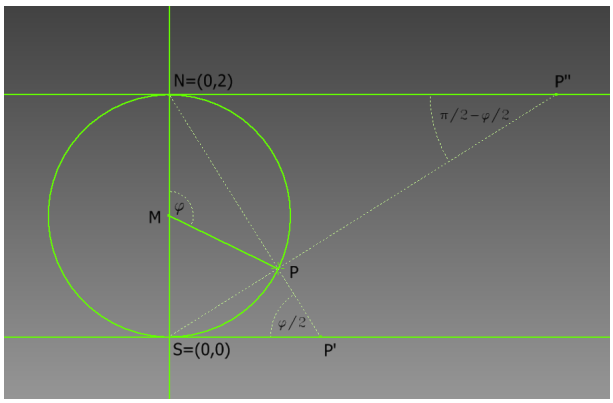
Stačí nám tedy na topologické varietě (T, τ) zadat nějaký C^∞-atlas a okamžitě tak dostáváme hladkou C^∞-strukturu na T.

Příklad 5.3. Prostor $\mathbb{R}^n$ spolu s atlasem, který obsahuje jen jednu mapu $\mathcal{C} = (U, i_{\mathbb{R}^n})$, kde $i_{\mathbb{R}^n}$ je identita na $\mathbb{R}^n$, je hladkou varietou.

Příklad 5.4. Pro n-sféru $\mathbb{S}^n$

$$\mathbb{S}^n = \left\{ \mathbf{x} = (x_1, x_2, \ldots, x_{n+1}) \in \mathbb{R}^{n+1}; \sum_{i=1}^{n+1} x_i^2 = 1 \right\}$$

již není možné zavést jedinou mapu, která by ji pokrývala celou. Je však možné ukázat, že $\mathbb{S}^n$ je varieta s pomocí dvou stereografických projekcí, které mapují otevřené množiny $U_1 = \mathbb{S}^n \setminus \{N\}$ a $U_2 = \mathbb{S}^n \setminus \{S\}$ na $\mathbb{R}^n$, kde N je severní a S jižní pól sféry. Provedeme konstrukci zobrazení jen pro $n = 1$, viz obrázek 20.



Obrázek 20: Stereografické projekce ze severního i jižního pólu

Označme r jako vzdálenost bodů M a P. První mapu $\mathcal{C}_1 = (U_1, \phi_1)$ dostáváme projekcí ze severního pólu N, kde zobrazení $\phi_1 : U_1 \to \mathbb{R}$ mapující bod $P \in \mathbb{S}^1$ na $P' \in \mathbb{R}$, který leží na reálné přímce $y = 0$, je dáno následovně

$$x = \frac{2r}{\operatorname{tg} \frac{\varphi}{2}}, \quad \varphi \neq 0 \tag{5.8}$$

Druhou mapu $\mathcal{C}_2 = (U_2, \phi_2)$ obdržíme projekcí z jižního pólu S, kde podle obr.20 dostáváme $\phi_2 : U_2 \to \mathbb{R}$, které mapuje P na bod $P'' \in \mathbb{R}$, ležící na přímce $y = 2$.

$$x = \frac{2r}{\operatorname{cotg} \frac{\varphi}{2}} = 2r \operatorname{tg} \frac{\varphi}{2}, \quad \varphi \neq \pi \tag{5.9}$$

Výpočtem přechodových funkcí $\phi_1 \circ \phi_2^{-1} : \mathbb{R} \to \mathbb{R}$ a $\phi_2 \circ \phi_1^{-1} : \mathbb{R} \to \mathbb{R}$ ověříme, že mapy $\mathcal{C}_1$ a $\mathcal{C}_2$ jsou C^∞-slučitelné. Využijeme inverzí $\phi_1^{-1} : (0, 2\pi) \to \mathbb{S}^1$ a $\phi_2^{-1} : (-\pi, \pi) \to \mathbb{S}^1$ a dostáváme pro obě přechodové funkce

$$\phi_1 \circ \phi_2^{-1}(x) = \phi_2 \circ \phi_1^{-1}(x) = \frac{4r^2}{x}, \quad x \neq 0$$

Přechodové funkce jsou tedy na $\mathbb{R} \setminus \{0\}$ jistě třídy C^∞. Vzniká tak C^∞-atlas $\mathcal{A} = \{\mathcal{C}_1, \mathcal{C}_2\}$, jenž je podle věty (5.2) obsažen v jediném maximálním C^∞-atlasu, který spolu s prostorem $\mathbb{S}^1$ tvoří hladkou varietu.

Dalším významným příkladem hladké variety je právě torus, jehož definici z pohledu topologie uvádíme nyní.

Definice 5.19. 2-*torus* nebo jen *torus* $\mathcal{T}^2$ definujeme jako součin topologických prostorů dvou 1-sfér

$$\mathcal{T}^2 = \mathbb{S}^1 \times \mathbb{S}^1.$$

Označme dvě 1-sféry $\mathbb{S}^1_1$ a $\mathbb{S}^1_2$. Ukážeme, že torus $\mathcal{T}^2$ jako součin topologických prostorů je hladkou varietou dimenze 2. Využijeme příkladu (5.4), kde jsme prokázali, že $\mathbb{S}^1 \subseteq \mathbb{R}^2$ s topologií zděděnou z $\mathbb{R}^2$ je Hausdorffův prostor se spočetnou bází.

Pro libovolný bod $P = (p_1, p_2) \in \mathcal{T}^2$ najdeme dvojici otevřených množin (U_1, U_2), kde $U_1 \subset \mathbb{S}^1_1$ a $U_2 \subset \mathbb{S}^1_2$ a zvolíme vhodnou dvojici stereografických projekcí z (5.8) nebo (5.9) jako funkcí $f_i : U_i \to \bar{U}_i$, kde $\bar{U}_i \subseteq \mathbb{R}$, $i = 1, 2$. Dostáváme tak zobrazení

$$f = f_1 \times f_2 : U_1 \times U_2 \to \mathbb{R} \times \mathbb{R},$$

kde funkce f je homeomorfismus po složkách. Topologický prostor $\mathbb{S}^1_1 \times \mathbb{S}^1_2$ je tedy topologickou varietou dimenze 2.

Pro zavedení hladké C^∞-struktury na toru je třeba prokázat, že libovolné dvě mapy $\mathcal{C}_1 = (U_1 \times U_2, f_1 \times f_2)$ a $\mathcal{C}_2 = (V_1 \times V_2, g_1 \times g_2)$ jsou C^∞-slučitelné, kde $U_1 \times U_2, V_1 \times V_2 \in \mathcal{T}^2$ a $f = f_1 \times f_2, g = g_1 \times g_2$ jsou příslušné homeomorfismy. Přechodová funkce $f \circ g^{-1}$

$$f \circ g^{-1} = (f_1 \times f_2) \circ (g_1 \times g_2)^{-1} = (f_1 \circ g_1^{-1}) \times (f_2 \circ g_2^{-1})$$

je po složkách funkcí třídy C^∞. Pro přechodovou funkci $g \circ f^{-1}$ postupujeme obdobně.

Tím jsme zavedli C^∞-atlas na toru a využitím věty (5.2) dostáváme C^∞-strukturu na toru. Získáváme tak ucelený přehled o topologických vlastnostech toru.

Poznámka 5.5. (Označení) V literatuře se často uvádí definice *n-toru* $\mathcal{T}^n$ jako součinu n 1-sfér. Vystačíme však s definicí jen pro torus dimenze 2. V dalším textu sjednotíme označení a pro zjednodušení budeme psát jen $\mathcal{T}$ místo $\mathcal{T}^2$.

6 Izometrie a algebraická definice toru

Předmětem zájmu této kapitoly bude zejména speciální typ zobrazení reálné roviny $\mathbb{R}^2$ opět na reálnou rovinu a význam takového zobrazení při studiu dvourozměrných variet. Na $\mathbb{R}^2$ měříme přirozeně vzdálenost mezi body $P = (x_1, y_1)$ a $Q = (x_2, y_2)$ pomocí eukleidovské metriky $\rho(P, Q)$, která je dána

$$\rho(P, Q) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

Reálná rovina $\mathbb{R}^2$ spolu s metrikou $\rho(P, Q)$ tvoří metrický prostor.

Definice 6.1. Zobrazení $f : \mathbb{R}^2 \to \mathbb{R}^2$ nazýváme *izometrie*, právě když zachovává vzdálenost $\rho(P, Q)$, tj. platí

$$\rho(f(P), f(Q)) = \rho(P, Q), \quad \forall P, Q \in \mathbb{R}^2$$

Na reálnou rovinu je možné nahlížet jako na prostor komplexních čísel $\mathbb{C}$. Vyjádření izometrií pomocí funkcí komplexní proměnné zjednodušuje výrazy a usnadňuje výpočet, proto v dalším textu využijeme těchto výhod a příklady izometrií a některé další výpočty uvedeme v komplexní aritmetice. Klasické vyjádření je možno vyhledat např. v [2].

Základními izometriemi jsou

1. *Posunutí* bodu $z \in \mathbb{C}$ o $c = (a + bi) \in \mathbb{C}$ je dáno funkcí $p_c(z) = p_{a+bi}(z)$

   $$p_{a+bi}(z) = a + bi + z$$

2. *Zrcadlení* bodu $z \in \mathbb{C}$ okolo reálné osy v Gaussově rovině je dáno funkcí $\overline{r}(z)$

   $$\overline{r}(z) = \overline{z},$$

   kde $\overline{z}$ značí číslo komplexně sdružené k z.

3. *Otočení* bodu $z \in \mathbb{C}$ okolo počátku soustavy souřadnic o úhel θ je dáno funkcí $o_\theta(z)$

   $$o_\theta(z) = e^{i\theta} z = (\cos\theta + i \sin\theta)\, z$$

Jestliže f a g jsou izometrie, pak také jejich složení fg je izometrie a je definováno jako obvyklé skládání zobrazení, tedy f po g. Nyní je možné uvažovat systémy různých izometrií a zapojit prostředky teorie grup.

Věta 6.1. Množina všech posunutí $\mathcal{P} = \{p_c;\ c \in \mathbb{C}\}$ v reálné rovině tvoří grupu.

Důkaz 6.1. V každém ze tří kroků důkazu předpokládejme bod $z \in \mathbb{C}$, na který aplikujeme posunutí.

a) (Asociativita) Uvažujme posunutí $p_c, p_d, p_e \in \mathcal{P}$ a dostáváme
$p_c(p_d p_e) \Rightarrow z \xrightarrow{p_e} z + e \xrightarrow{p_d} z + e + d \xrightarrow{p_c} z + e + d + c$,
$(p_c p_d)p_e \Rightarrow z \xrightarrow{p_d} z + d \xrightarrow{p_c} z + d + c \xrightarrow{p_e} z + d + c + e$,
díky komutativitě komplexních čísel platí $p_c(p_d p_e) = (p_c p_d)p_e$.

b) (Ex. neutrálního prvku) Pro každé posunutí p_c existuje nulové posunutí $0_p = p_{0+0\imath}$,
$0_p p_c \Rightarrow z \xrightarrow{p_c} z + c \xrightarrow{0_p} z + c$
$p_c 0_p \Rightarrow z \xrightarrow{p_0} z \xrightarrow{p_c} z + c.$
Platí tedy $0_p p_c = p_c 0_p = p_c$.

c) (Ex. inverzního prvku) Pro každé posunutí p_c existuje inverze $p_c^{-1} = p_{-c}$,
$p_c p_c^{-1} \Rightarrow z \xrightarrow{p_c^{-1}} z - c \xrightarrow{p_c} z$
$p_c^{-1} p_c \Rightarrow z \xrightarrow{p_c} z + c \xrightarrow{p_c^{-1}} z$
a dostáváme $p_c p_c^{-1} = p_c^{-1} p_c = 0_p$.

6.1 Faktorové prostory

Povšimněme si, že některé známé geometrické útvary v třírozměrném prostoru je možné vytvořit různým „slepením“ reálné roviny $\mathbb{R}^2$. Navíc pro popis těchto objektů je důležité, abychom zachovali vlastnost lokální podobnosti s $\mathbb{R}^2$. Takovým útvarem je například válec. Stačí vzít proužek $\mathbb{R}^2$, řekněme všechny body mezi přímkami $x = 0$ a $x = 1$, včetně těchto přímek a ztotožnit dvojice bodů $(0, y)$ s $(1, y)$. Tím dochází ke spojení konců proužku a výsledný prostor si můžeme představovat jako válec o neomezené délce. Avšak nabízí se lepší způsob jak zkonstruovat válec, neboť výběr proužku byl náhodný z mnoha variant a výběr zahrnuje jen část reálné roviny. V dalším textu prostudujeme tento přístup a popíšeme vzniklé prostory.

Způsobem, jak algebraicky popsat zmíněný proces, je definovat nově vzniklé prostory jako faktorové prostory dané faktorizací reálné roviny $\mathbb{R}^2$ a množiny izometrií Γ. Pro tyto prostory zaveďme označení $\mathcal{S} = \mathbb{R}^2/\Gamma$. Prvky prostorů $\mathcal{S}$ jsou množiny bodů $P \in \mathbb{R}^2$, které jsou nějakým způsobem ztotožněny.

Prvky $s \in \mathcal{S}$ jsou tedy systémy bodů z reálné roviny $\mathbb{R}^2$, které budeme nazývat Γ-*orbity bodu* $P = (x, y) \in \mathbb{R}^2$. Takové prvky označíme zkráceně ΓP, kde

$$\Gamma P = \{g(P);\ g \in \Gamma\}.$$

Zobrazení, které ke každému bodu $P = (x, y) \in \mathbb{R}^2$ přiřadí jeho Γ-orbitu, nazýváme *orbitální zobrazení*.

Ke kompletnímu popisu prostorů $\mathcal{S}$ je nutné připojit význam vzdálenosti na těchto prostorech. Díky definování $\mathcal{S}$ jako faktorového prostoru se zachovává lokální podobnost s reálnou rovinou a lokálně také můžeme měřit vzdálenosti pomocí aparátu zděděného z $\mathbb{R}^2$. Zavádíme pro prostor $\mathcal{S}$ funkci $d_{\mathcal{S}} : \mathcal{S}^2 \to \mathbb{R}^2$ takto

$$d_{\mathcal{S}}(\Gamma P, \Gamma Q) = \min\{\rho(P', Q');\ P' \in \Gamma P,\ Q' \in \Gamma Q\},$$

kde ρ je eukleidovská metrika.

Pro názornost můžeme prostor $\mathcal{S}$ vizualizovat v části reálné roviny, která obsahuje nejvýše jednoho reprezentanta každé Γ-orbity ve svém vnitřku. Takovou část roviny budeme nazývat *základní oblast*.

Dokončeme příklad z úvodu této podkapitoly. Pro algebraickou konstrukci válce $\mathcal{V}$ zvolíme za Γ grupu všech celočíselných posunutí v reálné ose x, tj. $\Gamma = \{p_{n+0i};\, n \in \mathbb{Z}\}$. Můžeme proto psát $\mathcal{V} = \mathbb{R}^2/\Gamma$. Každý bod válce $v \in \mathcal{V}$ je tedy dán jako systém bodů

$$v = \left\{(x+n, y) \in \mathbb{R}^2;\, n \in \mathbb{Z}\right\},$$

což je stejná Γ-orbita pro všechny body $(x+n, y) \in \mathbb{R}^2$, kde volíme n. Dochází tedy k identifikaci bodů v reálné rovině a takový proces si můžeme představovat, jako bychom srolovali celou rovinu až do tvaru válce. Základní oblastí může být například proužek reálné roviny mezi přímkami $x = 0$ a $x = 1$.

Na torus může být nyní nahlíženo jako na plochu, která vznikne srolováním reálné roviny do válce a navíc spojením protějších konců. Můžeme proto uvažovat obecně o toru[7] jako o faktorovém prostoru $\mathcal{T} = \mathbb{R}^2/\Gamma$, kde Γ je grupa generovaná posunutími v různých směrech p_a a p_b. Čili základní oblastí pro torus $\mathcal{T}$ by byl libovolný rovnoběžník.

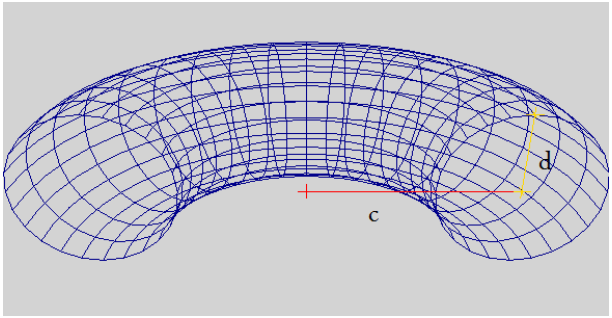
[7] Vzhledem k uvedené konstrukci válce $\mathcal{V}$ je možné definovat torus $\mathcal{T}$ také jako faktorizaci $\mathcal{V}/\Gamma$, kde Γ je grupa posunutí, avšak ve směru různém od posunutí prvního.

7 Geometrie toru

Pro praktickou implementaci a vizualizaci budeme využívat geometrického popisu toru $\mathcal{T} \subset \mathbb{R}^3$ jako plochy $f(r, s)$ v $\mathbb{R}^3$, která je popsána pomocí parametrických rovnic

$$\begin{aligned} x &= (c + d\cos s)\cos r \\ y &= (c + d\cos s)\sin r \\ z &= d\sin s \end{aligned} \tag{7.10}$$

Parametry zobrazení jsou $r, s \in (-\pi, \pi)$ a dále volitelné $c, d \in \mathbb{R}$, pro které platí $c > d$. Toto je přirozená podmínka, pokud chceme zachovat topologické vlastnosti. Pevně dané c a d totiž určují poloměry kružnic znázorněných na obrázku 21.



Obrázek 21: Pevné parametry c a d

7.1 Transformace reálné roviny

K přenesení libovolných geometrických útvarů z reálné roviny na torus využijeme jeho parametrických rovnic. Tedy obecně pracujeme se zobrazením $f : \mathbb{R}^2 \to \mathbb{R}^3$. Avšak abychom mohli využít parametrizace toru, bude třeba zobrazení zúžit na $f : (-\pi, \pi)^2 \to \mathbb{R}^3$, čili z reálné roviny vyjmeme otevřený čtverec $(-\pi, \pi) \times (-\pi, \pi)$, který je reprezentativní oblastí celé reálné roviny. Než funkci f využijeme, je třeba ještě nalézt vhodné transformace reálné roviny obecně na oblast jednotkového otevřeného čtverce $\mathbb{I}^2$

$$\mathbb{I}^2 = \left\{\mathbf{x} \in \mathbb{R}^2;\ 0 < x_i < 1\right\},$$

z kterého již lineární transformací stejnolehlosti můžeme snadno dostat požadovanou oblast čtverce $(-\pi, \pi) \times (-\pi, \pi)$.

V programové implementaci však využijeme přímo transformace reálné roviny na čtverec $(-\pi, \pi)^2$. Zkonstruujme tedy pro celou reálnou rovinu $\mathbb{R}^2$ funkci $g : \mathbb{R}^2 \ni (x, y) \mapsto (r, s) \in (-\pi, \pi)^2$ následovně

$$r = 2\operatorname{arctg} x \tag{7.11}$$

$$s = 2\operatorname{arctg} y, \tag{7.12}$$

kde $x, y \in \mathbb{R}$ a $r, s \in (-\pi, \pi)$.

Funkce g je zřejmě spojitá a zároveň bijekcí a inverze g^{-1}

$$x = \operatorname{tg} \frac{r}{2} \tag{7.13}$$

$$y = \operatorname{tg} \frac{s}{2}, \tag{7.14}$$

je spojitá pro $(\frac{r}{2}, \frac{s}{2}) \in (-\frac{\pi}{2}, \frac{\pi}{2})$. Funkce g je tedy homeomorfismus mezi topologickými prostory $\mathbb{R}^2$ a $(-\pi, \pi)^2$ a tyto prostory jsou topologicky ekvivalentní.

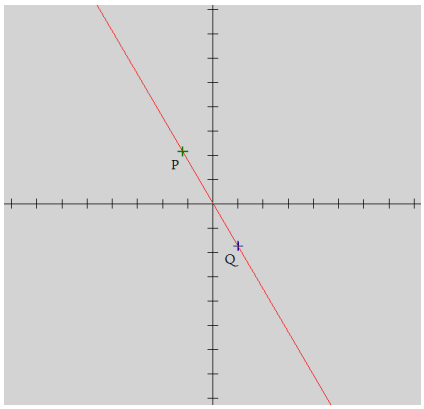
Uvažujme nyní množinu $X_1 \subseteq \mathbb{R}^2$ a zúžení zobrazení g na podmnožinu X_1 označme $h = g|_{X_1}$. Zvolme za X_1 nejdříve přímku procházející body $P = (p_1, p_2), Q = (q_1, q_2) \in \mathbb{R}^2$. Máme tedy množinu

$$X_1 = \left\{(x, y) \in \mathbb{R}^2;\ -(q_2 - p_2)x + (q_1 - p_1)y + p_1 q_2 - p_2 q_1 = 0\right\},$$

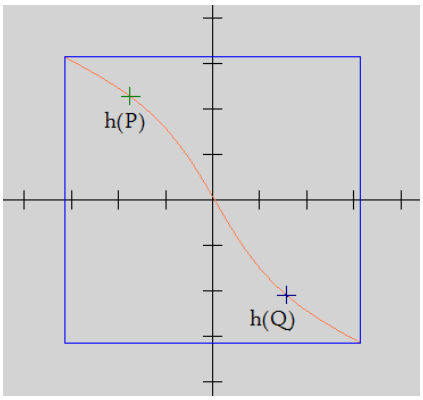
kterou pomocí funkce $h : X_1 \to (-\pi, \pi)^2$ transformujeme na množinu $X_2 = h(X_1)$.

$$X_2 = \left\{(r, s) \in (-\pi, \pi)^2;\ -(q_2 - p_2) \operatorname{tg} \frac{r}{2} + (q_1 - p_1) \operatorname{tg} \frac{s}{2} + p_1 q_2 - p_2 q_1 = 0\right\}$$

Příklad 7.1. (Vizualizace transformací) Položme $P = (-1.2, 2.16)$ a $Q = (1, -1.73)$.



Obrázek 22: X_1



Obrázek 23: X_2

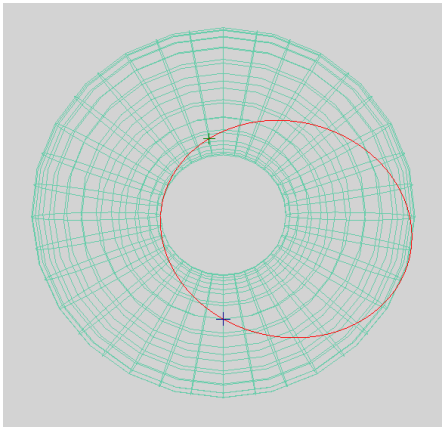
Vyjádřením parametru s jako funkce r z rovnice pro transformovanou přímku X_2 dostáváme vztah

$$s(r) = 2 \operatorname{arctg} \frac{(q_2 - p_2) \operatorname{tg} \frac{r}{2} + p_2 q_1 - p_1 q_2}{q_1 - p_1}, \quad r \in (-\pi, \pi).$$

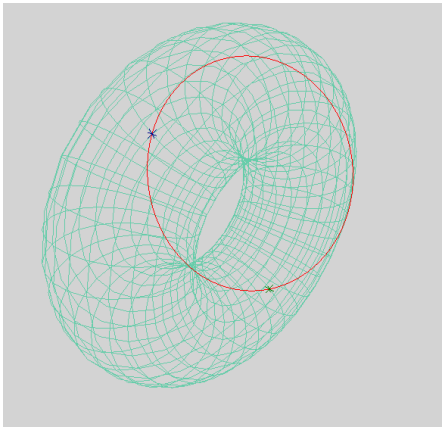
Nyní dosazením do parametrických rovnic toru (7.10) vytvoříme jednoparametrický systém rovnic popisující přímku na toru. Takto vzniklou množinu označíme X_3.

$$X_3 = \left\{ (x, y, z) \in \mathbb{R}^3;\ \begin{array}{rcl} x = & (c + d\cos s(r))\cos r & \\ y = & (c + d\cos s(r))\sin r, & r \in (-\pi, \pi) \\ z = & d \sin s(r) & \end{array} \right\} \tag{7.15}$$

Pokračujme v příkladu (7.1). Za volitené parametry toru vezměme $c = 4$ a $d = 2$, potom znázornění množiny X_3 je na následujících dvou obrázcích.

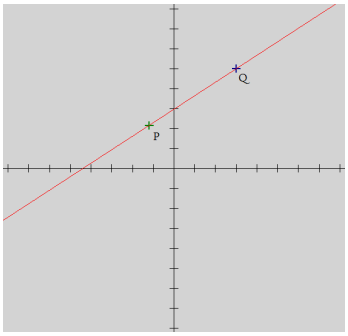


Obrázek 24: X_3

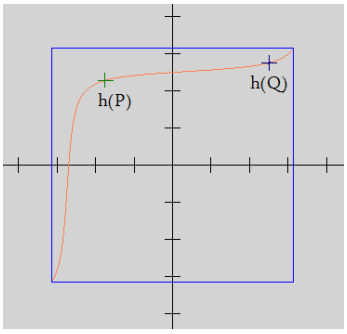


Obrázek 25: X_3

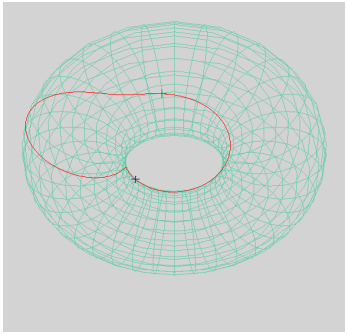
Příklad 7.2. Položme $P = (-1.2, 2.16)$, $Q = (3, 5)$.



Obrázek 26: X_1



Obrázek 27: X_2



Obrázek 28: X_3

7.2 Přenesení semi-eliptických křivek na polem $\mathbb{R}$

Stejný postup, který byl aplikován pro přenášení reálných přímek na torus, může být použit i pro přenesení libovolné křivky z $\mathbb{R}^2$. Provedeme zde konstrukci množin X_1, X_2, X_3 a příslušných transformací. Připomeňme, že pro účely vizualizace budeme využívat pojmu semi-eliptické křivky, která jako množina neobsahuje bod ∞ a navíc neklademe žádné nároky na diskriminant Δ.

Množina X_1 je definována následovně

$$X_1 = \mathcal{E}_1(\mathbb{R}, a, b) = \left\{(x, y) \in \mathbb{R}^2;\ y^2 = x^3 + ax + b\right\}$$

a po provedení transformace $h : \mathbb{R}^2 \to (-\pi, \pi)^2$ dostáváme X_2

$$X_2 = \left\{(r, s) \in (-\pi, \pi)^2;\ \operatorname{tg}^2 \frac{s}{2} = \operatorname{tg}^3 \frac{r}{2} + a \operatorname{tg} \frac{r}{2} + b\right\}$$

Označme $X_{2r} = \{r \in (-\pi, \pi);\ (r, s) \in X_2\}$ množinu parametrů r z X_2.

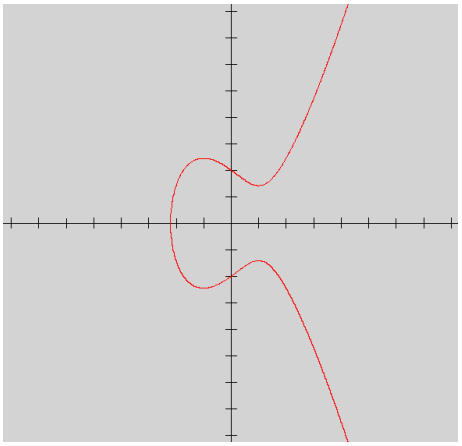
Vyjádříme $s(r)$ z definičního vztahu množiny X_2 a dostáváme

$$|s(r)| = 2 \operatorname{arctg} \sqrt{\operatorname{tg}^3 \frac{r}{2} + a \operatorname{tg} \frac{r}{2} + b}, \quad r \in X_{2r} \tag{7.16}$$

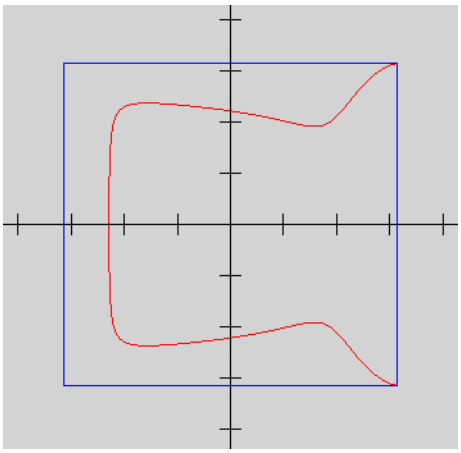
a získáme výslednou množinu X_3

$$X_3 = \left\{ (x, y, z) \in \mathbb{R}^3; \begin{array}{rcl} x = & (c + d\cos s(r))\cos r & \\ y = & (c + d\cos s(r))\sin r, & r \in X_{2r} \\ z = & d \sin s(r) & \end{array} \right\} \tag{7.17}$$

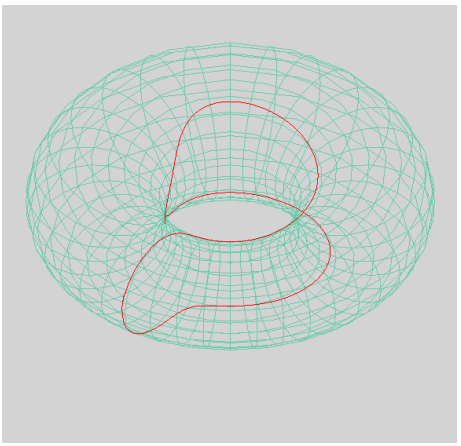
Provedeme konkrétní znázornění u tří vybraných semi-eliptických křivek nad polem reálných čísel. Začněme volbou $X_{1A} = \mathcal{E}_1(\mathbb{R}, -3, 4)$. Množiny X_{1A} a X_{2A} X_{3A} jsou zobrazeny na následujících obrázcích.



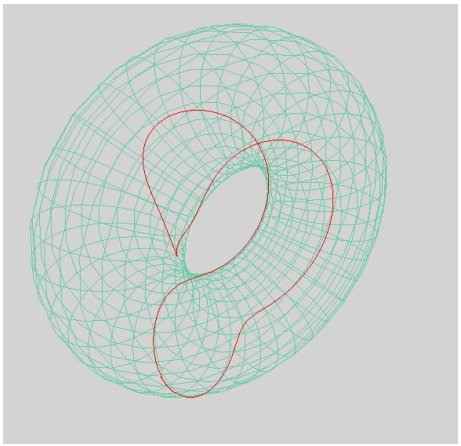
Obrázek 29: X_{1A}



Obrázek 30: X_{2A}

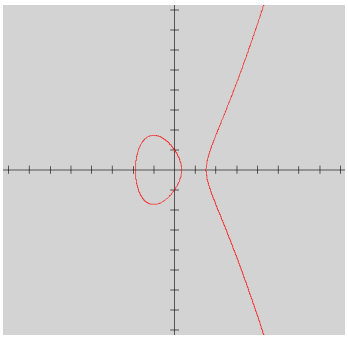


Obrázek 31: X_{3A}

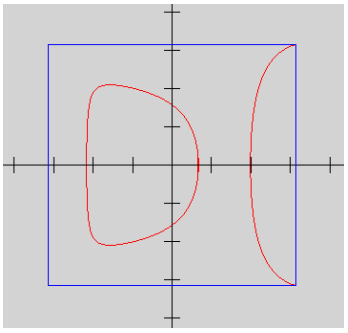


Obrázek 32: X_{3A}

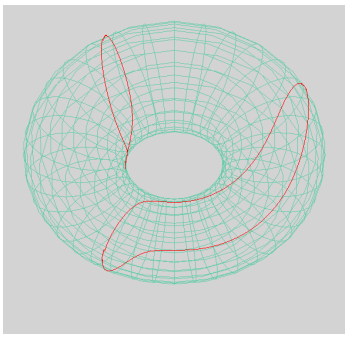
V dalším příkladu volíme $X_{1B} = \mathcal{E}_1(\mathbb{R}, -3, 1)$.



Obrázek 33: X_{1B}

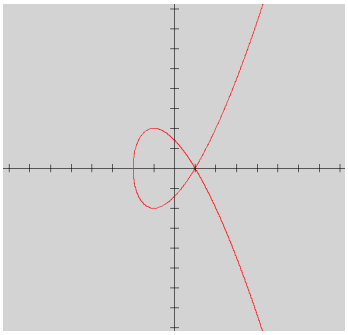


Obrázek 34: X_{2B}

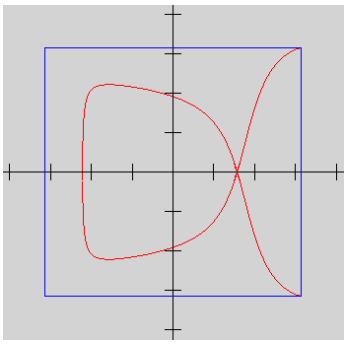


Obrázek 35: X_{3B}

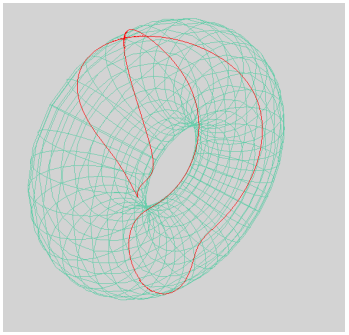
Zvolme nyní semi-eliptickou křivku s $\Delta = 0$, např. $X_{1C} = \mathcal{E}_1(\mathbb{R}, -3, 2)$.



Obrázek 36: X_{1C}



Obrázek 37: X_{2C}



Obrázek 38: X_{3C}

7.3 Přenesení semi-eliptických křivek nad poli $\mathbb{F}_p$

Semi-eliptickou křivku definovanou nad konečným polem můžeme chápat jako množinu diskrétních bodů v reálné rovině. Navíc pro případ prvočíselných polí $\mathbb{F}_p$ tyto body leží vždy v oblasti otevřeného čtverce $\mathbb{I}_p^2 = \left\{\mathbf{x} \in \mathbb{R}^2;\ -\frac{p}{2} < x_i < \frac{p}{2}\right\}$. Tento otevřený čtverec nyní stačí zobrazit stejnolehlostí na otevřený čtverec $(-\pi, \pi)^2$.

Stejnolehlost $g : \mathbb{I}_p^2 \ni (x, y) \mapsto (r, s) \in (-\pi, \pi)^2$ je dána

$$r = \frac{2\pi x}{p} \tag{7.18}$$

$$s = \frac{2\pi y}{p} \tag{7.19}$$

Inverzní zobrazení g^{-1} je dáno

$$x = \frac{rp}{2\pi} \tag{7.20}$$

$$y = \frac{sp}{2\pi}, \tag{7.21}$$

kde $x, y \in \mathbb{I}_p$ a $r, s \in (-\pi, \pi)$.

Analogicky jako v případě semi-eliptických křivek nad reálnými čísly sestrojme zobrazení $h = g|_{X_1}$, kde X_1 je podmnožinou $\mathbb{I}_p^2$. Za X_1 můžeme zvolit přímo semi-eliptickou křivku $\mathcal{E}(\mathbb{F}_p, a, b)$, tj.

$$X_1 = \mathcal{E}(\mathbb{F}_p, a, b) = \left\{(x, y) \in I_p^2;\ (x, y) \in \mathcal{E}(\mathbb{F}_p, a, b)\right\} \tag{7.22}$$

a po aplikaci zobrazení $h : X_1 \to (-\pi, \pi)^2$ obdržíme množinu, kterou v souladu s předchozím textem označíme $X_2 = h(X_1)$. V našem konkrétní případě dostáváme

$$X_2 = \left\{(r, s) \in (-\pi, \pi)^2;\ (r, s) = h\left((x, y)\right),\ (x, y) \in \mathcal{E}(\mathbb{F}_p, a, b)\right\}$$

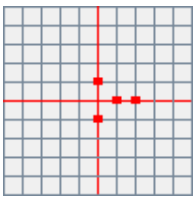
Každý bod množiny X_2 nyní může být chápán jako dvojice parametrů r, s, které dosazujeme do parametrických rovnic toru. Množina bodů na toru X_3 je dána v našem konkrétním případě následovně

$$X_3 = \left\{ \begin{array}{rcc} & x = & (c + d\cos s(r))\cos r \\ (x, y, z) \in \mathbb{R}^3; & y = & (c + d\cos s(r))\sin r, \quad (r, s) \in X_2 \\ & z = & d\sin s(r) \end{array} \right\} \tag{7.23}$$

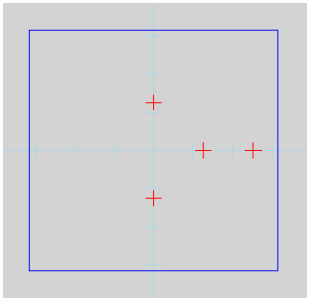
Torus si lze nadále přestavovat jako souvislou množinu, avšak při práci s diskrétními množinami by bylo vhodné tuto plochu popsat také množinou diskrétních bodů. Využijeme přitom prvočíselná pole $\mathbb{F}_p$. *Diskrétním torem definovaným nad prvočíselným polem* $\mathbb{F}_p$ rozumíme takovou množinu X_3 podle (7.23), která vznikne, pokud za X_1 podle (7.22) volíme množinu $\mathbb{F}_p \times \mathbb{F}_p$. Disktrétní torus označíme $\mathcal{DT}_p$.

Při notaci prvků $-\frac{p-1}{2}, \ldots, \frac{p-1}{2}$ z $\mathbb{F}_p$ zřejmě platí $\mathbb{F}_p^2 \subset \mathbb{I}_p^2$ a můžeme provést stejnolehlost na otevřený čtverec $(-\pi, \pi)^2$, který určuje dvojice parametrů (r, s), jenž tvoří souřadnicový systém na toru. Zde si všimněme, že při zobrazení diskrétní množiny $\mathbb{F}_p^2$ dochází k rozdělení intervalů $r \in (-\pi, \pi)$ a $s \in (-\pi, \pi)$, vybrání právě p bodů z obou intervalů. Diskrétní torus $\mathcal{DT}_p$ je tedy množinou takto vybraných bodů a můžeme si představovat p úhelník, kde nad každým jeho vrcholem vytvoříme další p úhelník kolmo na rovinu původního a natočen směrem k počátku systému souřadnic.

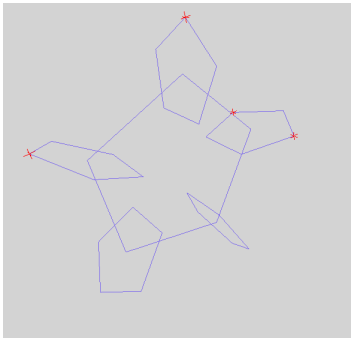
Příklad 7.3. Proveďme konstrukci množin X_1, X_2, X_3 pro semi-eliptické křivky $\mathcal{E}(\mathbb{F}_5, 3, 1)$, $\mathcal{E}(\mathbb{F}_7, 3, 1)$ a $\mathcal{E}(\mathbb{F}_{31}, 24, 21)$.



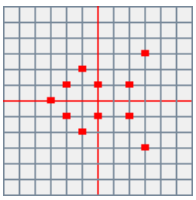
Obrázek 39: $X_1 = \mathcal{E}(\mathbb{F}_5, 3, 1)$



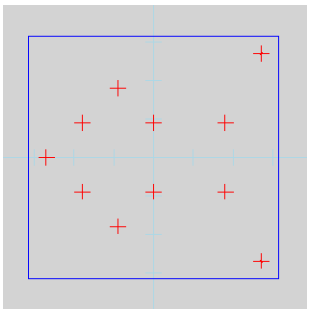
Obrázek 40: $X_2 = h(X_1)$



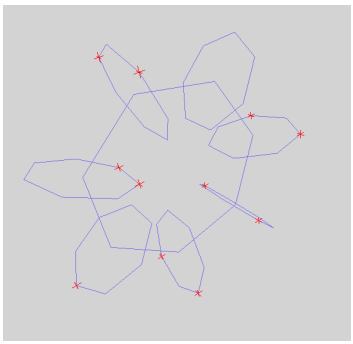
Obrázek 41: X_3



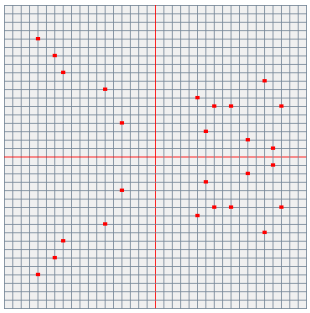
Obrázek 42: $X_1 = \mathcal{E}(\mathbb{F}_7, 3, 1)$



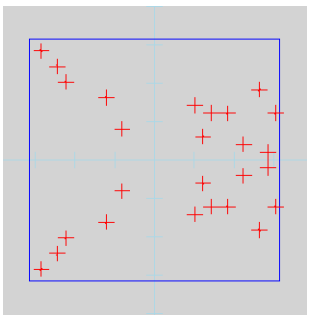
Obrázek 43: $X_2 = h(X_1)$



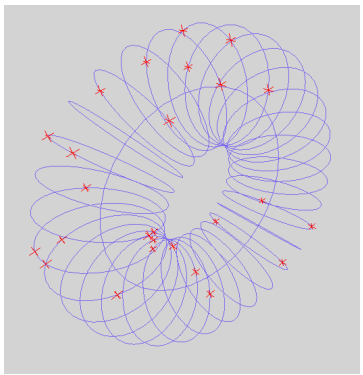
Obrázek 44: X_3



Obrázek 45:
$X_1 = \mathcal{E}(\mathbb{F}_{31}, 24, 21)$



Obrázek 46: $X_2 = h(X_1)$

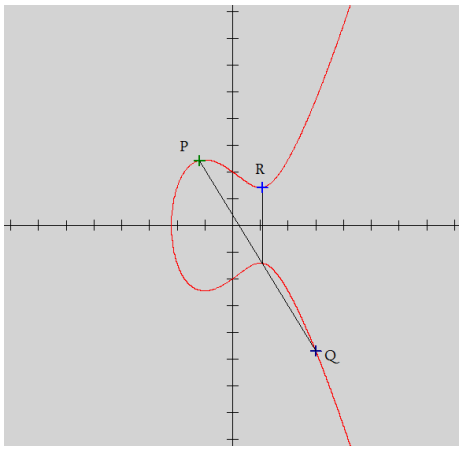


Obrázek 47: X_3

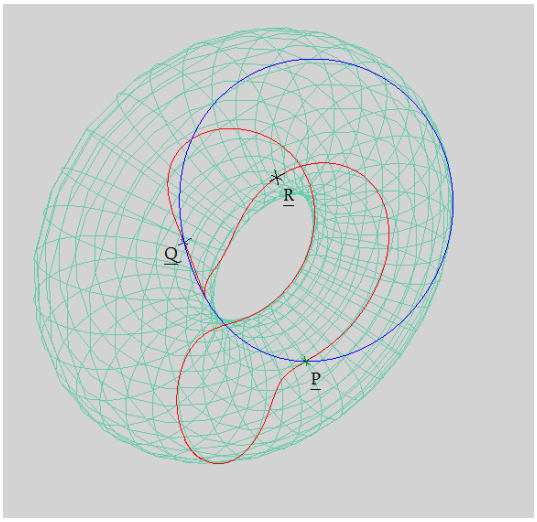
7.4 Vizualizace grupové operace na toru

Již máme prostředky, díky nimž jsme schopni vizualizovat přímky, stejně také semi-eliptické křivky a grupovou operaci na těchto křivkách na toru. Nezbývá, než uvést výsledky v podobě výstupu z programu `TrElC`. Připomeňme, že grupová operace je definována jen na semi-eliptických křivkách, které jsou eliptickými a je přidán bod ∞.

Uvažujme opět eliptickou křivku $\mathcal{E}(\mathbb{R}, -3, 4)$ a proveďme součet bodů $R = P \oplus Q$, kde $P = (-1.2, 2.423)$ a $Q = (3, -4.690)$. Y-složky bodů P a Q jsou zaokrouhleny. Situace je znázorněna na obrázku 48. Na vedlejším obrázku je dále zobrazena situace na toru, kde transformované body P, Q a R jsou označeny postupně $\underline{P}$, $\underline{Q}$ a $\underline{R}$.

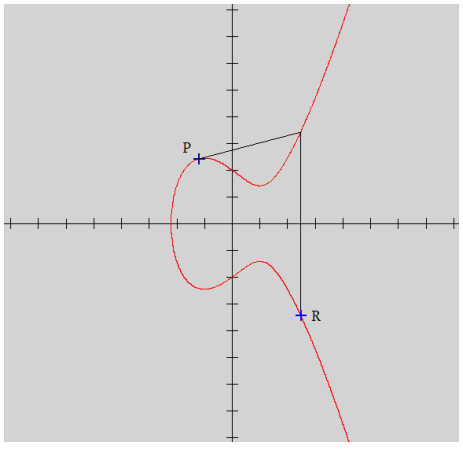


Obrázek 48: $R = P \oplus Q$

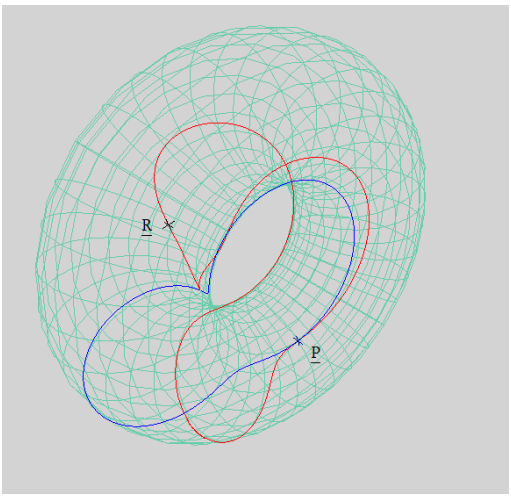


Obrázek 49: $\underline{R} = \underline{P} \oplus \underline{Q}$

Na téže eliptické křivce provedeme zdvojení bodu $P = (-1.2, 2.423)$.

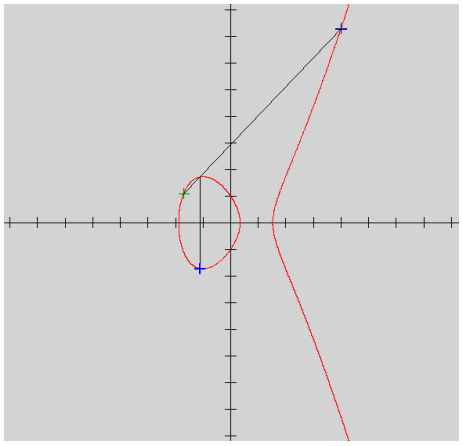


Obrázek 50: $R = P \oplus P$

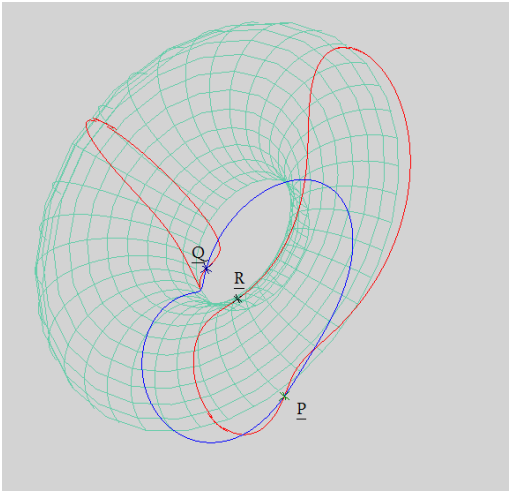


Obrázek 51: $\underline{R} = \underline{P} \oplus \underline{P}$

Uvažujme dále eliptickou křivku $\mathcal{E}(\mathbb{R}, -3, 1)$. Její transformace jsou uvedeny na obrázcích 33, 34, 35. Znázorníme součet dvou různých bodů křivky, avšak ve větším detailu bez zobrazení kompletního povrchu toru.



Obrázek 52: Součet bodů



Obrázek 53: Zdvojení bodu

7.5 Geodetické křivky

Věta 7.1. Nechť $\gamma = \gamma(t) = (r(t), s(t))$ je křivka na ploše $f(r, s)$ zadaná parametricky (Křivkou zde rozumíme zobrazení $\gamma : \mathbb{R} \ni t \mapsto (r, s) \in M \subset \mathbb{R}^2$ a plochou zobrazení $f : \mathbb{R}^2 \supset M \ni (r, s) \mapsto (x, y, z) \in \mathbb{R}^3$). Potom délka $L(\gamma)$ křivky mezi body o parametrech t_1, t_2 je dána

$$L(\gamma) = \int_{t_1}^{t_2} \sqrt{Er'^2(t) + 2Fr'(t)s'(t) + Gs'^2(t)}\,\mathrm{d}t,$$

kde E, F, G jsou koeficienty první základní formy definované

$$\begin{aligned} E &= f'_r \cdot f'_r \\ F &= f'_r \cdot f'_s \\ G &= f'_s \cdot f'_s \end{aligned}$$

Více o základních formách a další vlastnosti křivek na plochách viz [10].

Příklad 7.4. Pro torus definovaný v předchozí kapitole jako plocha zadaná parametricky

$$f(r, s) = ((c + d\cos s)\cos r, (c + d\cos s)\sin r, d\sin s)$$

spočtěme parciální derivace

$$\begin{aligned} f'_r = &\quad (-(c + d\cos s)\sin r, (c + d\cos s)\cos r, 0) \\ f'_s = &\quad\quad (-d\sin s\cos r, -d\sin s\sin r, d\cos s) \end{aligned}$$

a následně koeficienty první základní formy $E = (c + d\cos s)^2$, $F = 0$, $G = d^2$.

Definice 7.1. Uvažujme plochu $f(r, s)$, libovolné dva body $P = f(r_1, s_1)$, $Q = f(r_2, s_2)$ a množinu $\mathcal{K}$ všech křivek γ třídy C^1 na ploše $f(r, s)$ s krajními body P a Q. *Geodetickou křivkou na ploše* $f(r, s)$ pak nazýváme takovou křivku $\gamma \in \mathcal{K}$, jejíž délka $L(\gamma)$ je minimální.

Definici geodetické křivky na ploše $f(r, s)$ uvádíme v souvislosti s myšlenkou, zda přímky v reálné rovině přenesené na torus podle (7.15) jsou geodetické křivky. Tato otázka zůstává otevřená.

8 Závěr

V bakalářské práci jsme prostudovali eliptické křivky nad polem reálných čísel a důsledně provedli analýzu i nad poli prvočíslenými. Pro vizualizaci i přesnější vyjádření jsme v kapitole 4 zavedli pojem obecnější semi-eliptické křivky a pomocí experimentálních výsledků se podařilo zformulovat věty (4.1),(4.2) a jejich důkazy. Pomocí Mestreho teorému (4.3) jsme prokázali platnost hypotézy (4.1) pro eliptické křivky, nikoliv však obecně pro semi-eliptické křivky. Hypotéza tak zůstává otevřená.

Kapitolu 5 jsme věnovali odvození hladké variety a analýze zobrazení mezi topologickými prostory. Prozkoumali jsme vlastnosti toru $\mathcal{T}$ z hlediska topologie, geometrie a uvedli jsme další alternativní definice toru jako faktorového prostoru $\mathbb{R}^2/\Gamma$ v kapitole 6 a jako plochy popsané pomocí parametrických rovnic v kapitole 7. Získali jsme tak prostředky k odvození vhodných zobrazení mezi reálnou rovinou a torem pro případ přenesení semi-eliptických křivek nad $\mathbb{R}$ i nad $\mathbb{F}_p$.

Odvozená zobrazení jsme úspěšně implementovali v programech `TrElC` a `ElCOFF`, jejichž dokumentace je k nahlédnutí v příloze C.

9 Příloha A

Teorém 9.1. (Hasse) Nechť $\mathcal{E}_\infty$ je eliptická křivka definovaná nad $\mathbb{F}_p$. Potom

$$p + 1 - 2\sqrt{p} \leq \#\mathcal{E}_\infty(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

Interval $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ se nazývá *Hasseho interval.*

Důkaz Teorému 9.1. Uvažujme $\mathcal{E}_\infty$ eliptickou křivku definovanou nad $\mathbb{F}_p$ danou ve tvaru[8] $\mathcal{E}_\infty : Y^2 = X^3 + aX + b$ pro nějaká $a, b \in \mathbb{F}_p$. V následujícím textu budeme pro zjednodušení psát již jen $\mathcal{E}$ místo $\mathcal{E}_\infty$. Jestliže $p = 2$ nebo $p = 3$, potom je Hasseho teorém splněn ihned, protože množina $\mathcal{E}(\mathbb{F}_p, a, b)$ má nejméně 1 prvek (neutrální prvek ∞) a nemá více než $2p$ prvků. Tedy číslo $\#\mathcal{E}(\mathbb{F}_p)$ pro $p = 2$ nebo $p = 3$ jistě patří do Hasseho intervalu $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$.

Abychom získali odhad o počtu prvků množiny $\mathcal{E}(\mathbb{F}_p, a, b)$ v případě, kdy $p > 3$, musíme se zaměřit na eliptickou křivku $\mathcal{E}'/\mathbb{F}_p(x)$, kde $\mathbb{F}_p(x)$ je pole racionálních funkcí s koeficienty v $\mathbb{F}_p$. V našem případě x reprezentuje transcendentní proměnnou, zatímco X je proměnná v poli $\mathbb{F}_p(x)$. Rovnice definující eliptickou křivku $\mathcal{E}'/\mathbb{F}_p(x)$ nad polem $\mathbb{F}_p(x)$ je následující

$$Y^2 = \frac{X^3 + aX + b}{x^3 + ax + b}. \tag{9.24}$$

Prozkoumáme nyní množinu bodů eliptické křivky $\mathcal{E}'(\mathbb{F}_p(x))$. Tedy množinu dvojic $(X, Y) \in \mathbb{F}_p^2(x)$, které jsou řešením (9.24).

Množina $\mathcal{E}'(\mathbb{F}_p(x))$ s neutrálním prvkem ∞ tvoří grupu. Jistě platí, že bod $(X, Y) = (x, 1)$ patří do $\mathcal{E}'(\mathbb{F}_p(x))$,

$$1^2 = \frac{x^3 + ax + b}{x^3 + ax + b}$$

Stejně také bod $(X, Y) = (x^p, (x^3 + ax + b)^{\frac{p-1}{2}}) \in \mathcal{E}'(\mathbb{F}_p(x))$,

$$Y^2(x^3 + ax + b) = (x^3 + ax + b)^{p-1}(x^3 + ax + b) = (x^3 + ax + b)^p = (X^3 + aX + b).$$

Můžeme nyní pro každé $n \in \mathbb{Z}$ definovat prvek grupy $\mathcal{E}'(\mathbb{F}_p(x))$ následovně

$$\mathbb{Z}_n = (x^p, (x^3 + ax + b)^{\frac{p-1}{2}}) \oplus n(x, 1).$$

Každý prvek $\mathbb{Z}_n$ kromě neutrálního $\mathbb{Z}_n = \infty$ je tedy tvaru $\mathbb{Z}_n = (X_n, Y_n)$, kde $X_n, Y_n \in \mathbb{F}_p(x)$. Nechť $X_n = \frac{P_n}{Q_n}$, pro $P_n, Q_n \in \mathbb{F}_p[x]$ nesoudělné.

[8] V důkazu zachováme původní značení z literatury [8].

Pro každý prvek $\mathbb{Z}_n$ definujme hodnotu d_n takto

$$d_n = \begin{cases} 0 & , \mathbb{Z}_n = \infty \\ \deg(P_n) & , \mathbb{Z}_n = (X_n, Y_n); \end{cases}$$

Uvedeme nyní dvě lemma, s jejichž pomocí dokážeme Hasseho teorém. První udává vztah hodnot d_{-1} a $\#\mathcal{E}(\mathbb{F}_p)$. Druhé lemma umožňuje spočíst obecně d_n, což nám poskytne hranice pro $\#\mathcal{E}(\mathbb{F}_p)$.

Lemma 1. $d_{-1} - d_0 - 1 = \#\mathcal{E}(\mathbb{F}_p) - p - 1$.

Lemma 2. Nechť $t = d_{-1} - p - 1$. Potom

$$d_n = n^2 - tn + d_0, \forall n \in \mathbb{Z}.$$

Jistě $d_0 = p$, potom

$$d_n = n^2 - (\#\mathcal{E}(\mathbb{F}_p) - p - 1)n + p.$$

K důkazu Hasseho teorému nyní stačí ukázat, že $n^2 - tn + p \geq 0, \forall n \in \mathbb{R}$. Tj. pro diskriminant této kvadratické rovnice musí platit $t^2 - 4p \leq 0$, ekvivalentním vyjádřením je $(\#\mathcal{E}(\mathbb{F}_p) - p - 1)^2 \leq 4p$, a proto

$$|p + 1 - \#\mathcal{E}(\mathbb{F}_p)| \leq 2\sqrt{p}.$$

Abychom dokázali $t^2 - 4p \leq 0$, uvažujme, že funkce $d(n) = n^2 - tn + p < 0$ pro nějaké $n \in \mathbb{R}$. Platí však $d(n) > 0$, $\forall n \in \mathbb{Z}$, protože $d(n) = d_n \geq 0$. Tedy pro dva reálné kořeny funkce $d(n)$, řekněme α, β, musí platit nerovnost $0 < |\alpha - \beta| < 1$. Obecně u normované kvadratické rovnice se ale kvadrát rozdílu dvou reálných rořenů rovná kvadrátu diskriminantu. V našem případě tedy platí $(\alpha - \beta)^2 = t^2 - 4p$, což je celé číslo. Dostáváme spor, protože $0 < (\alpha - \beta)^2 < 1$.

Vztah $t^2 - 4p \leq 0$ platí a Hasseho teorém je tímto dokázán za předpokladu pravdivosti lemmat 1 a 2. Podrobný postup důkazu je uveden v [8].

10 Příloha B

Uvádíme tabulku kvadratických reziduí pro $3 \leq p \leq 61$. Pro vyhledání kvadratických reziduí pro větší prvočísla je užitečná stránka [16].

p	počet kv. reziduí	kv. rezidua	kv. nerezidua
3	1	1	2
5	2	1,4	2,3
7	3	1,2,4	3,5,6
11	5	1,3,4,5,9	2,6,7,8,10
13	6	1,3,4,9,10,12	2,5,6,7,8,11
17	8	1,2,4,8,9,13,15,16	3,5,6,7,10,11,12,14
19	9	1,4,5,6,7,9,11,16,17	2,3,8,10,12,13,14,15,18
23	11	1,2,3,4,6,8,9, 12,13,16,18	5,7,10,11,14,15,17, 19,20,21,22
29	14	1,4,5,6,7,9,13, 16,20,22,23,24,25,28	2,3,8,10,11,12,14, 15,17,18,19,21,26,27
31	15	1,2,4,5,7,8,9,10,14, 16,18,19,20,25,28	3,6,11,12,13,15,17,21, 22,23,24,26,27,29,30
37	18	1,3,4,7,9,10,11, 12,16,21,25,26,27,28, 30,33,34,36	2,5,6,8,13,14,15, 17,18,19,20,22,23,24, 29,31,32,35
41	20	1,2,4,5,8,9,10,16 18,20,21,23,25,31,32,33, 36,37,39,40	3,6,7,11,12,13,14,15 17,19,22,24,26,27,28,29, 30,34,35,38
43	21	1,4,6,9,10,11,13,14, 15,16,17,21,23,24,25,31, 35,36,38,40,41	2,3,5,7,8,12,18,19, 20,22,26,27,28,29,30,32, 33,34,37,39,42
47	23	1,2,3,4,6,7,8,9, 12,14,16,17,18,21,24,25, 27,28,32,34,36,37,42	5,10,11,13,15,19,20,22, 23,26,29,30,31,33,35,38, 39,40,41,43,44,45,46
53	26	1,4,6,7,9,10,11,13,15, 16,17,24,25,28,29,36,37,38 40,42,43,44,46,47,49,52	2,3,5,8,12,14,18,19,20, 21,22,23,26,27,30,31,32,33, 34,35,39,41,45,48,50,51
59	29	1,3,4,5,7,9,12,15,16,17, 19,20,21,22,25,26,27,28,29,35, 36,41,45,46,48,49,51,53,57	2,6,8,10,11,13,14,18,23,24, 30,31,32,33,34,37,38,39,40,42, 43,44,47,50,52,54,55,56,58
61	30	1,3,4,5,9,12,13,14,15,16, 19,20,22,25,27,34,36,39,41,42, 45,46,47,48,49,52,56,57,58,60	2,6,7,8,10,11,17,18,21,23, 24,26,28,29,30,31,32,33,35,37, 38,40,43,44,50,51,53,54,55,59

11 Příloha C - Dokumentace k programům

Ke studiu semi-eliptických křivek, jejich transformací a vlastností postupně vznikaly programy `TrElC` a `ElCOFF`. Oba programy jsou napsány v prostředí `C#`.

11.1 Program `TrElC`

Program `TrElC` (Transfer elliptic curves) je zaměřen na zpracování a následnou vizualizaci toru, přímek a semi-eliptických křivek nad polem reálných čísel $\mathbb{R}$.

11.1.1 Formulář ControlPanel

Vstupním bodem programu `TrElC` je právě formulář **ControlPanel**, který zajišťuje kontrolu a zpracování vstupních dat.

Vstupní data se skládají

- z parametrů a, b semi-eliptické křivky $\mathcal{E}(\mathbb{R}, a, b)$, na která nejsou kladena žádná omezení.
- z X-souřadnic bodů P, Q na semi-eliptické křivce, viz poznámka (11.1).
- z parametrů toru c, d, pro které musí platit relace $c > d$.

Funkce tlačítek

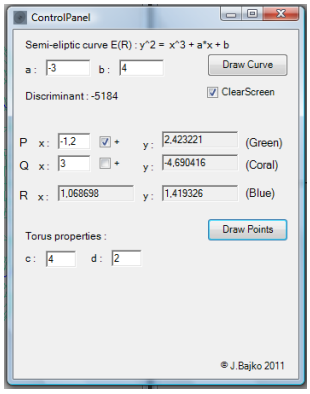
- (Draw Curve): Po stisknutí se zpracují informace o parametrech a, b a zobrazí se nový formulář **ElCEngine**, kde se vykreslí semi-eliptická křivka $\mathcal{E}(\mathbb{R}, a, b)$. Dále se uloží parametry c, d pro další využití.
- (Draw Points): Tlačítko se stane aktivní až po stiknutí (Draw Curve) a zároveň musí být splněna podmínka nenulovosti diskriminantu Δ semi-eliptické křivky $\mathcal{E}(\mathbb{R}, a, b)$. Po stisku (Draw Points) se zpracují X-souřadnice bodů P, Q a pokud se nejedná o speciální situace (viz poznámka (11.1)), spočte se pomocí vztahů (4.6) nebo (4.7) výsledný bod $R = P \oplus Q$. Proběhne zakreslení bodů P, Q, R do formuláře **ElCEngine** a geometrická konstrukce bodu R.

Poznámka 11.1. (Body P, Q) Y-souřadnice se dopočítávají buď jako kladné, či záporné podle volby příslušného zaškrtávacího pole. Z takto zadávaných X-souřadnic bodů P, Q plynou jistá omezení. X-souřadnice bodů P, Q je možné zadat jen z definičního oboru funkce $f(x) = \pm\sqrt{x^3 + ax + b}$, jinak se zobrazí chybová hláška.

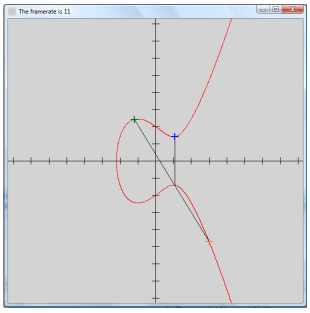
Pokud zvolíme stejné X-souřadnice u bodů P i Q a zároveň zatrhneme různě příslušná zaškrtávací pole, získáváme tak výsledný bod ∞ a vykreslí se rovnoběžka s osou y.

11.1.2 Formulář ElCEngine a TorusEngine

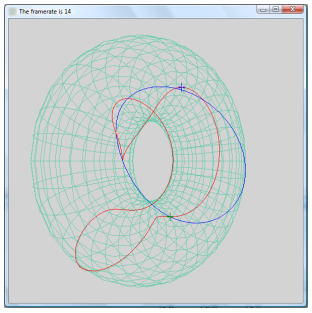
Jakmile dojde k aktivaci formuláře **ElCEngine**, dvojité poklepání na tento formulář vyvolá spuštění dalšího fomuláře **TorusEngine**, který využívá předchozí data k vykreslení[9] drátěného modelu toru a zobrazení transformované semi-eliptické křivky. V případě, že je již vykreslena grupová operace bodů P, Q na semi-eliptické křivce, zobrazí se transformovaná přímka i body $\underline{P}, \underline{Q}, \underline{R}$ na toru.



Obrázek 54: **ControlPanel**



Obrázek 55: **ElCEngine**



Obrázek 56: **TorusEngine**

Přikládáme ukázku zdrojového kódu programu `TrElC`.

```
float h1, h2, h3;
float hx = (x2 - x1) / this.Width /  2;
float hy = (y2 - y1) / this.Height / 2;
float x, y;

x = x1;
while (x < x2)
{
    y = y1;
    while (y < y2)
    {
        h1 = y * y - x * x * x - a * x - b;
        y += hy;
        h2 = y * y - x * x * x - a * x - b;
        x += hx;
        h3 = y * y - x * x * x - a * x - b;
        x -= hx;

        if ((h1 * h2 < 0) | (h2 * h3 < 0))
        {
            CustomVertex.PositionColored OnePoint =
            new CustomVertex.PositionColored(x, y, 0, Color.Red.ToArgb());
            PoleBoduKrivky.Add(OnePoint);
        }
    }
    x += hx;
}
```

Obrázek 57: Vykreslení semi-eliptické křivky

```
private void DrawTgEllipticCurveOnTorusExplicitForm(Color color)...

private void DrawParametricSurface(Color color)...

private void DrawAxis(Color color)...

private void DrawRectangle(Color color)...

private void DrawPointOnTorus(PointF P, Color color)...

private void DrawLineOnTorus(PointF P, PointF Q, Color color)...

private Vector3 TorusTransformation(float r, float s)
{
    return new Vector3((float)(Math.Cos(r) * (c + d * Math.Cos(s))),
                       (float)(Math.Sin(r) * (c + d * Math.Cos(s))),
                       (float)(d * Math.Sin(s)));
}

protected override void OnMouseWheel(MouseEventArgs e)...
protected override void OnMouseDown(MouseEventArgs e)...
protected override void OnMouseMove(MouseEventArgs e)...
protected override void OnMouseUp(MouseEventArgs e)...
protected override void OnKeyDown(KeyEventArgs e)...
```

Obrázek 58: Výběr několika metod, rozvinutá metoda transformace bodu na torus

11.2 Program `ElCOFF`

Program `ElCOFF` (Elliptic curves over finite fields) se zabývá opět zpracováním a vizualizací semi-eliptických křivek, avšak nad prvočíselnými poli $\mathbb{F}_p$. Další funkcí programu je zobrazení přenosu křivek na diskrétní torus $\mathcal{DT}_p$ a analýza množiny všech semi-eliptických křivek $\mathcal{M}(\mathbb{F}_p)$.

11.2.1 Formulář FiniteForm

Vstupním bodem programu `ElCOFF` je právě formulář **FiniteForm**, který se stará o zpracování a kontrolu dat zadaných uživatelem.

[9] Inspirace vytvoření vykreslovací smyčky z [15].

Vstupní data se skládají

- z prvočísla p.
- z parametrů a, b semi-eliptické křivky $\mathcal{E}(\mathbb{F}_p, a, b)$; $a, b \in \{0, 1, \ldots, p-1\}$.
- ze souřadnic bodů $P = (x_1, y_1)$ a $Q = (x_2, y_2)$, kde $P, Q \in \mathcal{E}(\mathbb{F}_p, a, b)$.
- z parametrů diskrétního toru c, d, pro které musí platit relace $c > d$.
- z parametru *IndexEn* určující velikost vykreslované plochy. Pro vykreslení všech bodů dané semi-eliptické křivky definované nad $\mathbb{F}_p$ je třeba nastavit *IndexEn* minimálně na hodnotu $p + 1$.

Funkce tlačítek

- (Draw Curve): Po stisku tlačítka si program uloží zadávaná vstupní data a vykreslí semi-eliptickou křivku $\mathcal{E}(\mathbb{F}_p, a, b)$. Dále vypíše všechny body množiny $\mathcal{E}(\mathbb{F}_p, a, b)$, spočte diskriminant Δ a $\texttt{card}(\mathcal{E}(\mathbb{F}_p, a, b))$. Provede se také aktivace dalších funkcí programu.
- (Addition): Program provede součet bodů $R = P \oplus Q$ na semi-eliptické křivce $E(\mathbb{F}_p, a, b)$ a grafické znázornění za předpokladu $\Delta \neq 0$.
- (Clear): Provede vyčištění vykreslovací plochy a vymazání vnitřních proměnných.
- (Record): Stiskem se aktivuje formulář **RecordForm**, jež si do privátních proměnných nageneruje všechny prvky množiny $\mathcal{M}(\mathbb{F}_p)$ z aktuálně zadaného prvočíselného pole $\mathbb{F}_p$. Uživatel může tato data nadále zpracovávat.
- (VizForm): Stiskem se aktivuje formulář pro manuální zadávání bodů, které se posléze vykreslí na diskrétní torus.

Po stisku tlačítka (Draw Curve) i (Addition) se stane aktivní událost dvojité kliknutí na vykreslovací plochu, která zobrazí nový formulář **ViewForm**, na němž se vykreslí model diskrétního toru $\mathcal{DT}_p$ a transformovaná množina $\mathcal{E}(\mathbb{F}_p, a, b)$. V případě, že ve formuláři **FiniteForm** byl proveden součet bodů P a Q, vykreslí se také transformace těchto bodů.

11.2.2 Formulář RecordForm

Formulář **RecordForm** zpracovává data odevzdaná formulářem **FiniteForm** a zaměřuje se na analýzu konkrétní množiny všech semi-eliptických křivek $\mathcal{M}(\mathbb{F}_p)$.

Funkce tlačítek

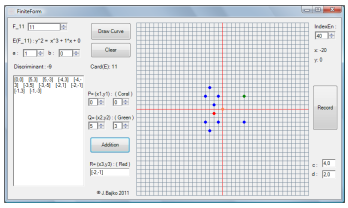
- (Color Curve): Funguje stejně jako tlačítko (Draw Curve) s rozdílem, že uživatel má možnost měnit barvu křivky a již vykreslené semi-eliptické křivky po stisknutí zůstavají stále vykreslovány. Můžeme tak názorně graficky interpretovat větu (4.1).

- (ToData.txt): Stiskem tlačítka se do kořenového adresáře vygeneruje soubor *data.txt*, jehož hlavička obsahuje údaje o prvočíselném poli $\mathbb{F}_p$, příslušná kvadratická rezidua a Hasseho interval. Tělo textového dokumentu je tvořeno výčtem informací o všech semi-eliptických křivkách nad $\mathbb{F}_p$, pro konkrétnost údaji o koeficientech (a, b), diskriminantu Δ, j-invariantu $j(\mathcal{E}(\mathbb{F}_p, a, b))$, počtu bodů semi-eliptické křivky $\texttt{card}(\mathcal{E}(\mathbb{F}_p, a, b))$ a také výpisem všech bodů množiny $\mathcal{E}(\mathbb{F}_p, a, b)$.

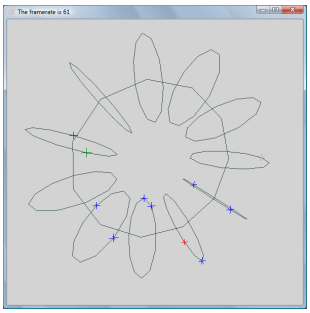
- (ToCounts.txt): Stiskem tlačítka se do kořenového adresáře vygeneruje soubor *counts.txt*, jehož hlavička se opět skládá z údajů o prvočíselném poli $\mathbb{F}_p$ a Hasseho intervalu. Dále se vypíše počet semi-eliptických křivek nad $\mathbb{F}_p$, které mají nulový diskriminant, viz věta (4.2). Tělo dokumentu obsahuje údaje o počtu semi-eliptických křivek v závislosti na možných počtech bodů těchto křivek, viz obrázek (13) a hypotéza (4.1).

V podkapitole (4.4) jsme se zabývali právě daty pořízenými z programu `ElCOFF`. Tabulky uvedené v podkapitole (4.4) znázorňují strukturu souborů *data.txt* a *counts.txt* pro volbu prvočíselného pole $\mathbb{F}_5$. Avšak, pokračujeme-li s generováním těchto souborů pro větší prvočísla, narůstá výpočetní doba a nároky na paměť velice rychle. Experimentálně pro pole $\mathbb{F}_{131}$, soubor *data.txt* je výpočetní doba 3 min, 40 s a velikost 18212 kB. Efektivní využití programu `ElCOFF` tedy leží v analýze množin $\mathcal{M}(\mathbb{F}_p)$ pro malá p.

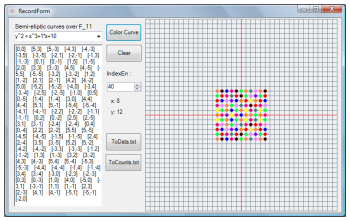
Na následujících obrázcích uvádíme ukázku formulářů a souborů *data.txt* a *counts.txt* pro prvočíselné pole $\mathbb{F}_{11}$.



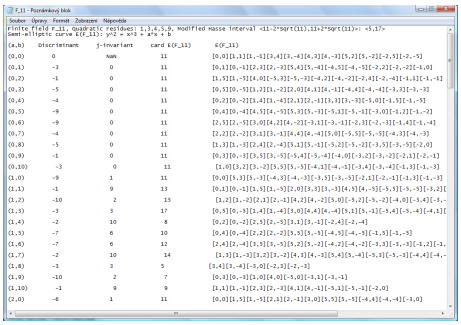
Obrázek 59: **FiniteForm**



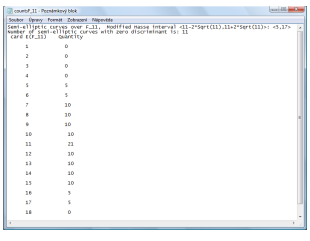
Obrázek 60: **ViewForm**



Obrázek 61: **RecordForm**



Obrázek 62: *data.txt*



Obrázek 63: *counts.txt*

Literatura

[1] HANKERSON, D., MENEZES, A., VANSTONE, S.: *Guide to Elliptic Curve Cryptography*. Springer-Verlag, New York, Inc., 2004. ISBN 0-387-95273-X.

[2] STILLWELL, J.: *Geometry of surfaces*. 2.opravené vydání. Springer-Verlag, New York, Inc., 1992. ISBN 0-387-97743-0.

[3] MUKHI, S., MUKUNDA, N: *Lectures on Advanced Mathematical Methods for Physicists*. World Scientific Publishing Co. Pte. Ltd. 5 Toh Tuck Link, Singapur 596224. Hindustan Book Agency 2010. Tištěno v Indii. ISBN-13 978-981-4299-73-2.

[4] KRUPKA, D.: *Úvod do analýzy na varietách*. 1.vydání. Univerzita J. E. Purkyně v Brně roku 1985. Státní pedagogické nakladatelství, n.p., Praha 1.

[5] LEE, J., M.: *Introduction to smooth manifolds*. 2003 Springer Science+Business Media, Inc. ISBN-13: 978-0387-95448-6.

[6] SCHWARZ, Š.: *Algebraické čísla*. 1.vydání. Vydala: Jednota československých matematiků a fyziků roku 1950 v Praze. Edice: Kruh, svazek 16.

[7] KARÁSEK, J., SKULA, L.: *Obecná algebra*. 1.vydání. Vysoké učení technické v Brně roku 2008. ISBN 978-80-214-3794-4.

[8] FRENCH, T.: *Counting Points on Elliptic Curves and Applications to Cryptography*. University of Western Australia, 1999.

[9] ZAVÍRALOVÁ, L.: *Rings of endomorphisms of elliptic curves and Mestre's theorem*. Brno: Brno University of Technology, Faculty of Mechanical Engineering, 2009.

[10] ONDRAŠÍK, P.: *Křivky na plochách*. Brno: Brno University of Technology, Faculty of Mechanical Engineering, 2003.

[11] Wikipedie. *Normal subgroup* [online]. Poslední úprava 2011-04-27 [cit. 2011-04-29]. <http://en.wikipedia.org/wiki/Normal_subgroup>.

[12] Wikipedie. *Finite field arithmetic* [online]. Poslední úprava 2011-04-17 [cit. 2011-04-29]. <http://en.wikipedia.org/wiki/Finite_field_arithmetic>.

[13] Wikipedie. *Product topology* [online]. Poslední úprava 2011-05-03 [cit. 2011-05-18]. <http://en.wikipedia.org/wiki/Product_topology>.

[14] Wikipedie. *Quotient space* [online]. Verze 2, poslední úprava 2003-03-13 [cit. 2011-04-23]. <http://planetmath.org/encyclopedia/QuotientSpace.html>.

[15] Microsoft development. *Channel 9* [online]. Poslední úprava 2006-11-02 [cit. 2011-05-24]. <http://channel9.msdn.com/coding4fun/articles/Beginning-Game-Development-Part-I--Introduction>.

[16] *Quadratic residues* [online]. [cit. 2011-05-18]. <http://www.math.mtu.edu/mathlab/COURSES/holt/dnt/quadratic4.html>.