STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Vyjadřování prvočísel kvadratickými formami

Tomáš Perutka
Jihomoravský kraj

Brno 2017

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Vyjadřování prvočísel kvadratickými formami

Representing prime numbers by quadratic forms

Autor: Tomáš Perutka
Škola: Gymnázium Brno, třída Kapitána Jaroše, p. o.
Kraj: Jihomoravský
Konzultant: prof. RNDr. Radan Kučera, DSc.

Prohlášení

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

V Brně dne: ..... Podpis: .....

Poděkování

Na tomto místě bych chtěl velice poděkovat prof. RNDr. Radanovi Kučerovi, DSc. za mimořádnou ochotu a vstřícnost při vedení mé práce a též za cenné rady a připomínky. Také bych rád poděkoval Mgr. Petrovi Pupíkovi za to, že mě přivedl k myšlence přihlásit se do středoškolské odborné činnosti. Tato práce byla vypracována za finanční podpory JMK.

Abstrakt

Cílem práce je jazykem srozumitelným středoškolskému studentovi popsat základní teorii kvadratických forem. V práci jsou představeny základní pojmy této teorie, jako ekvivalence forem, diskriminant nebo redukovaná forma, ale také některé hlubší výsledky, konkrétně grupa tříd forem a elementární teorie genů. Získané poznatky jsou v práci aplikovány na řešení problému, která lichá prvočísla můžeme pro dané přirozené číslo n vyjádřit ve tvaru $x^2 + ny^2$, $x, y \in \mathbb{Z}$.

Klíčová slova

kvadratický zbytek; Legendreův symbol; kvadratická forma; grupa tříd forem; geny forem

Abstract

The goal of this thesis is to work out text about quadratic forms accesible to highschool students. Elementary concepts of quadratic forms theory are introduced and defined in this work, for example equivalence of forms, discriminant, or reduced form, but also some deeper results, namely form class group and elementary genus theory. Obtained results are applied to study the following problem: given a positive integer n, which odd primes can be expressed in the form $p = x^2 + ny^2$, $x, y \in \mathbb{Z}$?

Key words

quadratic residue; Legendre symbol; quadratic form; form class group; genera

Obsah

Úvod **5**

1 Okruh zbytkových tříd a kvadratické zbytky **6**
1.1 Grupa, okruh, těleso a zbytkové třídy 6
1.2 Kvadratické zbytky a Legendreův symbol 10

2 Kvadratické formy **15**
2.1 Základní poznatky o kvadratických formách 15
2.2 Redukované formy daného diskriminantu 21

3 Grupa tříd forem a úvod do teorie genů **25**
3.1 Podgrupa, homomorfismus, faktorgrupa 25
3.2 Grupa tříd forem 28
3.3 Geny forem 32

Závěr **36**

Úvod

Cílem práce je vytvořit text zabývající se teorií kvadratických forem, který je psán jazykem srozumitelným středoškolskému čtenáři. O tomto tématu, ačkoli je velmi zajímavé, totiž v českém jazyce nalezneme velmi málo informací.

V textu se také zabýváme následujícím problémem: máme-li dáno přirozené číslo n, jaká lichá prvočísla lze vyjádřit ve tvaru $x^2 + ny^2$ pro nějaká celá čísla x, y? Touto otázkou se zabývalo mnoho slavných matematiků, jako například Carl Friedrich Gauss nebo Leonhard Euler. Už oni dokázali vyřešit tento problém pro velmi malá n, např. pro $n = 1, 2, 3$. Jak to ale bude např. v případě $n = 105$? Na konci třetí kapitoly to budeme schopni říci, protože právě teorie popsána v této práci je klíčem k řešení onoho starého problému.

V první kapitole se čtenář dozví více o okruzích zbytkových tříd a seznámí se s algebraickými pojmy jako grupa, okruh nebo těleso. Dále je zde popsána základní teorie kvadratických zbytků.

Druhá kapitola se zabývá elementární teorií kvadratických forem. Čtenář se seznámí s důležitými pojmy, jako například ekvivalence forem, diskriminant, redukovaná forma apod.

Na začátku třetí kapitoly je opět třeba zavést několik pojmů z algebry – jedná se o pojmy podgrupa, homomorfismus, faktorgrupa. Potom se konečně dostáváme k pokročilejším pojmům z teorie kvadratických forem – ke genům a grupě tříd forem. Díky studiu těchto objektů se nám podaří zjistit mnohem více o problému popsaném výše.

Pokud čtenáře tato problematika zaujme, mohu ho odkázat na knihu [1], z níž jsem při psaní práce vycházel a jež se tímto tématem zabývá na mnohem pokročilejší úrovni.

Kapitola 1

Okruh zbytkových tříd a kvadratické zbytky

V první kapitole nejprve zavedeme některé pojmy z algebry, jejichž znalost je pro tento text nezbytná, a to především pojem grupa. Také si připomeneme, co to jsou zbytkové třídy. Poté se seznámíme s pojmem kvadratický zbytek, který bude hrát důležitou roli při studiu kvadratických forem.

1.1 Grupa, okruh, těleso a zbytkové třídy

Podívejme se na množinu nenulových racionálních čísel a operaci násobení. Pokud násobíme dvě racionální čísla, výsledkem je vždy racionální číslo. Násobení je také jistě asociativní, tedy platí $(ab)c = a(bc)$ pro každá tři čísla $a, b, c \in \mathbb{Q}$. Je dokonce komutativní, tedy $ab = ba$. Dále se v této množině vyskytuje číslo 1, které má tu zajímavou vlastnost, že pro libovolné $a \in \mathbb{Q}$ platí $1a = a$. A dokonce pro každé nenulové racionální číslo m existuje racionální číslo n takové, že $mn = 1$ (pro zlomek $m = \frac{a}{b}$ položme $n = \frac{b}{a}$).

Uvažujme nyní množinu celých čísel a operaci sčítání. Součtem dvou celých čísel je vždy opět celé číslo, operace sčítání je asociativní a komutativní, oním „zajímavým“ prvkem je nyní nula: $0 + a = a$, $a + (-a) = 0$ pro všechna $a \in \mathbb{Z}$.

Podívejme se ještě na poněkud jinou operaci, než klasické sčítání a násobení. Uvažujme množinu uspořádaných dvojic $M = \{(1,1), (1,-1), (-1,1), (-1,-1)\}$ a operaci $\odot$ mezi uspořádanými dvojicemi definovanou jako $(a,b) \odot (c,d) = (ac, bd)$. Opět zde platí komutativita a asociativita. Pro všechny prvky (a,b) množiny M platí $(1,1) \odot (a,b) = (a,b)$, ke každému prvku můžeme najít prvek tak, aby jejich součinem byla dvojice $(1,1)$ (součin libovolného prvku z této množiny s ním samým je roven dvojici $(1,1)$).

Takovouto sadu vlastností operace na množině můžeme najít na mnoha dalších příkladech. Například reálná nebo racionální čísla s operací sčítání, nenulová reálná čísla s násobením, množina $\{1,-1\}$ s násobením. Pokud je čtenář obeznámen s imaginární jednotkou i, může si ověřit, že stejné vlastnosti má i množina $\{1,-1,i,-i\}$ s operací násobení.

Pojem grupa tyto poznatky zobecňuje.

Nejprve definujme, co je to binární operace na množině.

Definice 1.1.1. *Binární operací na množině M rozumíme zobrazení $\odot\colon M \times M \to M$. Pro libovolná $x, y, z \in M$ značíme skutečnost $\odot(x, y) = z$ obvykle jako $x \odot y = z$.*

Na předchozí straně jsme definovali několik příkladů binární operace na množině. Odčítání v přirozených číslech nebo dělení v celých číslech jsou příklady, které požadavky z definice nesplňují, protože výsledek operace nemusí ležet v zadané množině ($2 - 5 \notin \mathbb{N}$, $5 : 12 \notin \mathbb{Z}$).

Nyní můžeme definovat grupu.

Definice 1.1.2. *Množinu G spolu s binární operací $\odot$ na ní definovanou nazveme grupou, pokud splňuje tyto podmínky:*

1. *operace je asociativní, tzn. pro každé $x, y, z \in G$ platí $(x \odot y) \odot z = x \odot (y \odot z)$,*
2. *existuje tzv. neutrální prvek, tedy nějaké $e \in G$ takové, že pro každé $x \in G$ platí $e \odot x = x = x \odot e$,*
3. *ke každému prvku můžeme nalézt prvek k němu inverzní, tedy pro každé $x \in G$ existuje $y \in G$ tak, že $x \odot y = e = y \odot x$.*

Všimněme si, že v definici jsme nepožadovali komutativitu operace. V případě, že operace komutativní je, nazýváme naši grupu komutativní nebo Abelovskou grupou (to podle norského matematika Nielse Abela, který jako jeden z prvních grupy zkoumal). Existuje mnoho nekomutativních grup, např. grupa všech permutací na nějaké množině mající alespoň tři prvky. V tomto textu se však budou vyskytovat převážně komutativní grupy.

Je nutno poznamenat, že se při práci s grupou užívá dvojí symbolika. Zaprvé je to tzv. aditivní symbolika vycházející z operace sčítání, kdy inverzní prvek k prvku x označujeme jako $-x$, pro neutrální prvek užíváme symbol 0 a prvek x n-krát sečtený se sebou samým (pro nějaké přirozené číslo n) značíme nx. Dále existuje tzv. multiplikativní symbolika vycházející z násobení, kdy inverzní prvek k x značíme x^{-1}, pro neutrální prvek používáme symbol 1 a prvek x vynásobený n-krát sám se sebou značíme jako x^n.

Počítání v dané grupě můžeme přehledně ilustrovat tzv. *multiplikativní tabulkou*. Ukažme si to na příkladu grupy $\{(1,1), (1,-1), (-1,1), (-1,-1)\}$ s operací násobení po složkách (definovanou na začátku kapitoly):

	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,-1)$	$(1,-1)$	$(1,1)$	$(-1,-1)$	$(-1,1)$
$(-1,1)$	$(-1,1)$	$(-1,-1)$	$(1,1)$	$(1,-1)$
$(-1,-1)$	$(-1,-1)$	$(-1,1)$	$(1,-1)$	$(1,1)$

Lze jednoduše ukázat, že každá grupa má právě jeden neutrální prvek, právě jeden inverzní prvek ke každému prvku a že v grupě můžeme jakoukoli rovnost bez obav krátit, tzn. vynásobit inverzním prvkem obě strany rovnosti zleva nebo zprava.

Ve třetí kapitole bude užitečné znát ještě jeden pojem, a to tzv. *řád prvku*. Řád prvku a grupy $(G, \cdot)$ je nejmenší přirozené číslo n takové, že $a^n = 1$. Pokud žádné takové n neexistuje, říkáme, že řád daného prvku je nekonečno. Například v grupě $(\mathbb{Q}, \cdot)$ je řád prvku 1 roven jedné a řád všech ostatních prvků nekonečnu, v grupě $\{(1,1),(1,-1),(-1,1),(-1,-1)\}$ popsané výše je řád prvku $(1,1)$ roven jedné a řád všech ostatních prvků roven dvěma. V grupě $\{1,-1,i,-i\}$ s operací násobení je řád prvku 1 roven jedné, u prvku -1 je roven dvěma a u prvků $\pm i$ je roven čtyřem, protože $(\pm i)^2 = -1, (\pm i)^3 = (-1)(\pm i) = \mp i, (\pm i)^4 = = (-1)^2 = 1$.

Abychom mohli hovořit o kvadratických zbytcích, je nejprve vhodné si připomenout pojem množina zbytkových tříd. Máme-li dané přirozené číslo n, můžeme pro každé celé číslo určit, jaký má zbytek po dělení n. Tím nám vzniknou množiny celých čísel se stejným zbytkem po dělení n – tzv. *zbytkové třídy modulo n*. Např. pro $n = 3$ jsou to množiny $\{\dots,-3,0,3,\dots\}$, $\{\dots,-2,1,4,\dots\}$, $\{\dots,-1,2,5,\dots\}$. Vidíme, že tyto množiny jsou vždy disjunktní a jejich sjednocením dostaneme opět množinu celých čísel.

Fakt, že dvě celá čísla a, b leží ve stejné zbytkové třídě modulo n, značíme $a \equiv b \pmod{n}$ a říkáme, že a je *kongruentní* s b modulo n. Zbytkovou třídu modulo n obsahující celé číslo m značíme $[m]_n$. Množinu všech zbytkových tříd modulo n budeme značit jako $\mathbb{Z}/n\mathbb{Z}$.

Mezi třídami můžeme definovat operace sčítání a násobení pomocí reprezentantů – vybereme z každé z obou tříd libovolné číslo a provedeme danou operaci s nimi. Součtem (resp. součinem) těchto tříd je pak ta třída, která obsahuje součet (resp. součin) zvolených reprezentantů. Jinou volbou reprezentantů se výsledek operace nezmění: zvolíme-li si libovolného reprezentanta $an + k$ třídy $[k]_n$ a reprezetnanta $bn + l$ třídy $[l]_n$, kde a, b, k, l jsou nějaká celá čísla, jejich sečtením dostaneme celé číslo tvaru $(a + b)n + (k + l)$, tedy vždy reprezentanta třídy $[k + l]_n$, jejich vynásobením celé číslo tvaru $(abn + al + bk)n + kl$, tedy reprezentanta třídy $[kl]_n$. Tudíž jsou výše uvedeným postupem opravdu korektně definované operace na množině $\mathbb{Z}/n\mathbb{Z}$. Při počítání se zbytkovými třídami často používáme reprezentanty $\{0, 1, ..., n-1\}$ nebo $\left\{\lfloor -\frac{n}{2} \rfloor + 1, \lfloor -\frac{n}{2} \rfloor + 2, ..., \lfloor \frac{n}{2} \rfloor - 1, \lfloor \frac{n}{2} \rfloor\right\}$ (kde $\lfloor r \rfloor$ značí dolní celou část racionálního čísla r).

Není těžké dokázat, že pro jakékoli $n \in \mathbb{N}$ tvoří množina zbytkových tříd modulo n spolu s operací sčítání pomocí reprezentantů grupu. Tato operace je jistě asociativní. Neutrální prvek je zbytková třída obsahující nulu. A inverzní prvek k třídě $[a]_n$ je třída $[-a]_n$.

Jak je na tom ale množina zbytkových tříd modulo n vůči násobení? Poznamenejme nejprve, že operace sčítání a násobení jsou na množině $\mathbb{Z}$ distributivní, tj. pro všechna $x, y, z \in \mathbb{Z}$ platí $x(y+z) = xy + xz, (y+z)x = yx + zx$. Proto je tedy distributivní i sčítání a násobení pomocí reprezentantů na množině $\mathbb{Z}/n\mathbb{Z}$. Také můžeme říci, že je násobení pomocí reprezentantů komutativní a asociativní.

Sestrojme nyní multiplikativní tabulku násobení v množině zbytkových tříd modulo 7 (uvažujme jen ty neobsahující nulu a pro stručnost zápisu budeme místo tříd psát jejich reprezentanty):

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Vidíme, že jsme dostali grupu! Násobení reprezentantů je asociativní operace na množině $\mathbb{Z}/n\mathbb{Z} \setminus \{[0]_n\}$. Zbytková třída reprezentovaná jedničkou hraje roli neutrálního prvku a ke každému prvku můžeme v tabulce nalézt inverzi (třídy $[2]_7$ a $[4]_7$ jsou navzájem svými inverzními prvky, stejně tak třídy $[3]_7$ a $[5]_7$, třída $[6]_7$ je sama svým inverzním prvkem).

Takové množině T, na které jsou zavedeny operace sčítání a násobení tak, že se sčítáním tvoří komutativní grupu a její podmnožina $T \setminus \{0\}$ (kde 0 je neutrální prvek vůči sčítání) tvoří komutativní grupu s násobením, přičemž tyto dvě operace jsou navíc distributivní na T, říkáme *těleso*.

Bohužel k takto krásnému výsledku nedojdeme vždy. Podíváme-li se na množinu zbytkových tříd modulo 4 bez nuly s násobením, dostáváme multiplikativní tabulku o poznání méně pěknou:

	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Jednička sice opět hraje roli neutrálního prvku, ale určitě nemůžeme říci, že by měl každý prvek svoji inverzi. Dokonce pokud se třída $[2]_4$ násobí sama se sebou, výsledkem je třída $[0]_4$.

Pokud množina T tvoří se sčítáním grupu, ale vůči násobení si zachová pouze vlastnost asociativity a existence neutrálního prvku, a navíc jsou tyto operace na T distributiviní, říkáme, že T je *okruh*. Vidíme tedy, že každé těleso je okruh, ale naopak to určitě být nemusí.

Lze ukázat, že množina zbytkových tříd modulo n s operacemi sčítání a násobení definovanými pomocí reprezentantů je okruh pro jakékoli přirozené n. Tento okruh je navíc těleso, právě když n je prvočíslo.

Vrátíme-li se k multiplikativní tabulce v $\mathbb{Z}/4\mathbb{Z}$, všimněme si, že některé prvky mají svoji inverzi, a to konkrétně třídy obsahující jedničku a trojku, tedy čísla s čtyřkou nesoudělná.

Je možné ukázat, že pro jakékoli přirozené n můžeme najít inverzní prvek právě ke všem zbytkovým třídám s reprezentanty nesoudělnými s n. Množina takovýchto prvků tvoří vůči násobení grupu, kterou nazýváme *grupa jednotek okruhu* a značíme ji $(\mathbb{Z}/n\mathbb{Z})^*$. Jako příklad uvedu multiplikativní tabulku v grupě $(\mathbb{Z}/12\mathbb{Z})^*$:

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Na závěr tohoto oddílu ještě uvedu bez důkazu dva významné poznatky z elementární teorie čísel, které budou v dalším textu využity, a to čínskou zbytkovou větu a Bezoutovu rovnost. První z nich souvisí s řešitelností soustav kongruencí modulo různá celá čísla (řešením soustavy kongruencí rozumíme právě takové celé číslo x, pro které všechny kongruence soustavy platí):

Věta 1.1.1. *Nechť $m_1, m_2, ..., m_r$ jsou po dvou nesoudělná přirozená čísla větší než jedna. Potom pro libovolná $a_1, a_2, ..., a_r \in \mathbb{Z}$ platí, že soustava kongruencí*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

má řešení x, které je jednoznačně určeno modulo $m_1 m_2 \cdots m_r$.

Bezoutova rovnost popisuje vztah mezi dvěma celými čísly a jejich největším společným dělitelem:

Věta 1.1.2. *Nechť a, b jsou nějaká celá čísla, $d = \mathrm{nsd}(a, b)$. Potom existují celá čísla u, v taková, že $ua + vb = d$.*

Definovali jsme základní pojmy, které budeme v celé práci potřebovat. Nyní už se můžeme pustit do studia kvadratických zbytků.

1.2 Kvadratické zbytky a Legendreův symbol

Pojem kvadratický zbytek se vztahuje právě k okruhu zbytkových tříd modulo m.

Definice 1.2.1. *O celém čísle a nesoudělném s přirozeným číslem m řekneme, že je kvadratický zbytek modulo m, pokud existuje nějaké $c \in \mathbb{Z}$ takové, že $a \equiv c^2 \pmod{m}$. Pokud žádné takové c neexistuje, říkáme, že a je kvadratický nezbytek modulo m.*

Není velký problém určit kvadratické zbytky modulo liché prvočíslo. Zkusme určit všechny kvadratické zbytky modulo jedenáct. Zbytkové třídy si zapíšeme pomocí reprezentantů jako $\pm1, \pm2, \pm3, \pm4, \pm5$. Neuvažujeme třídu obsahující nulu, leží v ní totiž násobky jedenáctky, které podle definice kvadratickými zbytky být nemohou. Všechny tyto třídy umocníme na druhou modulo 11: $(\pm1)^2 \equiv 1$, $(\pm2)^2 \equiv 4$, $(\pm3)^2 \equiv 9$, $(\pm4)^2 \equiv 5$, $(\pm5)^2 \equiv 3$. Tedy celé číslo a je kvadratický zbytek modulo 11 právě tehdy, když $a \equiv 1, 3, 4, 5, 9 \pmod{11}$. Předchozí úvahu lze zobecnit pro libovolné liché prvočíslo. Všechny kvadratické zbytky modulo p jsou tedy tvaru $1^2, 2^2, ..., (\frac{p-1}{2})^2$. Můžeme jednoduše ukázat, že se opravdu jedná o $\frac{p-1}{2}$ různých zbytků: kdyby totiž pro dvě celá čísla m, n, $0 < m < n \leq \frac{p-1}{2}$, platilo $m^2 \equiv n^2 \pmod{p}$, dostali bychom $0 \equiv m^2 - n^2 \equiv (m+n)(m-n) \pmod{p}$, a tedy p dělí součin $(m+n)(m-n)$. Pokud ale prvočíslo dělí součin, musí dělit alespoň jednoho z činitelů, tedy p dělí $m+n$ nebo $m-n$, což je ve sporu s tím, jak jsme volili čísla m, n. Poznamenejme ještě, že jelikož pro každé liché prvočíslo p máme právě $\frac{p-1}{2}$ kvadratických zbytků, zbývá nám tedy nutně rovněž $\frac{p-1}{2}$ kvadratických nezbytků. U předchozího příkladu $p = 11$ vidíme, že celé číslo a je kvadratický nezbytek, právě když $a \equiv 2, 6, 7, 8, 10 \pmod{11}$.

Jsme tedy schopni rozhodnout, zda je nějaké celé číslo kvadratickým zbytkem modulo dané liché prvočíslo. Jak ale určit, modulo které liché prvočíslo je dané celé číslo kvadratickým zbytkem? Abychom si na tuto a další otázky mohli odpovědět, musíme se seznámit s Legendreovým symbolem a zákonem kvadratické reciprocity.

Definice 1.2.2. *Nechť $a \in \mathbb{Z}$ a p je liché prvočíslo. Pak Legendreův symbol $\left(\frac{a}{p}\right)$ je definován následovně:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{pokud je } a \text{ kvadratický zbytek modulo } p, \\ 0 & \text{pokud } p \text{ dělí } a, \\ -1 & \text{pokud je } a \text{ kvadratický nezbytek modulo } p. \end{cases}$$

Toto značení nám usnadňuje počítání s kvadratickými zbytky. Je třeba si všimnout, že pokud $m \equiv n \pmod{p}$, tak $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$, tedy zbytková třída zachovává Legendreův symbol. Mezi další významné vlastnosti Legendreova symbolu patří následující:

Věta 1.2.1. *Pro všechna $a \in \mathbb{Z}$ a všechna lichá prvočísla p platí*

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

Důkaz. Vzpomeňme si na jeden z nejdůležitějších poznatků elementární teorie čísel, malou Fermatovu větu, která nám říká, že pro všechna celá čísla a, která nejsou dělitelná daným prvočíslem p, platí

$$a^{p-1} \equiv 1 \pmod{p}.$$

Tedy $p \mid (a^{p-1} - 1) = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$. Pokud ale prvočíslo dělí součin celých čísel, dělí nutně alespoň jednoho z činitelů, tudíž $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$.

Tvrzení je jistě pravdivé, jestliže $p|a$. Pokud $\left(\frac{a}{p}\right) = 1$, tak existuje nějaké $m \in \mathbb{Z}$ tak, že $a \equiv m^2 \pmod{p}$. Potom ale $a^{\frac{p-1}{2}} \equiv m^{p-1} \equiv 1 \pmod{p}$. Předpokládejme nyní $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Všechna taková a jsou kořeny polynomu $x^{\frac{p-1}{2}} - 1$. Zde mi čtenář bude muset uvěřit jedno tvrzení známé z teorie okruhů (důkaz lze najít např. v [2]), totiž to, že takový polynom může mít nejvýše tolik kořenů modulo p, kolik je jeho stupeň, tedy nejvýše $\frac{p-1}{2}$. Ale my už víme, že jich má právě tolik, totiž $1^2, 2^2, ..., (\frac{p-1}{2})^2$. To jsou ale všechno kvadratické zbytky.

Zatím jsme ukázali, že $\left(\frac{a}{p}\right) = 1$, právě když $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Pro zbývající celá čísla a nesoudělná s p ale vzhledem k předchozímu platí nejen $\left(\frac{a}{p}\right) = -1$, ale i $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Tím je tedy tvrzení dokázáno. □

Podstatným důsledkem tohoto tvrzení je, že pro celá čísla a, b a liché prvočíslo p vždy platí $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$. To lze dokázat pomocí předchozí věty přímým výpočtem: $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}$.

Abychom mohli počítat s kvadratickými zbytky, je potřeba znát ještě několik dalších vztahů. Ty však uvádím bez důkazu, protože přesahují rámec této práce.

Věta 1.2.2. *Nechť p, q jsou různá lichá prvočísla. Potom:*

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$,
3. $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}$.

Třetí z těchto vztahů se nazývá zákon kvadratické reciprocity a je pro počítání s kvadratickými zbytky zcela zásadní.

Uvedli jsme si nyní dost vlastností na to, abychom byli schopni počítat s Legendreovými symboly. Zamysleme se nad následujícím příkladem: pro která lichá prvočísla p existuje celé číslo x takové, že $p \mid (x^2 + 5)$?

Vidíme, že tento příklad je ekvivalentní otázce, pro která lichá prvočísla p je -5 kvadratický zbytek modulo p. Zkusme to tedy zjistit. Počítejme: $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{5}{p}\right) = = (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right) \cdot (-1)^{\frac{(p-1)(5-1)}{4}} = (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right) \cdot (-1)^{p-1} = (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right)$. (Využili jsme vztahů 1 a 3 z předchozí věty a navíc faktu, že jelikož p je liché prvočíslo, tak $p-1$ je číslo sudé a tedy $(-1)^{p-1} = 1$.) Tedy požadujeme $(-1)^{\frac{p-1}{2}} = \left(\frac{p}{5}\right) = \pm 1$. Abychom zjistili hodnoty prvního výrazu, musíme se podívat, jaký zbytek dává p po dělení čtyřmi, hodnotu druhého výrazu zjistíme, podíváme-li se, jaký dává p zbytek po dělení pěti. To už je ale problém velmi jednoduchý:

$p \mod 4$	$(-1)^{\frac{p-1}{2}}$	$p \mod 5$	$\left(\frac{p}{5}\right)$
1	1	± 1	1
3	-1	± 2	-1

Aby tedy bylo číslo -5 kvadratickým zbytkem modulo liché prvočíslo p, musí p splňovat buď $p \equiv 1 \pmod 4, p \equiv \pm 1 \pmod 5$, nebo $p \equiv 3 \pmod 4, p \equiv \pm 2 \pmod 5$. To jsou vlastně čtyři soustavy kongruencí, podle čínské zbytkové věty tedy získáváme právě čtyři řešení modulo dvacet: $p \equiv 1, 3, 7, 9 \pmod{20}$. Tato kongruence je tedy nutná a postačující podmínka k tomu, aby platilo $\left(\frac{-5}{p}\right) = 1$. Uveďme ještě několik vhodných příkladů pro konkrétní prvočísla. Například $-5 \equiv 6^2 \pmod{41}$, $-5 \equiv 8^2 \pmod{23}$, $-5 \equiv 3^2 \pmod 7$, $-5 \equiv 11^2 \pmod{29}$.

Nevýhodou Legenderova symbolu je, že se v jeho „jmenovateli“ může nacházet pouze liché prvočíslo. To může být v některých ohledech značně omezující podmínka. Proto byl zaveden tzv. *Jacobiho symbol*, který je jednoduchým zobecněním Legendreova symbolu: pro celé číslo m a liché přirozené číslo n je definován jako

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right),$$

přičemž $n = p_1 p_2 \cdots p_r$ je prvočíselný rozklad n a $\left(\frac{m}{p_i}\right)$ jsou Legendreovy symboly.

Uvědomme si, že pokud je m kvadratický zbytek modulo n, je také kvadratický zbytek modulo p_i, kde p_i je libovolný prvočíselný dělitel čísla n. Tedy pokud je m kvadratický zbytek modulo n, tak $\left(\frac{m}{n}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right) = 1$. Narozdíl od Legendreova symbolu to ale neplatí naopak, pokud $\left(\frac{m}{n}\right) = 1$, neznamená to ještě, že je m kvadratický zbytek modulo n. Například $\left(\frac{2}{39}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{13}\right) = (-1) \cdot (-1) = 1$, ale 2 není kvadratický zbytek modulo 39.

Pro Jacobiho symboly platí analogie předchozích uvedených vztahů platných pro Legendreovy symboly.

Věta 1.2.3. *Nechť $M, N \in \mathbb{Z}$ a m, n jsou lichá přirozená čísla. Pak platí následující vztahy:*

1. $\left(\frac{MN}{m}\right) = \left(\frac{M}{m}\right) \cdot \left(\frac{N}{m}\right)$,
2. $\left(\frac{M}{mn}\right) = \left(\frac{M}{m}\right) \cdot \left(\frac{M}{n}\right)$,
3. $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$,
4. $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$,
5. $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) \cdot (-1)^{\frac{(m-1)(n-1)}{4}}$.

Navíc pro Jacobiho symboly platí tato užitečná vlastnost: pokud $m \equiv n \pmod D$, kde m, n jsou lichá přirozená čísla a $D \equiv 0, 1 \pmod 4$, tak $\left(\frac{D}{m}\right) = \left(\frac{D}{n}\right)$. Důkaz neuvádím, protože je poměrně dlouhý a pro následující text nemá žádný význam.

V 1. kapitole jsme se seznámili s definicemi grupy, okruhu a tělesa, ujasnili si pojem zbytkové třídy a seznámili jsme se s kvadratickými zbytky. Pro lepší práci s nimi jsme zavedli Legendreův a Jacobiho symbol a poznali jsme některé jejich důležité vlastnosti. Máme tedy dostatečný aparát, abychom se mohli pustit do studia kvadratických forem.

Kapitola 2

Kvadratické formy

U zrodu teorie kvadratických forem stáli slavní matematici jako Lagrange, Legendre nebo Gauss. Motivací pro detailní výzkum vlastností těchto objektů byla otázka: máme-li dáno přirozené číslo n, jaká lichá prvočísla lze vyjádřit ve tvaru x^2+ny^2 pro nějaká celá čísla x, y? Pro $n = 1$ můžeme tento problém vyřešit elementárními metodami, podobným způsobem lze postupovat i v případě $n = 2$ a $n = 3$. Pro vyšší n jsou však tyto postupy nedostačující. Uvidíme, že právě kvadratické formy tvaru $x^2 + ny^2$ hrají v teorii, kterou vybudujeme, důležitou roli.

2.1 Základní poznatky o kvadratických formách

Nejprve je nutno definovat, co kvadratická forma vlastně je.

Definice 2.1.1. *Kvadratickou formou rozumíme objekt tvaru $f(x, y) = ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{Z}$. Za x a y dosazujeme celá čísla.*

Ve středoškolské matematice se můžeme setkat s polynomy jedné proměnné – výrazy ve tvaru $f(x) = \sum_{i=0}^{n} a_i x^i$. Kvadratická forma je tedy jakýsi polynom dvou celočíselných proměnných x, y ve speciálním tvaru. Vidíme také, že pro $a = 1, b = 0, c = n$ získáváme tvar $f(x, y) = x^2 + ny^2$.

Definice 2.1.2. *Nechť $f(x, y) = ax^2 + bxy + cy^2$ je kvadratická forma a $m \in \mathbb{Z}$.*

O formě $f(x, y)$ řekneme, že je primitivní, pokud jsou koeficienty a, b, c nesoudělné.

O číslu m řekneme, že je reprezentováno formou $f(x, y)$, pokud za x a y můžeme dosadit celá čísla u, v tak, aby platilo $m = f(u, v)$. Pokud navíc platí, že u a v jsou nesoudělná, nazýváme tuto reprezentaci vhodnou.

Pro ujasnění pojmů uvedu několik příkladů. Forma $4x^2 + 12xy + 6y^2$ není primitivní, protože všechny její koeficienty jsou dělitelné dvojkou. Naopak formy $2x^2 + 5xy + 4y^2$ nebo $x^2 + 42xy + 15y^2$ primitivní jsou. Čísla reprezentovaná formou $6x^2 + xy + y^2$ jsou například 32 (pro $x = y = 2$), 39 (pro $x = 2, y = 3$), 36 (pro $x = 1, y = 5$), přičemž poslední dvě

z nich jsou reprezentována vhodně. Forma $x^2+2xy+y^2$ reprezentuje právě druhé mocniny celých čísel.

Nyní se seznámíme s pojmem, který má v teorii kvadratických forem zásadní význam.

Definice 2.1.3. *O dvou kvadratických formách $f(x,y), g(x,y)$ řekneme, že jsou ekvivalentní, pokud existují vhodná celá čísla p,q,r,s tak, aby $f(x,y) = g(px+qy, rx+sy)$ a $ps-qr = \pm 1$. Pokud navíc $ps-qr = 1$, říkáme o ekvivalenci, že je vhodná, pokud $ps-qr = -1$, tak je nevhodná.*

Tato definice není zcela intuitivní; jak taková ekvivalence vypadá, ukažme na příkladu. Uvažujme formu $f(x,y) = 3x^2 + 2xy + 5y^2$. Zkusme k ní nalézt nějakou ekvivalentní formu. Položme $p = 2, q = 3, r = 1, s = 2$. Pak forma $g(x,y) = f(2x+3y, x+2y) = 3(2x+3y)^2+2(2x+3y)(x+2y)+5(x+2y)^2 = 21x^2+70xy+59y^2$ je forma s ní ekvivalentní, a to dokonce vhodně, protože $ps-qr = 2\cdot 2 - 3\cdot 1 = 1$.

Je nutné poznamenat, že lze ukázat, že forma ekvivalentní s primitivní formou je také primitivní.

Jaký má vůbec význam definovat takovou na první pohled podivnou skutečnost? Nesmírný. S pomocí některých poznatků o maticích můžeme totiž snadno ukázat, že ekvivalence dvou forem je relace ekvivalence v pravém slova smyslu – je to tedy relace reflexivní (forma je ekvivalentní sama se sebou), symetrická (pokud je f ekvivalentní s g, tak je i g ekvivalentní s f) a transitivní (pokud je f ekvivalentní s g a g ekvivalentní s h, je také f ekvivalentní s h). Příkladů relace ekvivalence můžeme ve středoškolské matematice najít mnoho – např. relace rovnosti prvků nějaké množiny, relace rovnoběžnosti přímek či rovin, nebo kongruence dvou celých čísel modulo n.

Z tohoto faktu (konkrétně symetrie ekvivalence dvou forem) plyne podstatný poznatek:

Věta 2.1.1. *Dvě ekvivalentní kvadratické formy reprezentují tatáž čísla.*

Důkaz. Nechť $f(x,y) = g(px+qy, rx+sy)$, kde p,q,r,s splňují naše podmínky. Pak ke každému m reprezentovanému formou f můžeme najít $u,v \in \mathbb{Z}$ tak, že $f(u,v) = m$. Ale pak také existují celá čísla $k = pu+qv, l = ru+sv$ taková, že $g(k,l) = m$. Tedy všechna čísla reprezentovaná formou f jsou reprezentována i formou g. Jelikož relace ekvivalence dvou kvadratických forma je symetrická, existují také celá čísla P,Q,R,S taková, že $g(x,y) = f(Px+Qy, Rx+Sy), PS-QR = \pm 1$. Tedy můžeme obdobně ukázat, že všechna čísla reprezentovaná formou g jsou reprezentována formou f. Obě formy tedy reprezentují ta samá čísla. □

Ekvivalence kvadratických forem dokonce zachovává vhodnou reprezentaci. Důkaz je jednoduchý: nechť $m = f(u,v) = g(pu+qv, ru+sv)$ stejně jako výše. Předpokládejme, že $\mathrm{nsd}(u,v) = 1$. Nechť $\mathrm{nsd}(pu+qv, ru+sv) = k$. Pak $k|(s(pu+qv) - q(ru+sv)) = (ps-qr)u = \pm u$, ale také $k|(r(pu+qv) - p(ru+sv)) = (qr-ps)v = \pm v$, tedy $k = 1$. Tudíž pokud je m reprezentováno formou $f(x,y)$ vhodně, tato vlastnost se pro formu ekvivalentní s f zachová.

Pokud máme danou kvadratickou formu $f(x, y)$ a nějaké celé číslo m, zatím nemáme žádné prostředky k tomu, abychom určili, zda je m touto formou reprezentováno. Motivací k následujícím úvahám je mimo jiné snaha určit podmínky, které číslo musí splňovat, aby bylo reprezentováno nějakou formou.

Věta 2.1.2. *Forma $f(x, y) = ax^2 + bxy + cy^2$ vhodně reprezentuje celé číslo m, právě když existují celá čísla k, l tak, že je $f(x, y)$ vhodně ekvivalentní s formou $mx^2 + kxy + ly^2$.*

Důkaz. Musíme dokázat dvě implikace. Nejprve ukažme, že pokud pro nějaká dvě nesoudělná celá čísla p, q platí $f(p, q) = m$, tak je forma $f(x, y)$ vhodně ekvivalentní s formou $mx^2+kxy+ly^2$ pro nějaká celá čísla k, l. Jelikož $\mathrm{nsd}(p, q) = 1$, Bezoutova rovnost nám říká, že existují celá čísla q, s taková, že $ps-qr = 1$. Potom $f(px+ry, qx+sy)$ je po roznásobení a úpravě rovno $f(p, q)x^2 + (2apr + bps + brq + 2cqs)xy + f(r, s)y^2 = mx^2 + kxy + ly^2$.

Abychom ukázali opačnou implikaci, stačí si uvědomit, že pokud jsou formy $f(x, y)$ a $mx^2+kxy+ly^2$ vhodně ekvivalentní, vhodně reprezentují tatáž čísla. Jelikož při dosazení $(x, y) = (1, 0)$ dostáváme $mx^2 + kxy + ly^2 = m$, tak forma $f(x, y)$ jistě také reprezentuje číslo m. Jelikož $\mathrm{nsd}(1, 0) = 1$, je tato reprezentace vhodná. □

Nyní zavedeme pojem, který nám velmi usnadní orientaci mezi kvadratickými formami.

Definice 2.1.4. *Nechť $f(x, y) = ax^2 + bxy + cy^2$ je kvadratická forma. Celému číslu $D = b^2 - 4ac$ říkáme diskriminant této formy.*

Pojem diskriminant známe už ze základní školy. Bylo to číslo definované podobně jako nyní a určovalo počet řešení kvadratické rovnice a tvar těchto řešení. I diskriminant kvadratické formy je číslo velice užitečné. Pro ekvivalentní formy se totiž nemění! Nechť D (resp. D') je diskriminant formy $f(x, y)$ (resp. $g(x, y)$) a navíc jsou tyto formy ekvivalentní, tedy $f(x, y) = g(px + qy, rx + sy)$, $p, q, r, s \in \mathbb{Z}, ps - qr = \pm 1$. Pak přímým výpočtem můžeme dojít ke vztahu $D = (ps - qr)^2 D' = D'$.

Diskriminant nám říká jednu podstatnou věc o číslech reprezentovaných nějakou formou. Pro $f(x, y) = ax^2 + bxy + cy^2$ totiž platí rovnost $4af(x, y) = (2ax + by)^2 – Dy^2$ (platnost rovnosti je možno si ověřit jednoduchým výpočtem). Z této jednoduché úpravy plyne, že pokud je diskriminant záporný, tak daná forma reprezentuje kromě nuly pouze kladná či pouze záporná čísla (podle znaménka koeficientu a). Formy se záporným diskriminantem nazýváme *pozitivně definitní*, pokud je koeficient a kladný. Pokud jsou diskriminant i koeficient a zápornými čísly, formě říkáme *negativně definitní*. Naopak formám s kladným diskriminantem říkáme *indefinitní*. Je možné ukázat, že indefinitní formy mohou reprezentovat čísla kladná i záporná.

Všimněme si ještě jedné věci. Jelikož $D = b^2-4ac$, tak $D \equiv 0, 1 \pmod 4$. Můžeme tedy říct, že koeficient b je sudý (resp. lichý), právě když je diskriminant kongruentní s nulou (resp. jedničkou) modulo 4.

Následující věta nám řekne nutnou a postačující podmínku pro to, aby bylo číslo m vhodně reprezentováno některou primitivní formou diskriminantu D:

Věta 2.1.3. *Nechť $D \equiv 0, 1 \pmod 4$ a m je liché přirozené číslo nesoudělné s D. Pak existuje primitivní forma diskriminantu D vhodně reprezentující m právě tehdy, když je D kvadratický zbytek modulo m.*

Důkaz. Nejprve předpokládejme, že forma $f(x, y)$ vhodně reprezentuje m. Protože vhodná ekvivalence zachovává diskriminant, můžeme bez újmy na obecnosti na základě věty 2.1.2 předpokládat $f(x, y) = mx^2 + bxy + cy^2$. Tedy $D = b^2 - 4mc \Rightarrow D \equiv b^2 \pmod m$ a tedy D kvadratický zbytek modulo m, což jsme chtěli.

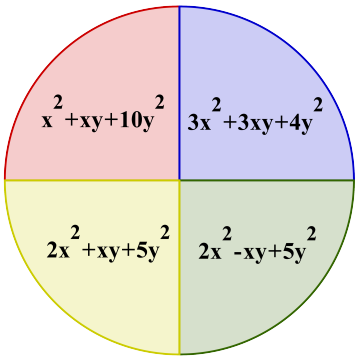
Nyní předpokládejme, že existuje přirozené číslo b takové, že $D \equiv b^2 \pmod m$. Jelikož m je liché, můžeme předpokládat, že b a D mají stejnou paritu – nezapomeňme, že se stále pohybujeme v okruhu zbytkových tříd a pokud mají D a b paritu různou, b můžeme vyměnit za $b + m$, reprezentanta stejné zbytkové třídy modulo m. Tedy $D \equiv b \pmod 2$ a navíc $D \equiv 0, 1 \pmod 4$, dohromady tedy $D \equiv b^2 \pmod 4$ a spolu s předchozím konečně $D \equiv b^2 \pmod{4m}$. To znamená, že $D = b^2 - 4mc$ pro nějaké $c \in \mathbb{Z}$. Tudíž forma $mx^2 + bxy + cy^2$ diskriminantu D vhodně reprezentuje m, a tato forma je primitivní, jelikož její koeficienty jsou nesoudělné díky požadavku nesoudělnosti m a D. □

Tato věta má následující důsledek: nechť $n \in \mathbb{N}$ a p je liché prvočíslo, které nedělí n. Pak $\left(\frac{-n}{p}\right) = 1$ právě tehdy, když je p vhodně reprezentováno primitivní formou diskriminantu $-4n$.

Poprvé si můžeme všimnout přínosu teorie kvadratických forem při hledání prvočísel tvaru $x^2 + ny^2$. Otázka, která lichá prvočísla můžeme napsat ve tvaru $x^2 + ny^2$, je ekvivalentní otázce, která lichá prvočísla jsou vhodně reprezentována kvadratickou formou $x^2 + ny^2$. To je forma diskriminantu $-4n$ a tedy vidíme, že pro všechna hledaná prvočísla musí platit $\left(\frac{-n}{p}\right) = 1$.

Diskriminant a vhodná ekvivalence forem nám pomohli vnést do světa kvadratických forem trochu světla. Můžeme je nyní roztřídit na množiny forem stejného diskriminantu a dokážeme říct, co musí číslo splňovat, aby bylo nějakou z těchto forem vhodně reprezentováno. Na množině forem daného diskriminantu můžeme také díky relaci ekvivalence provést totéž, co v případě zbytkových tříd: rozdělit nosnou množinu na tzv. *třídy ekvivalence* (v předchozím případě jsme pro ně měli speciální název – zbytkové třídy modulo m). To totiž můžeme provést vždy, když máme na množině definovou relaci ekvivalence. Z vlastností tohoto druhu relace plyne, že třídy ekvivalence jsou disjunktní, tj. průnikem dvou různých tříd je prázdná množina, a jejich sjednocením je celá nosná množina.

V případě, kdy je nosnou množinou množina všech primitivních forem daného diskriminantu, tedy pomocí vhodné ekvivalence dostáváme třídy ekvivalence. Výše jsme si navíc ukázali, že všechny formy jedné třídy reprezentují tatáž čísla. Pořád však mnoho nevíme. Neurčili jsme, zdali je tříd ekvivalence konečně mnoho či ne, nejsme schopni třídy charakterizovat nějakým význačným reprezentantem, jako tomu bylo u zbytkových tříd. V onom případě jsme dokonce mezi třídami zavedli operaci a zformovali grupu. Nabízí se otázka, je-li něco takového možné i v případě kvadratických forem. Smyslem dalšího textu bude tuto teorii vybudovat.



Na obrázku můžeme vidět schematické znázornění výše popisované situace u množiny primitivních kvadratických forem diskriminantu $D = -39$. Nosná množina je znázorněna kruhem, který je rozdělen na čtvrtiny představující třídy ekvivalence. V každé čtvrtině je navíc uveden jeden zástupce – zanedlouho uvidíme, že tito reprezentanti nebyli zvoleni náhodně.

V následujícím textu se budeme zabývat pouze pozitivně definitními kvadratickými formami, tedy těmi se záporným diskriminantem a kladným koeficientem u x^2. Jejich teorie je totiž přehlednější a je snad možno i říci, že elegantnější. Také mezi nimi leží formy $x^2 + ny^2$.

Jako reprezentanty tříd ekvivalence obvykle volíme ty v nějakém smyslu nejmenší. Svým způsobem „nejmenší“ formy matematici objevili i v případě kvadratických forem – všechny požadavky splňuje tzv. redukovaná forma.

Definice 2.1.5. *O primitivní pozitivně definitní formě $f(x, y) = ax^2 + bxy + cy^2$ řekneme, že je redukovaná, pokud $|b| \leq a \leq c$, a navíc pokud $|b| = a$ nebo $a = c$, tak $b \geq 0$.*

Na obrázku výše jsme mohli vidět všechny redukované formy diskriminantu -39 – $x^2 + xy + 10y^2$, $3x^2 + 3xy + 4y^2$, $2x^2 \pm xy + 5y^2$. Další příklady: formy $2x^2 + xy + 5y^2, x^2 + xy + y^2, 4x^2 - 2xy + 7y^2$ jsou redukované, naopak formy $2x^2 - 2xy + 3y^2, 2x^2 + 7xy + 3y^2, 5x^2 - xy + 5y^2$ redukované nejsou. Forma $x^2 + ny^2$ je pro každé přirozené číslo n redukovaná.

Přínos redukovaných forem nám ukáže následující věta:

Věta 2.1.4. *Každá primitivní pozitivně definitní forma je vhodně ekvivalentní s právě jednou redukovanou formou.*

Důkaz. Důkaz této věty nevyžaduje žádné pokročilé znalosti, ale je velmi zdlouhavý a technicky náročný. Uvedu tedy pouze ideu důkazu.

Nejprve ukážeme, že daná forma f je vhodně ekvivalentní nějaké formě splňující podmínku $|b| \leq a \leq c$. Abychom snížili koeficient b, vytvoříme vhodně ekvivalentní formu

$g(x,y) = f(x+my,y)$, kde m je dobře zvolené celé číslo. Pokud ve výsledku platí $a > c$, tak koeficienty vyměníme postupem $h(x,y) = g(-y,x)$. Pokud nyní stále neplatí podmínka $|b| \leq a \leq c$, předchozí postup opakujeme, dokud nedostaneme formu tuto podmínku splňující.

Dále je nutno dokázat, že forma, kterou jsme vytvořili, je vhodně ekvivalentní nějaké redukované formě. Podmínka $|b| \leq a \leq c$ je již splněna, zbývá pouze vyřešit případ, kdy $b < 0$, ale $-b = a$ nebo $a = c$. V případě $a = -b$ stačí nahradit $(x,y) \to (x+y,y)$, v případě $a = c$ provést $(x,y) \to (-y,x)$.

Tím jsme dokázali, že každá primitivní pozitivně definitní forma je vhodně ekvivalentní s nějakou redukovanou. Nyní je nutno ukázat, že tato redukovaná forma je právě jedna. K tomu stačí dokázat, že dvě redukované formy nemohou být vhodně ekvivalentní. Tuto část důkazu úplně vynechám, opravdu není nezbytné, aby ji čtenář znal. □

Všimněme si, že uvedená část důkazu je konstruktivní, dává nám totiž návod, jak redukovanou formu sestrojit. Podívejme se například na formu $f(x,y) = 3x^2+19xy+32y^2$. Vytvořme redukovanou formu vhodně ekvivalentní s f. Nejprve snížíme koeficient u xy: $g(x,y) = f(x-3y,y) = 3x^2 - 18xy + 27y^2 + 19xy - 57y^2 + 32y^2 = 3x^2 + xy + 2y^2$. Nyní je třeba vyměnit koeficienty u x^2 a y^2: $h(x,y) = g(-y,x) = 2x^2 - xy + 3y^2$. Tato forma již redukovaná je.

Konstruktivita důkazu nám také udává algoritmus, jak určit, zda jsou dvě dané primitivní pozitivně definitní formy téhož diskriminantu vhodně ekvivalentní: ke každé z obou forem najdeme redukovanou formu s ní vhodně ekvivalentní a pokud nám v obou případech vyšla tatáž, zkoumané formy vhodně ekvivalentní jsou.

Ačkoli důkaz věty 2.1.4 je mechanicky a technicky náročná práce, rozhodně se zúročila. Máme totiž to, oč jsme se snažili – reprezentanty tříd ekvivalence primitivních pozitivně definitních forem daného diskriminantu, se kterými se dá dobře pracovat. Redukovanou formu vhodně ekvivalentní se zadanou formou navíc dokážeme vždy sestrojit. To nás posunulo velmi daleko. Je ale tříd konečně mnoho? Můžeme ukázat, že ano.

Všimněme si následující vlastnosti diskriminantu redukované formy. Z definice jistě $b^2 \leq a^2$ a $a \leq c$, tedy $-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$ a tedy $a \leq \sqrt{\frac{-D}{3}}$. Jelikož D je dáno a $|b| \leq a$, existuje pouze konečně mnoho možností, jak vybrat a i b. A protože $c = \frac{b^2-D}{4a}$, existuje pro zvolená čísla a, b nejvýše jedno c. Redukovaných forem je tudíž konečně mnoho a máme tedy pouze konečně mnoho tříd vhodně ekvivalentních primitivních pozitivně definitních forem daného diskriminantu! Tato skutečnost jistě udělala čtenáři radost.

Množinu tříd vhodně ekvivalentních pozitivně definitních forem daného záporného diskriminantu označujeme jako $C(D)$, jejich počet pak $h(D)$. Vidíme, že $h(D)$ je konečné číslo, na které se zároveň můžeme dívat jako na počet redukovaných forem.

2.2 Redukované formy daného diskriminantu

Zavedli jsme velké množství teorie, zastavme se tedy nyní na chvíli a podívejme se na nějaké příklady. Zkusme najít všechny redukované formy daného diskriminantu.

Například $D = -40$. Hledáme redukované formy $ax^2 + bxy + cy^2$. Víme, že $0 \leq a$, $a \leq \sqrt{\frac{-D}{3}} = \sqrt{\frac{40}{3}}$, tedy $0 \leq a \leq 3$. Dále víme, že $|b| \leq a$ a jelikož D je dělitelé čtyřmi, b musí být sudé, tedy $b = 0$ nebo $b = \pm 2$. Pro $b = 0$ dostáváme $ac = \frac{b^2 - D}{4} = 10$, jelikož $a \leq c$, tak buď $a = 1, c = 10$, nebo $a = 2, c = 10$. Získali jsme tedy redukované formy $x^2 + 10y^2$ a $2x^2 + 5y^2$. Pokud $b = \pm 2$, tak $ac = 11$. Potom se ale a musí rovnat jedné, což je ve sporu s podmínkou $|b| \leq a$. Žádné další redukované formy tohoto diskriminantu již nejsou.

Máme tedy dvě třídy ekvivalence, jejichž reprezentanti jsou redukované formy tvaru $x^2 + 10y^2$ a $2x^2 + 5y^2$. Podívejme se nyní na to, která lichá prvočísla (nedělící diskriminant, tedy různá od pěti) můžeme vyjádřit nějakou formou diskriminantu -40. Víme, že to jsou právě ta prvočísla p, pro které platí, že -10 je kvadratický zbytek modulo p. Počítejme tedy:

$$\left(\tfrac{-10}{p}\right) = \left(\tfrac{-1}{p}\right)\cdot\left(\tfrac{2}{p}\right)\cdot\left(\tfrac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p^2-1}{8}}\cdot\left(\tfrac{p}{5}\right)\cdot(-1)^{\frac{p-1}{2}\cdot\frac{5-1}{2}} = (-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p^2-1}{8}}\cdot\left(\tfrac{p}{5}\right).$$

Aby bylo číslo -10 kvadratický zbytek modulo p, musí být součin těchto tří výrazů roven jedné. Podívejme se jejich možné hodnoty:

$p \bmod 8$	$\left(\frac{-1}{p}\right)$	$\left(\frac{2}{p}\right)$	$p \bmod 5$	$\left(\frac{p}{5}\right)$
1	1	1	1	1
-1	-1	1	2	-1
3	-1	-1	-1	1
-3	1	-1	-2	-1

Aby platilo $\left(\frac{-10}{p}\right) = 1$, musí platit $\left(\frac{-2}{p}\right) = \left(\frac{p}{5}\right) = \pm 1$. Tabulka výše nám říká, že oba symboly jsou:

1. rovny jedné, pokud $p \equiv 1, 3 \pmod 8$, $p \equiv \pm 1 \pmod 5$, celkem tedy $p \equiv 1, 9, 11, 19 \pmod{40}$,

2. rovny mínus jedné, pokud $p \equiv -1, -3 \pmod 8$, $p \equiv \pm 2 \pmod 5$, celkem tedy $p \equiv 7, 13, 23, 37 \pmod{40}$.

Nevíme ale, která prvočísla jsou vhodně reprezentována formami které třídy ekvivalence. Jak na to? Uvažujme obě redukované formy modulo deset. Uvědomme si, že pokud má být liché prvočíslo vyjádřeno formou $x^2 + 10y^2$, x musí být liché číslo. Dostáváme tedy $p \equiv x^2 \pmod{10} \Rightarrow p \equiv 1, 9 \pmod{10}$.

Naopak pokud má být liché prvočíslo vyjádřenou formou $2x^2 + 5y^2$, musí být liché číslo y. Tedy $p \equiv 2x^2 + 5 \pmod{10}$. Protože x nemůže být dělitelné pěti, pro všechny možné volby čísla x dostáváme $p \equiv 3, 7 \pmod{10}$.

Prvočíslo p musí navíc splňovat podmínku $\left(\frac{-10}{p}\right) = 1$. Dohromady s předchozím tedy pro libovolné liché prvočíslo $p \neq 5$ dostáváme:

1. $p = x^2 + 10y^2 \Leftrightarrow p \equiv 1, 9, 11, 19 \pmod{40}$,
2. $p = 2x^2 + 5y^2 \Leftrightarrow p \equiv 7, 13, 23, 37 \pmod{40}$.

Dostali jsme se ke krásnému a jednoduchému výsledku. Jednoznačně jsme určili, které prvočíslo je vhodně reprezentovánou kterou redukovanou formou (tedy formami které třídy). Pokud by to platilo pro každý diskriminant, otázka, kdy $p = x^2 + ny^2$, by byla vyřešena. Bohužel na následujícím příkladu si ukážeme, že situace není vždy tak růžová.

Nechť $D = -39$. Dostáváme $0 \leq a \leq \sqrt{\frac{39}{3}} \Rightarrow 0 \leq a \leq 3$. Nyní je D liché, tedy i b musí být liché. Pro $b = \pm 1$ dostáváme $ac = 10$ a aby byla získaná forma redukovaná, musí $(a, c) = (1, 10)$ nebo $(a, c) = (2, 5)$. V prvním případě platí $|b| = a$, tedy z definice musí být b kladné. Získáváme první tři redukované formy: $x^2 + xy + 10y^2, 2x^2 \pm xy + 5y^2$. Pro $b = \pm 3$ dostáváme $ac = 12$ a tedy $a = 3, c = 4$. Jelikož $|b| = a$, musí být b opět kladné a získáváme tedy formu $3x^2 + 3xy + 4y^2$. Celkem tedy máme 4 redukované formy diskriminantu $D = -39$.

Určeme nyní, která lichá prvočísla (nedělící diskriminant, tedy různá od tří a třinácti) můžeme vyjádřit těmito formami. Jak již víme, -39 musí být kvadratický zbytek modulo p. Počítejme: $\left(\frac{-39}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{39}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{39}\right)\cdot(-1)^{\frac{p-1}{2}\cdot\frac{39-1}{2}} = (-1)^{\frac{p-1}{2}(1+19)}\left(\frac{p}{39}\right) = \left(\frac{p}{3}\right)\cdot\left(\frac{p}{13}\right)$.

Aby tedy $\left(\frac{-39}{p}\right) = 1$, musí $\left(\frac{p}{13}\right) = \left(\frac{p}{3}\right) = \pm 1$. Očividně je p kvadratický zbytek (resp. nezbytek) modulo tři, pokud $p \equiv 1 \pmod 3$ (resp. $p \equiv -1 \pmod 3$). I kvadratické zbytky modulo 13 můžeme snadno určit:

$\left(\frac{p}{13}\right) = 1 \Leftrightarrow p \equiv (\pm 1)^2, (\pm 2)^2, ..., (\pm 6)^2 \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$, odkud plyne $\left(\frac{p}{13}\right) = -1 \Leftrightarrow p \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$.

Dohromady dostáváme $p \equiv 1, 4, 10, 16, 22, 25 \pmod{39}$, pokud je p kvadratický zbytek modulo 3 i 13, a $p \equiv 2, 5, 8, 11, 20, 32 \pmod{39}$, pokud je p kvadratický nezbytek modulo 3 i 13.

Jak nyní určit, která prvočísla vyjadřuje která forma? V předchozím příkladu jsme si situaci usnadnili trikem s paritou čísel x a y. V obecném případě to ale tak jednoduché být nemusí. Vzpomeňme si nyní na vztah $4af(x, y) = (2ax+by)^2 - Dy^2$. Modulo $|D|$ dostáváme rovnost $4af(x, y) \equiv (2ax + by)^2 \pmod{|D|}$. Pokud jsou čísla D a $4a$ nesoudělná, má $4a$ svůj inverzní prvek modulo $|D|$ a na levé straně kongruence můžeme osamostatnit danou formu. Aplikujme tento postup na redukované formy diskriminantu -39:

$4(x^2+xy+10y^2) \equiv (2x+y)^2 \Rightarrow 10\cdot 4(x^2+xy+10y^2) \equiv 10(2x+y)^2 \Rightarrow x^2+xy+10y^2 \equiv$
$\equiv 7^2(2x+y)^2 \Rightarrow x^2+xy+10y^2 \equiv (14x+7y)^2 \pmod{39}$, tedy tato forma může vyjadřovat jen druhé mocniny modulo 39. Aby mohlo být liché prvočíslo vhodně reprezentováno touto formou, musí tedy $p \equiv 1, 4, 10, 16, 22, 25 \pmod{39}$.

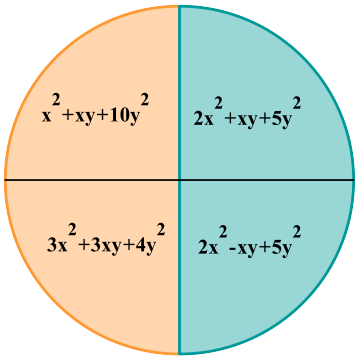
$8(2x^2 \pm xy + 5y^2) \equiv (4x \pm y)^2 \Rightarrow 2x^2 \pm xy + 5y^2 \equiv 5(4x \pm y)^2 \pmod{39}$, tedy liché prvočíslo vyjádřeno některou z těchto dvou forem musí být pětinásobkem některé druhé mocniny – celkem tedy $p \equiv 2, 5, 8, 11, 20, 32 \pmod{39}$.

Co se týče poslední formy, $3x^2 + 3xy + 4y^2$, všimněme si, že $\mathrm{nsd}(4 \cdot 3, 39) \neq 1$, tedy prvek $4a$ v tomto případě nemá inverzi. Tohoto problému se jednoduše zbavíme – použijeme formu vhodně ekvivalentní s tou naší, která tento problém mít nebude. Po dosazení $(x, y) \to$ $\to (-y, x)$ máme formu $4x^2 - 3xy + 3y^2, \mathrm{nsd}(4 \cdot 4, 39) = 1$. Tedy $16(4x^2 - 3xy + 3y^2) \equiv$ $\equiv (8y+3x)^2 \Rightarrow 4x^2-3xy+3y^2 \equiv 22(8y+3x)^2 \Rightarrow 4x^2-3xy+3y^2 \equiv (80y+30x)^2 \pmod{39}$. Liché prvočíslo vyjádřené touto formou tudíž musí být opět kongruentní s vhodnou druhou mocninou modulo 39 – tedy $p \equiv 1, 4, 10, 16, 22, 25 \pmod{39}$.

Dostáváme tedy:

1. $p = 2x^2 \pm xy + 5y^2 \Leftrightarrow p \equiv 2, 5, 8, 11, 20, 32 \pmod{39}$,
2. $p = x^2 + xy + 10y^2$ nebo $3x^2 + 3xy + 4y^2 \Leftrightarrow p \equiv 1, 4, 10, 16, 22, 25 \pmod{39}$.

V tomto případě bohužel nemůžeme rozlišit, která prvočísla jsou reprezentovaná formami kterých tříd – můžeme rozlišit jen skupiny tříd. Těmto podmnožinám $C(D)$, mezi nimiž v tuto chvíli nemůžeme rozlišit, která prvočísla jsou vhodně reprezentována formami které třídy, říkáme geny (situaci $D = -39$ vidíme na schematickém obrázku níže). S přesnější definicí a dalším popisem genů se setkáme ve třetí kapitole.



Všimněme si, že v bodě 1 obě formy reprezentují tatáž čísla, protože jsou ekvivalentní (ačkoli nevhodně). Naopak, u forem v bodě dva lze ukázat, že každé z nalezených prvočísel lze vyjádřit právě jednou z těchto forem. Podívejme se například na prvočíslo 43. Je vidět, že toto prvočíslo je vhodně reprezentováno formou $g(x, y) = x^2+xy+10y^2$; přeci $f(1, 2) =$ $= 43$. Ukažme, že toto prvočíslo nemůžeme vyjádřit ve tvaru $3x^2 + 3xy + 4y^2$. Použijeme opět onu užitečnou rovnost $4af(x, y) = (2ax + by)^2 - Dy^2$. V tomto případě dostáváme $f(x, y) = 3x^2 + 3xy + 4y^2 = \frac{1}{12}\big((6x + 3y)^2 + 39y^2\big) = \frac{3}{4}(2x + y)^2 + \frac{13}{4}y^2 \geq \frac{13}{4}y^2$, tedy pokud by pro vhodná x, y platilo $f(x, y) = 43$, tak musí platit $43 \geq \frac{13}{4}y^2$ a tedy $|y| \leq 3$. Dále také z rovnosti $43 = f(x, y) = \frac{3}{4}(2x+y)^2 + \frac{13}{4}y^2$ plyne rovnost $\frac{4 \cdot 43}{3} - \frac{13}{3}y^2 = (2x+y)^2$, v níž tedy

výraz na levé straně musí být roven druhé mocnině nějakého celého čísla pro $|y| \leq 3$. Ten ale nabývá pro $|y|$ od nuly do tří hodnot $\frac{172}{3}, 53, 40, \frac{55}{3}$, což ani v jednom případě druhá mocnina celého čísla není. Prvočíslo 43 tedy formou $f(x,y) = 3x^2 + 3xy + 4y^2$ vyjádřit nemůžeme.

Stejným způsobem, jako v předchozích dvou příkladech, můžeme postupovat pro každý „rozumně malý“ diskriminant. Uvedu bez postupu další dva příklady:

1. $D = -20 \Rightarrow \begin{cases} p = x^2 + 5y^2 & \Leftrightarrow p \equiv 1, 9 \pmod{20}, \\ p = 2x^2 + 2xy + 3y^2 & \Leftrightarrow p \equiv 3, 7 \pmod{20}, \end{cases}$

2. $D = -56 \Rightarrow \begin{cases} p = x^2 + 14y^2, 2x^2 + 7y^2 & \Leftrightarrow p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}, \\ p = 3x^2 \pm 2xy + 5y^2 & \Leftrightarrow p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}. \end{cases}$

Umíme tedy zatím rozlišit, která prvočísla jsou vyjádřena formami kterého genu. Všimněme si, že pro jakýkoli záporný diskriminant D určitě existuje redukovaná forma $x^2 - \frac{D}{4}y^2$, pokud je D sudé, a $x^2 + xy + \frac{1-D}{4}y^2$, pokud D je liché. Tyto formy nazýváme *hlavní* a gen, v němž tyto formy leží, nazýváme hlavní gen. Nabízí se tedy otázka: kdy v hlavním genu leží jediná forma? Odpovíme si na ni v třetí kapitole.

Zobecněme nyní postup, jímž jsme určili, která prvočísla se dají vyjádřit hlavní formou.

Pro $D = -4n, n \in \mathbb{N}$ jsme nejdřív uvažovali o paritě. Aby forma $x^2 + ny^2$ vyjadřovala liché prvočíslo, musí mít x a ny různou paritu. Pro $y = 2k, k \in \mathbb{Z}$ máme $p = x^2 + n(2k)^2 = = x^2 + 4nk^2 \equiv x^2 \pmod{|D|}$, pro $y = 2k + 1, k \in \mathbb{Z}$ dostáváme $p = x^2 + n(2k+1)^2 = = x^2 + 4nk^2 + 4nk + n \equiv x^2 + n \pmod{|D|}$.

Pro $D = 1 - 4n, n \in \mathbb{N}$ jsme použili postup $4(x^2 + xy + ny^2) = 4x^2 + 4xy + y^2 - y^2 + 4ny^2 = = (2x + y)^2 - (1 - 4n)y^2 \equiv (2x + y)^2 \pmod{|D|}$.

Pokud tato pozorování shrneme, dostáváme následující větu:

Věta 2.2.1. *Nechť $D \equiv 0, 1 \pmod 4$ je dané záporné celé číslo. Pak hlavní gen redukovaných forem diskriminantu D vyjadřuje pouze lichá prvočísla p tvaru:*

1. $p \equiv \alpha^2, \alpha^2 - \frac{D}{4} \pmod{|D|}$, *pokud* $D \equiv 0 \pmod 4$,

2. $p \equiv \alpha^2 \pmod{|D|}$, *pokud* $D \equiv 1 \pmod 4$.

Ve třetí kapitole si ukážeme, jak tato pozorování zobecnit a co z nich plyne. Abychom tak mohli učinit, musíme se seznámit s pojmy podgrupa a homomorfismus a také konečně sestrojit grupu tříd primitivních pozitivně definitních forem daného diskriminantu.

Kapitola 3

Grupa tříd forem a úvod do teorie genů

Na konci předchozí kapitoly jsme zjistili o reprezentaci lichých prvočísel primitivními pozitivně definitními kvadratickými formami mnoho informací. Učinili jsme také pozorování, jejichž platnost jsme však nezformulovali obecně. Abychom tak mohli učinit, nejprve je nutno stručně se obeznámit s několika pojmy z teorie grup.

3.1 Podgrupa, homomorfismus, faktorgrupa

Máme-li množinu G a na ní definovanou operaci, víme už, co musí být splněno, aby dohromady tvořily grupu. Mluvíme-li o podgrupách grupy G, zajímají nás takové podmnožiny množiny G, které spolu se zúžením dané operace tvoří rovněž grupu.

Definice 3.1.1. *Nechť $(G, \cdot)$ je grupa, H je neprázdná podmnožina G. Pak $(H, \cdot)$ je podgrupa grupy $(G, \cdot)$, pokud:*

1. $1 \in H$;
2. *pro všechna $a \in H$ platí $a^{-1} \in H$;*
3. *pro všechna $a, b \in H$ platí $a \cdot b \in H$.*

Je třeba poznamenat, že tyto podmínky na sobě nejsou nezávislé a lze je sloučit do jedné: nechť $(G, \cdot)$ je grupa, $H \subseteq G$, H je neprázdná. Pak $(H, \cdot)$ je podgrupa grupy $(G, \cdot)$, pokud pro všechna $a, b \in H$ platí $a \cdot b^{-1} \in H$.

Můžeme uvést mnoho příkladů. Každá grupa G má vždy podgrupy G a tzv. triviální podgrupu obsahující pouze neutrální prvek. Grupa $(\mathbb{Z}, +)$ je podgrupa grupy $(\mathbb{Q}, +)$, což je podgrupa grupy $(\mathbb{R}, +)$. Grupa $(\mathbb{Q} \setminus \{0\}, \cdot)$ je podgrupa grupy $(\mathbb{R} \setminus \{0\}, \cdot)$. Pro libovolné $m \in \mathbb{Z}$ je grupa $m\mathbb{Z} = \{..., -2m, -m, 0, m, 2m, ...\}$ s operací sčítání podgrupa grupy $(\mathbb{Z}, +)$. Množina $\{-1, 1\}$ s operací násobení je podgrupa grupy $\{-1, 1, -i, i\}$ s operací násobení.

Naopak například množina lichých celých číslech s operací sčítání není podgrupa celých čísel s operací sčítání, protože v této množině neleží neutrální prvek 0. Stejně tak množina nezáporných celých čísel s operací sčítání není podgrupou grupy $(\mathbb{Z}, +)$, protože ačkoli v ní leží neutrální prvek i součet jejich libovolných dvou prvků, žadný prvek kromě nuly zde nemá svoji inverzi.

Všimněme si také, že pokud je grupa komutativní, její podgrupa tuto vlastnost zdědí.

Podgrupa je pojem velice intuitivní. Co je však homomorfismus? O zobrazení mezi dvěma grupami řekneme, že je homomorfismus, pokud splňuje jednu nám sympatickou vlastnost – zachovává operaci.

Definice 3.1.2. *Nechť $f\colon G \to H$ je zobrazení, $(G, \cdot), (H, \cdot)$ jsou grupy. Pak o tomto zobrazení řekneme, že je homomorfismus, pokud pro všechna $a, b \in G$ platí $f(a \cdot b) = f(a) \cdot f(b)$.*

Z této jedné sympatické vlastnosti plynou hned dvě další sympatické vlastnosti: homomorfismus zachovává neutrální a inverzní prvek.

Věta 3.1.1. *Nechť $f\colon G \to H$ je homomorfismus. Pak:*

1. $f(1) = 1$,
2. *pro všechna $x \in G$ platí $f(x^{-1}) = f(x)^{-1}$.*

Důkaz. Ad 1: Nejprve je vhodné poznamenat, že na levé straně rovnosti symbol 1 představuje neutrální prvek grupy G, zatímco na pravé straně rovnosti je takto označen neutrální prvek grupy H. Potom můžeme snadno spočítat $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$. Po vynásobení obou stran rovnosti prvkem inverzním k $f(1)$ tedy $f(1) = 1$.

Ad 2: $1 = f(1) = f(x \cdot x^{-1}) = f(x)f(x^{-1})$. Pokud obě strany rovnosti vynásobíme zleva prvkem $f(x)^{-1}$, dostáváme $f(x^{-1}) = f(x)^{-1}$. □

Zobrazení $f\colon (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ dané předpisem $f(x) = mx$ je pro každé $m \in \mathbb{Z}$ homomorfismus, jelikož $f(x+y) = m(x+y) = mx+my = f(x)+f(y)$. Vidíme, že $f(0) = 0m = 0$ a $f(-x) = -mx = -f(x)$.

Víme, že homomorfismus zobrazí neutrální prvek opět na neutrální prvek. Nemusí to být ale jediný prvek, který se na něj zobrazí. Uvažujme zobrazení $f\colon (\mathbb{Z}, +) \to (\mathbb{Q}, \cdot)$ definované předpisem $f(x) = \begin{cases} 1 & \Leftrightarrow 2 \mid x \\ -1 & \Leftrightarrow 2 \nmid x \end{cases}$. Snadno si ověříme, že f je homomorfismus, a na neutrální prvek – jedničku se zobrazí všechna sudá celá čísla (tedy i neutrální prvek 0). Ty ale se sčítáním tvoří podgrupu grupy celých čísel. Můžeme ukázat, že to platí vždy. Nejprve však musíme definovat jádro homomorfismu.

Definice 3.1.3. *Nechť $f\colon G \to H$ je homomorfismus. Množinu prvků G, jež se zobrazily na neutrální prvek grupy H, nazýváme jádro homomorfismu a značíme* $\ker f$*, tedy*

$$\ker f = \{x \in G \mid f(x) = 1\}.$$

Nyní můžeme zobecnit pozorování učiněné výše.

Věta 3.1.2. *Nechť $f\colon G \to H$ je homomorfismus. Potom platí, že* $\ker f$ *je podgrupa grupy G.*

Důkaz. Je nutné ukázat následující:

1. $1 \in \ker f$;
2. $a \in \ker f \Rightarrow a^{-1} \in \ker f$;
3. $a, b \in \ker f \Rightarrow a \cdot b \in \ker f$.

Ad 1: Z 1. bodu věty 3.1.1. víme, že $f(1) = 1$, čímž jsme hotovi. Ad 2: Opět ve výpočtu využijeme větu 3.1.1, a to bod 2. Pro všechna $a \in \ker f$ můžeme psát: $f(a^{-1}) = f(a)^{-1} = = 1^{-1} = 1$. Z toho tedy plyne, že pokud je a prvkem $\ker f$, tak $a^{-1} \in \ker f$. Ad 3: Z definice homorfismu můžeme pro libovolná a, b z $\ker f$ počítat $f(ab) = f(a)f(b) = 1 \cdot 1 = 1$. Tedy i $ab \in \ker f$, čímž jsme důkaz dokončili. □

Abychom porozuměli dalšímu textu, potřebujeme se seznámit ještě s jedním pojmem z teorie grup, jímž je faktorgrupa.

Vraťme se na chvíli ke grupě zbytkových tříd modulo m s operací sčítání pomocí reprezentantů. Tuto grupu jsme dostali tím, že jsme rozdělili celá čísla podle toho, jaký dávají zbytek modulo m, na třídy ekvivalence – tedy systém neprázdných disjunktních množin, jejichž sjednocením je opět celá množina celých čísel. Tomuto procesu říkáme faktorizace. V tomto případě jsme na faktorizaci potřebovali kongruenci, což je relace ekvivalence.

Faktorizovat můžeme ale i jiným způsobem. Výše jsme si ukázali, že grupa $(m\mathbb{Z}, +)$ je pro jakékoli přirozené m podgrupou grupy $(\mathbb{Z}, +)$. K množině $m\mathbb{Z}$ nyní „přičtěme“ libovolné pevně zvolené celé číslo a v tom smyslu, že utvoříme množinu součtů tohoto a s postupně všemi prvky množiny $m\mathbb{Z}$. Tím jsme ale dostali zbytkovou třídu $[a]_m$! Pokud tomuto procesu podrobíme všechna celá čísla a, dostaneme tedy jako výsledek množinu všech zbytkových tříd modulo m. O této množině ale víme, že se sčítáním definovaným pomocí sčítání reprezentantů tvoří grupu.

Co jsme tedy v předchozím odstavci udělali? Opět jsme faktorizovali, ale ne jen nějakou množinu podle nějaké relace ekvivalence, ale grupu podle její podgrupy. A co bylo výsledkem? Opět grupa. Pokusme se nyní tento postup zobecnit.

Nechť $(G, \cdot)$ je grupa, $(H, \cdot)$ její podgrupa. Pro nějaké $a \in G$ označme $a \cdot H = = \{a \cdot h \mid h \in H\}$. Lze ukázat, že pokud tuto množinu vytvoříme pro všechna a z G, dostaneme vždy systém disjunktních množin, jejichž sjednocením je množina G. Důkaz to není nijak složitý, ale není nutné ho zde uvádět.

Faktorizovali jsme tedy grupu podle její podgrupy a dostali jsme množinu prvků $\{a \cdot H \mid a \in G\}$. Zkusme opět definovat operaci pomocí reprezentantů, tedy pro všechna a, b z G definujme $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$. Aby tato operace byla korektní, nesmí záviset

na volbě reprezentantů, tedy pokud $a \cdot H = b \cdot H$ a $c \cdot H = d \cdot H$, musí platit $(a \cdot c) \cdot H = (b \cdot d) \cdot H$. V případě zbytkových tříd tomu tak bylo, obecně to ale platit nemusí. To však můžeme napravit, pokud budeme požadovat, aby podgrupa, podle níž faktorizujeme, byla tzv. *normální podgrupa* – to je taková podgrupa H grupy G, pro jejíž každý prvek $h \in H$ a pro jakýkoli prvek $a \in G$ platí $a \cdot h \cdot a^{-1} \in H$. V tomto případě lze ukázat, že operace opravdu korektní je. Jelikož ale v textu pracujeme výhradně s komutativními grupami, nemusíme být příliš obezřetní, protože jakákoli podgrupa komutativní grupy je jistě normální.

Vytvořili jsme tedy grupu. Jelikož jsme tuto grupu získali faktorizací, její název je faktorgrupa.

3.2 Grupa tříd forem

V druhé kapitole jsme shromáždili několik indicií, podle nichž by třídy vhodně ekvivalentních primitivních pozitivně definitních kvadratických forem daného diskriminantu (dále jen třídy forem) mohli utvořit grupu. Stále nám však chybí nějaká operace, kterou bychom mohli mezi třídami forem definovat.

První, kdo se o to pokusil, byl Gauss. Skutečně ukázal, že třídy forem daného diskriminantu spolu s operací zvanou přímá kompozice tvoří grupu. S touto operací se však pracuje nesmírně zdlouhavě a komplikovaně. Na mnohem vhodnější operaci přišel až Dirichlet – budeme se nyní bavit o tzv. *Dirichletově kompozici*.

Definice 3.2.1. *Nechť $f(x,y) = ax^2 + bxy + cy^2$, $g(x,y) = a'x^2 + b'xy + c'y^2$ jsou primitivní pozitivně definitní formy se stejným diskriminantem D, které navíc splňují podmínku* $\mathrm{nsd}(a, a', \frac{b+b'}{2}) = 1$. *Potom Dirichletova kompozice forem $f(x,y)$ a $g(x,y)$ je kvadratická forma*

$$F(x,y) = aa'x^2 + Bxy + \frac{B^2 - D}{4aa'}y^2,$$

kde B je celé číslo jednoznačně určené modulo $2aa'$ soustavou kongruencí

1. $B \equiv b \pmod{2a}$
2. $B \equiv b' \pmod{2a'}$
3. $B^2 \equiv D \pmod{4aa'}$.

Dokázat, že číslo B existuje a je jednoznačně určeno modulo $2aa'$, je poměrně zdlouhavé, důkaz proto neuvádím.

Abychom mohli vytvořit grupu, Dirichletova kompozice nám musí udávat korektně definovanou operaci na množině tříd forem daného diskriminantu. Lze ukázat, že tomu tak skutečně je. Zaprvé, celé číslo B sice není určeno jednoznačně, ale formy vzniklé různými volbami B jsou spolu vhodně ekvivalentní. Dále, pokud je forma f vhodně ekvivalentní s f' a g s g', je i kompozice forem f a g vhodně ekvivalentní s kompozicí forem f' a g'. A nakonec, pokud formy f a g nesplňují podmínku nesoudělnosti koeficientů z definice, vždy

existuje forma g' vhodně ekvivalentní s g, která už tuto podmínku spolu s původní formou f splňuje. Tedy vybereme-li si dvě třídy vhodně ekvivalentních forem, můžeme vždy zvolit reprezentanty z obou tříd tak, abychom mezi nimi mohli provést Dirichletovu kompozici, a navíc různou volbou reprezentantů se nemění třída, jíž bude náležet výsledná forma.

Nyní máme dostatek informací, abychom vytvořili grupu.

Věta 3.2.1. *Nechť $D \equiv 0, 1 \pmod 4$ je záporné, nechť $C(D)$ je množina tříd primitivních forem tohoto diskriminantu. Pak Dirichletova kompozice udává korektně definovanou binární operaci na množině $C(D)$, která spolu s touto množinou tvoří konečnou komutativní grupu s $h(D)$ prvky.*

Neutrální prvek této grupy je třída obsahující hlavní formu – nazýváme ji hlavní třídou. Inverzní prvek třídy obsahující formu $ax^2+bxy+cy^2$ je třída obsahující formu $ax^2-bxy+cy^2$, kterou nazýváme opačnou formou.

Důkaz neuvádím. Větu je možno dokázat pomocí vlastností Dirichletovy kompozice, ale je to důkaz velice dlouhý a pracný. Pro rychlejší a jednodušší důkaz bychom museli být seznámeni s pojmem grupa tříd ideálů, který výrazně přesahuje rámec této práce.

Spokojme se tedy s konkrétním příkladem, na němž budeme demonstrovat počítání v grupě tříd forem.

Nechť $D = -56$. Redukované formy tohoto diskriminantu jsou $h(x,y) = x^2 + 14y^2$, $a(x,y) = 3x^2 + 2xy + 5y^2$, $b(x,y) = 3x^2 - 2xy + 5y^2$, $r(x,y) = 2x^2 + 7y^2$. Třídy obsahující tyto formy označme H, A, B, R. Dirichletovu kompozici forem f a g označme $f \odot g$. Podle věty 3.2.1. bychom měli být schopni předpovědět, jak vypadají kompozice v této grupě: H je neutrální prvek, A, B jsou navzájem inverzní, R je inverzní sám sobě. Multiplikativní tabulka této grupy by měla tedy vypadat takto:

	H	A	B	R
H	H	A	B	R
A	A	R	H	B
B	B	H	R	A
R	R	B	A	H

Pojďme si to nyní ověřit. Číslo B z definice 3.2.1. nyní budeme značit b, aby se nepletlo s formami. Nejdříve spočítejme druhé mocniny všech tříd: nejjednodušší postup je vzít kompozici dané redukované formy $f(x,y)$ s vhodně ekvivalentní formou $f(-y,x)$ – to nám zaručuje podmínku o nesoudělnosti koeficientů.

$$H^2 : (x^2+14y^2) \odot (14x^2+y^2) \Rightarrow \left\{ \begin{array}{cc} b \equiv 0 & (\mathrm{mod}\ 2) \\ b \equiv 0 & (\mathrm{mod}\ 28) \\ b^2 \equiv -56 \equiv 0 & (\mathrm{mod}\ 56) \end{array} \right\} \Rightarrow b \equiv 0 \ (\mathrm{mod}\ 28).$$

$$\text{Volme } b = 0 \Rightarrow F(x,y) = 1 \cdot 14x^2 + 0xy + \tfrac{0+56}{4 \cdot 1 \cdot 14} y^2 = 14x^2 + y^2 \in H \Rightarrow H^2 = H.$$

$$A^2 \ : \ (3x^2+2xy+5y^2) \odot (5x^2-2xy+3y^2) \ \Rightarrow \ \left\{ \begin{array}{cc} b \equiv 2 & (\mathrm{mod}\ 6) \\ b \equiv -2 & (\mathrm{mod}\ 10) \\ b^2 \equiv -56 \equiv 4 & (\mathrm{mod}\ 60) \end{array} \right\} \Rightarrow$$

$\Rightarrow b \equiv 8 \pmod{30}$.

Volme $b = 8 \Rightarrow F(x,y) = 3 \cdot 5x^2 + 8xy + \frac{8+56}{4 \cdot 3 \cdot 5} y^2 = 15x^2 + 8xy + 2y^2$. Známým postupem nyní můžeme najít formu s touto vhodně ekvivalentní: $15x^2 + 8xy + 2y^2 \sim 2x^2 - 8xy + 15y^2 \sim 2x^2 + 7y^2 \in R \Rightarrow A^2 = R$.

$$B^2 \ : \ (3x^2-2xy+5y^2) \odot (5x^2+2xy+3y^2) \ \Rightarrow \ \left\{ \begin{array}{cc} b \equiv -2 & (\mathrm{mod}\ 6) \\ b \equiv 2 & (\mathrm{mod}\ 10) \\ b^2 \equiv -56 \equiv 4 & (\mathrm{mod}\ 60) \end{array} \right\} \Rightarrow$$

$\Rightarrow b \equiv 22 \pmod{30}$.

Volme $b = -8 \Rightarrow F(x,y) = 3 \cdot 5x^2 - 8xy + \frac{-8+56}{4 \cdot 3 \cdot 5} y^2 = 15x^2 - 8xy + 2y^2 \sim 2x^2 + 8xy + +15y^2 \sim 2x^2 + 7y^2 \in R \Rightarrow B^2 = R$.

$$R^2 : (2x^2+7y^2) \odot (7x^2+2y^2) \Rightarrow \left\{ \begin{array}{cc} b \equiv 0 & (\mathrm{mod}\ 4) \\ b \equiv 0 & (\mathrm{mod}\ 14) \\ b^2 \equiv -56 \equiv 0 & (\mathrm{mod}\ 56) \end{array} \right\} \Rightarrow b \equiv 0 \pmod{28}.$$

Volme $b = 0 \Rightarrow F(x,y) = 2 \cdot 7x^2 + 0xy + \frac{56}{4 \cdot 2 \cdot 7} y^2 = 14x^2 + y^2 \sim x^2 + 14y^2 \in H \Rightarrow R^2 = H$.

Nyní spočítejme ostatní kompozice.

$$H \odot A = A \odot H : (x^2+14y^2) \odot (3x^2+2xy+5y^2) \Rightarrow \left\{ \begin{array}{cc} b \equiv 0 & (\mathrm{mod}\ 2) \\ b \equiv 2 & (\mathrm{mod}\ 6) \\ b^2 \equiv -56 \equiv 4 & (\mathrm{mod}\ 12) \end{array} \right\} \Rightarrow$$

$\Rightarrow b \equiv 2 \pmod{6}$.

Volme $b = 2 \Rightarrow F(x,y) = 1 \cdot 3x^2 + 2xy + \frac{4+56}{4 \cdot 1 \cdot 3} y^2 = 3x^2 + 2xy + 5y^2 \in A \Rightarrow H \odot A = = A \odot H = A$.

$$H \odot B = B \odot H : (x^2+14y^2) \odot (3x^2-2xy+5y^2) \Rightarrow \left\{ \begin{array}{cc} b \equiv 0 & (\mathrm{mod}\ 2) \\ b \equiv -2 & (\mathrm{mod}\ 6) \\ b^2 \equiv -56 \equiv 4 & (\mathrm{mod}\ 12) \end{array} \right\} \Rightarrow$$
$\Rightarrow b \equiv -2 \pmod 6$.

Volme $b = -2 \Rightarrow F(x,y) = 1 \cdot 3x^2 - 2xy + \frac{4+56}{4 \cdot 1 \cdot 3} y^2 = 3x^2 - 2xy + 5y^2 \in B \Rightarrow H \odot B = B \odot H = B$.

$$H \odot R = R \odot H : (x^2+14y^2) \odot (2x^2+7y^2) \Rightarrow \left\{ \begin{array}{cc} b \equiv 0 & (\mathrm{mod}\ 2) \\ b \equiv 0 & (\mathrm{mod}\ 4) \\ b^2 \equiv -56 \equiv 0 & (\mathrm{mod}\ 8) \end{array} \right\} \Rightarrow$$
$\Rightarrow b \equiv 0 \pmod 4$.

Volme $b = 0 \Rightarrow F(x,y) = 1 \cdot 2x^2 + \frac{56}{4 \cdot 1 \cdot 2} y^2 = 2x^2 + 7y^2 \in R \Rightarrow H \odot R = R \odot H = R$.

$$A \odot B = B \odot A : (3x^2+2xy+5y^2) \odot (5x^2+2xy+3y^2) \Rightarrow \left\{ \begin{array}{cc} b \equiv 2 & (\mathrm{mod}\ 6) \\ b \equiv 2 & (\mathrm{mod}\ 10) \\ b^2 \equiv -56 \equiv 4 & (\mathrm{mod}\ 60) \end{array} \right\} \Rightarrow$$
$\Rightarrow b \equiv 2 \pmod{30}$.

Volme $b = 2 \Rightarrow F(x,y) = 3 \cdot 5x^2 + 2xy + \frac{4+56}{4 \cdot 3 \cdot 5} y^2 = 15^2 + 2xy + y^2 \sim x^2 - 2xy + 15y^2 \sim \sim x^2 + 14y^2 \in H \Rightarrow B \odot A = A \odot B = H$.

$$R \odot A = A \odot R : (2x^2+7y^2) \odot (3x^2+2xy+5y^2) \Rightarrow \left\{ \begin{array}{cc} b \equiv 0 & (\mathrm{mod}\ 4) \\ b \equiv 2 & (\mathrm{mod}\ 6) \\ b^2 \equiv -56 \equiv 16 & (\mathrm{mod}\ 24) \end{array} \right\} \Rightarrow$$
$\Rightarrow b \equiv 8 \pmod{12}$.

Volme $b = -4 \Rightarrow F(x,y) = 2 \cdot 3x^2 - 4xy + \frac{16+56}{4 \cdot 2 \cdot 3} y^2 = 6x^2 - 4xy + 3y^2 \sim 3x^2 + 4xy + 6y^2 \sim \sim 3x^2 - 2xy + 5y^2 \in B \Rightarrow R \odot A = A \odot R = B$.

$$R \odot B = B \odot R : (2x^2+7y^2) \odot (3x^2-2xy+5y^2) \Rightarrow \left\{ \begin{array}{cc} b \equiv 0 & (\mathrm{mod}\ 4) \\ b \equiv -2 & (\mathrm{mod}\ 6) \\ b^2 \equiv -56 \equiv 16 & (\mathrm{mod}\ 24) \end{array} \right\} \Rightarrow$$

$\Rightarrow b \equiv 4 \pmod{12}$.

Volme $b = 4 \Rightarrow F(x,y) = 2 \cdot 3x^2 + 4xy + \frac{16+56}{4 \cdot 2 \cdot 3} y^2 = 6x^2 + 4xy + 3y^2 \sim 3x^2 - 4xy + 6y^2 \sim$ $\sim 3x^2 + 2xy + 5y^2 \in A \Rightarrow R \odot B = B \odot R = A$.

Tímto jsme hotovi a vidíme, že se naše výpočty shodují s předpovězenou multiplikativní tabulkou.

Konečně jsme zformovali grupu. Máme tedy dostatečný nástroj na to, abychom mohli o něco více prozkoumat geny forem.

3.3 Geny forem

Vraťme se nejdříve k pozorováním, která jsme učinili, když jsme na konci druhé kapitoly u několika záporných diskriminantů zkoumali, která prvočísla jsou vhodně reprezentována kterými redukovanými formami. Abychom tato pozorování mohli popsat poněkud formálnějším jazykem, musíme se na chvíli vrátit na samotný začátek – k Jacobiho symbolu.

V následujícím textu budeme často pracovat s grupou jednotek okruhu $(\mathbb{Z}/|D|\mathbb{Z})^*$, kde D bude nějaký záporný diskriminant. Pro jednoduchost budeme používat zápis bez absolutní hodnoty, tedy $(\mathbb{Z}/D\mathbb{Z})^*$. Také jednotlivé zbytkové třídy modulo $|D|$ budeme značit $[a]_D$.

Věta 3.3.1. *Nechť $D \equiv 0, 1 \pmod 4$ je nenulové celé číslo. Pak existuje jediné zobrazení $\chi\colon (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$ takové, že $\chi([p]_D) = \left(\frac{D}{p}\right)$ pro každé liché prvočíslo nedělící D. Toto zobrazení je navíc homomorfismus splňující $\chi([m]_D) = \left(\frac{D}{m}\right)$ pro všechna lichá přirozená čísla m nesoudělná s D.*

To, že je χ opravdu korektně definovaný homomorfismus, plyne z vlastností Jacobiho symbolu uvedených v první kapitole. To, že existuje jediné zobrazení splňující podmínku danou ve větě, nám říká tzv. *Dirichletova věta o prvočíslech v aritmetických posloupnostech*, podle níž v každé zbytkové třídě obsahující čísla nesoudělná s modulem leží nekonečně mnoho prvočísel.

Posuňme se nyní ke kvadratickým formám. Věta 2.1.3 nám říká, že libovolné liché $m \in \mathbb{Z}$ nesoudělné s D je vhodně reprezentováno nějakou formou daného diskriminantu D, právě když je D kvadratický zbytek modulo m. Ve světle věty 3.3.1 to tedy znamená $\chi([m]_D) = 1$ a tedy $[m]_D \in \ker \chi$. Tedy všechny třídy v $(\mathbb{Z}/D\mathbb{Z})^*$, které obsahují lichá čísla, jež lze vyjádřit některou z redukovaných forem daného diskriminantu, tvoří podgrupu $\ker \chi$ grupy $(\mathbb{Z}/D\mathbb{Z})^*$.

Připomeňme si, jak tato situace vypadá pro $D = -20$:

$$D = -20 \Rightarrow \begin{cases} p = x^2 + 5y^2 & \Leftrightarrow p \equiv 1, 9 \pmod{20}, \\ p = 2x^2 + 2xy + 3y^2 & \Leftrightarrow p \equiv 3, 7 \pmod{20}. \end{cases}$$

Pokud je p vhodně reprezentováno některou z kvadratických forem diskriminantu -20, tak $p \in \{[1]_{20}, [3]_{20}, [7]_{20}, [9]_{20}\}$. Je to opravdu podgrupa grupy $(\mathbb{Z}/D\mathbb{Z})^* = \{[1]_{20}, [3]_{20}, [7]_{20}, [9]_{20}, [11]_{20}, [13]_{20}, [17]_{20}, [19]_{20}\}$? Leží zde neutrální prvek $[1]_{20}$ a snadno si ověříme, že v této podmnožině leží součin jakýchkoli dvou jejich prvků. Inverzní prvek třídy $[3]_{20}$ je třída $[7]_{20}$ a naopak, třída $[9]_{20}$ je sama svým inverzním prvkem. Opravdu to tedy podgrupa je.

Nyní můžeme zobecnit pozorování učiněná na konci druhé kapitoly.

Věta 3.3.2. *Nechť $D \equiv 0, 1 \pmod 4$ je dané záporné celé číslo, $\ker \chi \subset (\mathbb{Z}/D\mathbb{Z})^*$ stejně jako výše a $f(x, y)$ je primitivní pozitivně definitní forma diskriminantu D.*

1. *Třídy v $(\mathbb{Z}/D\mathbb{Z})^*$ obsahující lichá čísla reprezentovaná hlavní formou tvoří (normální) podgrupu $H \subset \ker \chi$,*
2. *Třídy v $(\mathbb{Z}/D\mathbb{Z})^*$ obsahující lichá čísla reprezentovaná formou $f(x, y)$ tvoří množinu $H' \in \ker \chi / H$.*

Jednotlivé geny tedy opravdu reprezentují jednotlivé třídy v $\ker \chi / H$. Pokud gen reprezentuje hodnoty ležící v třídě H', říkáme mu gen *příslušný* H'. Vidíme také, že jelikož H je normální podgrupa $\ker \chi$, můžeme podle ní faktorizovat a třídy $H' \in \ker \chi / H$ reprezentované různými geny tudíž tvoří prvky faktorgrupy.

Opět se vraťme k příkladu $D = -20$. Lichá přirozená čísla vhodně reprezentovaná některou z forem hlavního genu ležela v množině $H = \{[1]_{20}, [9]_{20}\}$, čísla vhodně reprezentovaná některou z forem druhého genu ležela v množině $K = \{[3]_{20}, [7]_{20}\}$. Ověřme si na tomto příkladě platnost předchozí věty. Ta nám říká, že H je normální podgrupa grupy $\ker \chi = \{[1]_{20}, [3]_{20}, [7]_{20}, [9]_{20}\}$, a že navíc platí $\ker \chi / H = \{H, K\}$. Je tomu opravdu tak?

Nejdříve ukažme, že H je podgrupa $\ker \chi$ (protože pracujeme s komutativními strukturami, bude jistě normální). Musí v ní tedy ležet neutrální prvek, ale ten v ní je; vždyť $[1]_{20} \in H$. Dále v ní musí ležet součin každých jejich dvou prvků. Počítejme ${[1]_{20}}^2 = [1]_{20} \in H, [1]_{20} \cdot [9]_{20} = [9]_{20} \in H, {[9]_{20}}^2 = [1]_{20} \in H$. I toto kritérium je tedy splněno. Také vidíme, že každá třída z H je sama sobě inverzním prvkem, tedy H je opravdu podgrupa.

Nyní ukažme $\ker \chi / H = \{H, K\}$. Podle definice platí:

$$\ker \chi / H = \{[1]_{20} \cdot H, [3]_{20} \cdot H, [7]_{20} \cdot H, [9]_{20} \cdot H\}.$$

Počítejme:

$$\begin{aligned} [1]_{20} \cdot H &= \{[1]_{20} \cdot [1]_{20}, [1]_{20} \cdot [9]_{20}\} = \{[1]_{20}, [9]_{20}\} = H, \\ [3]_{20} \cdot H &= \{[3]_{20} \cdot [1]_{20}, [3]_{20} \cdot [9]_{20}\} = \{[3]_{20}, [7]_{20}\} = K, \\ [7]_{20} \cdot H &= \{[7]_{20} \cdot [1]_{20}, [7]_{20} \cdot [9]_{20}\} = \{[7]_{20}, [3]_{20}\} = K, \\ [9]_{20} \cdot H &= \{[9]_{20} \cdot [1]_{20}, [9]_{20} \cdot [9]_{20}\} = \{[9]_{20}, [9]_{20}\} = H. \end{aligned}$$

Tedy opravdu $\ker \chi/H = \{H, K\}$. Navíc vidíme, že výpočty v této faktorgrupě vypadají následovně: $H^2 = K^2 = H, HK = KH = K$.

Ověřili jsme si tedy na příkladu $D = -20$ platnost věty 3.3.2. Čtenář si může tuto větu obdobně ověřit i na dalších výše probíraných příkladech $D = -56, -40, -39$.

Všechny předchozí poznatky můžeme shrnout do následující věty:

Věta 3.3.3. *Nechť $D \equiv 0, 1 \pmod 4$ je dané záporné celé číslo, $H \subset \ker \chi$ jako výše. Nechť $H' \in \ker \chi/H$ a p je liché prvočíslo nedělící D. Pak $[p]_D \in H'$ právě tehdy, když je p reprezentováno nějakou redukovanou formou diskriminantu D z genu příslušného H'.*

Toto je hlavní poznatek elementární teorie genů. Říká nám mimo jiné, že existuje korektně definované zobrazení $\Phi\colon C(D) \to \ker \chi/H$, které každé třídě forem přiřadí množinu zbytkových tříd modulo diskriminant, které obsahují lichá přirozená čísla, jež jsou některou z forem dané třídy vhodně reprezentována. Lze navíc ukázat, že toto Φ je homomorfismus.

Hlavní cíl základní teorie genů je odpovědět na otázku, kolik genů má grupa tříd forem pro který diskriminant. Grupa $C(D)$ a homomorfismus Φ jsou dost silné nástroje, aby této odpovědi mohlo být dosaženo. Bez důkazů stručně popíšu, jak toho dosáhnout.

Nejdříve se ukáže, že všechny geny v dané grupě tříd forem obsahují stejný počet tříd, a že počet genů je mocnina dvojky. Dále se ukáže, že hlavní gen je roven množině všech druhých mocnin prvků $C(D)$ – druhou mocninou nějaké třídy rozumíme její kompozici s ní samotnou. To jsme mj. viděli u našeho příkladu $D = -56$: $(C(D))^2 = \{H^2, A^2, B^2, R^2\} = \{H, R\}$, což je hlavní gen.

Z těchto informací můžeme vyvodit, že hlavní gen obsahuje jedinou třídu, pokud má každý prvek řád nejvýše 2. Pak je hlavní gen totiž roven $(C(D))^2 = \{H\}$, kde H je třída obsahující hlavní formu, jelikož je to neutrální prvek.

Ukáže se také, že prvky řádu nejvýše dva jsou právě třídy obsahující redukovanou formu $ax^2 + bxy + cy^2$, pro niž platí buď $b = 0$, nebo $a = b$, nebo $a = c$. S touto informací lze dokonce obecně určit, kolik takovýchto prvků je.

Zvládneme-li určit všechny redukované formy daného záporného diskriminantu D, dokážeme tedy posléze i určit, zda hlavní gen obsahuje pouze hlavní formu.

Udejme na závěr ještě několik příkladů, které demonstrují sílu této teorie. Až doposud by pro nás u větších diskriminantů byla nesmírně zdlouhavá práce určit, které formy leží v hlavním genu a která prvočísla vhodně reprezentují – viz příklady z druhé kapitoly. Podívejme se nyní na grupu tříd forem diskriminantu $D = -280$. Je třeba nejprve určit všechny redukované formy – pro větší diskriminanty je asi nejjednodušší způsob napsat počítačový program, který nám pro všechny možné volby koeficientů a a b určí, zda je $c = \frac{b^2-D}{4a}$ celé číslo. Pro diskriminant $D = -280$ dostaneme tyto redukované formy: x^2+70y^2, $2x^2 + 35y^2$, $5x^2 + 14y^2$, $7x^2 + 10y^2$. Vidíme, že pro všechny tyto formy platí $b = 0$, a tedy v grupě tříd forem vždy reprezentují prvky řádu nejvýše 2. Uvedli jsme výše, že toto zjištění je ekvivalentní s tím, že v hlavním genu leží pouze jediná forma, a to hlavní – $x^2 + 70y^2$. Podle věty 2.2.1 tedy liché prvočíslo p tudíž můžeme vyjádřit ve tvaru $x^2 + 70y^2$, právě když $p \equiv \alpha^2, \alpha^2 + 70 \pmod{280}$, takové prvočíslo je například $2129 \equiv 13^2 \pmod{280}$.

Nyní se podívejme na diskriminant $D = -400$. Redukované formy jsou následující: x^2+100y^2, $4x^2+25y^2$, $8x^2+4xy+13y^2$, $8x^2-4xy+13y^2$. Bohužel vidíme, že poslední dvě formy jsou reprezentanty tříd, které mají v grupě tříd forem řád vyšší než dva. V hlavním genu tedy leží více forem, než ta hlavní. Výše jsme zjistili, že určit, jaké to jsou, můžeme umocněním všech prvků grupy tříd forem na druhou. Je nutné to provést jen u forem $8x^2 \pm 4xy+13y^2$, ostatní jsou řádu nejvýše dva (tedy jejich umocněním na druhou získáme neutrální prvek grupy – hlavní formu). Výsledkem je forma $4x^2 + 25y^2$, to je tedy druhá forma ležící v hlavním genu. V tomto případě tudíž můžeme pouze říci, že liché prvočíslo p můžeme vyjádřit ve tvaru $x^2 + 100y^2$ nebo $4x^2 + 25y^2$, právě když $p \equiv \alpha^2, \alpha^2 + 100 \pmod{400}$.

A nakonec příklad zmíněný v úvodu: uvažujme diskriminant $D = -420$. Dostaneme tyto redukované formy: $x^2 + 105y^2, 2x^2 + 2xy + 53y^2, 3x^2 + 35y^2, 5x^2 + 21y^2, 6x^2 + 6xy+$ $+19y^2, 7x^2 + 15y^2, 10x^2 + 10xy + 13y^2, 11x^2 + 8xy + 11y^2$. Vidíme, že všechny reprezentují prvky řádu nejvýše 2, máme tu dokonce všechny tři druhy takovýchto prvků (vyskytují se zde formy tvaru $b = 0$, $a = b$ i $a = c$). Tudíž v hlavním genu leží pouze jediná forma $x^2 + 105y^2$. Liché prvočíslo p tedy můžeme vyjádřit ve tvaru $x^2 + 105y^2$, právě když $p \equiv \alpha^2, \alpha^2 + 105 \pmod{420}$. Tedy např. o prvočíslu $2221 \equiv 121 \equiv 11^2 \pmod{420}$ nyní víme, že je můžeme napsat ve tvaru $x^2 + 105y^2$.

Závěr

Svou práci končím v bodě, kdy dokážeme pro několik (ale stále jen konečně mnoho) přirozených n určit, která lichá prvočísla můžeme vyjádřit ve tvaru $x^2 + ny^2$. Pro jakékoli záporné celé číslo $D \equiv 0, 1 \pmod 4$ navíc dokážeme říci, zda dané prvočíslo můžeme vyjádřit některou z forem hlavního genu. Vybudováním teorie kvadratických forem jsme tedy učinili značný pokrok od počátečního stavu, kdy jsem zmínil, že elementárními metodami je možné problém vyřešit pouze pro $n \leq 3$.

Otázku, kdy $p = x^2 + ny^2$, zodpovídá pro nekonečně mnoho n až věta, jejíž rozsah dalece přesahuje tuto práci. Pro zajímavost ji nyní uvedu:

Věta 3.3.4. *Nechť n je přirozené číslo, které navíc není dělitelné žádnou druhou mocninou prvočísla a platí $n \not\equiv 3 \pmod 4$. Pak existuje normovaný ireducibilní polynom $f_n(x)$ s celočíselnými koeficienty, jehož stupeň je roven číslu $h(-4n)$, tedy počtu redukovaných forem diskrimininantu $-4n$, s následující vlastností: pro libovolné liché prvočíslo p, které nedělí ani n, ani diskriminant polynomu $f_n(x)$, existují celá čísla x, y taková, že $p = x^2 + ny^2$, právě když $\left(\frac{-n}{p}\right) = 1$ a zároveň má kongruence $f_n(x) \equiv 0 \pmod p$ celočíselné řešení.*

Navíc platí, že $f_n(x)$ je minimální polynom reálného algebraického čísla α, pro něž je $L = K(\alpha)$ Hilbertovo těleso tříd tělesa $K = \mathbb{Q}(\sqrt{-n})$.

Vidíme, že i formulace této věty je značně náročná. Zjednodušeně řečeno existuje nějaký polynom f jistých vlastností tak, že pro každé liché prvočíslo p, které nedělí ani n, ani diskriminant polynomu f, platí, že p můžeme vyjádřit jako $x^2 + ny^2$, právě když $(-n/p) = 1$ a současně $p|f(t)$ pro vhodné celé číslo t. Známe stupeň tohoto polynomu a víme, že je normovaný a ireducibilní a jeho koeficienty jsou celá čísla.

Zajímavé je, že k důkazu této věty není potřeba znát teorii kvadratických forem. Důkaz vychází z poněkud jiné oblasti algebry, je v něm řeč o prvoideálech a Galoisových rozšířeních těles.

Nabízí se ovšem dvě otázky: zaprvé, co zbylá n, na něž se nevztahují podmínky věty 3.3.4, a zadruhé, jak najít onen polynom $f_n(x)$? K nalezení odpovědi na ně je třeba studovat geny a grupu tříd forem pomocí mnohem silnějších nástrojů. Věta 3.3.4 se dá generalizovat na veškerá přirozená n pomocí tzv. teorie těles tříd, a to pouhou změnou charakteristiky polynomu $f_n(x)$. Je však potřeba další silné teorie, tzv. teorie komplexního násobení, abychom dostali algoritmus, jak nalézt polynom $f_n(x)$. Pak můžeme opravdu odpovědět na otázku, kdy lze liché prvočíslo napsat ve tvaru $x^2 + ny^2$, pro všechna přirozená čísla n.

Literatura

[1] Cox, David A.: *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication.* Wiley: New York, 1989.
[2] Rosický, Jiří: *Algebra.* Brno: Masarykova univerzita, 2002.