APLIKACE CELOČÍSELNÝCH BODŮ ELIPTICKÝCH KŘIVEK V TEORII KUBICKÝCH A KVARTICKÝCH POLYNOMŮ

JIŘÍ KLAŠKA

Věnováno profesoru Michalu Křížkovi

Abstrakt. V 16. století došlo k průlomovým objevům, které umožnily nalézt řešení kubických a kvartických rovnic. I když od vydání slavné Cardanovy knihy Ars Magna uplynulo téměř 500 let, některé otázky související s kubickými a kvartickými polynomy jsou stále aktuální. V následující přehledové studii seznámíme čtenáře s několika zajímavými výsledky, které byly dosaženy v teorii kubických a kvartických polynomů s daným diskriminantem.

1. Úvod

Ve 14. a 15. století vynaložili někteří matematici velké úsilí, aby nalezli obecný postup pro řešení kubické rovnice. K těmto matematikům patřili Maestro Biaggio, Antonio de' Mazzinghi, Maestro Benedetto da Firenze, Maestro Dardi a Piero della Francesca. V roce 1494 vydal italský františkánský mnich Luca Pacioli (1445–1517) knihu *Summa de arithmetica, goeometria, proportioni at proportionalita*[1] (Souhrn vědomostí o aritmetice, geometrii, poměrech a úměrnosti), ve které sděluje, že řešení kubické rovnice nebylo doposud objeveno. Toto sdělení se stalo intelektuální výzvou pro nejlepší matematiky 16. století. Vydáním Pacioliho knihy začal zajímavý a spletitý příběh, ve kterém se v průběhu následujících století objevovala jména nejvýznamnějších matematických osobností. Jejich lidské osudy jsou často stejně zajímavé jako jejich objevy. V období let 1515–1540 došlo k významnému pokroku a metoda řešení kubických rovnic byla nalezena. Na vyřešení problému se podíleli

Scipione del Ferro	(1465–1526),
Niccolò Fontana Tartaglia	(1499–1557),
Gerolamo Cardano	(1501–1576),
Lodovicco Ferrari	(1522–1565).

Příběh Ferro – Tartaglia – Cardano – Ferrari je jedním z nejkontroverznějších příběhů dějin matematiky. Sled neobyčejných a dramatických událostí týkajících

2020 *MSC.* Primární 11D25; Sekundární 11D45.

Klíčová slova. Kubický polynom, kvartický polynom, diskriminant, eliptická křivka, Mordellova rovnice.

[1]Pro zajímavost uveďme, že jeden výtisk Pacioliho knihy vlastní Moravská zemská knihovna v Brně.

se objevu řešení kubické rovnice je poutavě popsán ve třetí kapitole knihy *The Equation That Couldn't Be Solved – How Mathematical Genius Discovered the Language of Symmetry*, jejímž autorem je Mario Livio. Kniha byla publikována v roce 2005 a český překlad této knihy vyšel v roce 2008 pod názvem *Neřešitelná rovnice*.

V roce 1545 Cardano publikoval knihu *Artis magnae sive de reguli algebraicis liber unus* (Velké umění neboli první kniha pravidel algebry), ve které byl poprvé uveden postup pro řešení kubické rovnice. Tato kniha, dnes známá jako *Ars Magna*, je považována za počátek moderní algebry. Cardanova kniha obsahuje rovněž řešení kvartické rovnice, které objevil v roce 1540 Lodovicco Ferrari. Podrobnou historii kubických a kvartických rovnic může čtenář nalézt také v knize *Rasskazy o fizikach i matematikach*, kterou napsal Semjon Grigorjevič Gindikin v roce 1981. V angličtině tato kniha vyšla v roce 1988 pod názvem *Tales of Physicists and Mathematicians*.

Dnes, téměř 500 let od vydání *Ars Magna*, je velmi obtížné si představit jak lidé v Cardanově době žili a přemýšleli. Díky Cardanovu životopisu *De Vita Propria Liber*, který Cardano napsal v průběhu posledního roku svého života, můžeme získat zajímavý pohled na dobu, kdy *Ars Magna* vznikla. Životopisné pojednání *De Vita Propria Liber* bylo poprvé publikováno v Paříži roku 1653. V roce 1914 byl Cardanův životopis přeložen do němčiny pod názvem *Des Girolamo Cardano von Mailand eigene Lebensbeschreibung* a v roce 1929 také do angličtiny pod názvem *The Book of My Life*. Český překlad z němčiny byl publikován v roce 2021 pod názvem *Můj život*.

Z historického hlediska je zajímavé připomenout, že téměř žádný z dnes běžně používaných matematických symbolů v Cardanově době ještě neexistoval. Pro lepší představu uveďme přehled autorů různých symbolů, používaných dnes v algebře, spolu s letopočtem prvního použití symbolu v tisku.

$+, -$	Widmann	(1489)
$(\ ,\ )$	Tartaglia	(1556)
$\cdot$	Clavius	(1593)
$\times$	Oughtread	(1631)
$:$	Johnson	(1633)
$\surd$	Rudolff	(1525)
$=$	Recorde	(1557)
$<, >$	Harriot	(1631)
$\leq\ ,\ \geq$	Bougere	(1734)
$i = \sqrt{-1}$	Euler	(1794)

Po nalezení postupu pro řešení kubických a kvartických rovnic bylo zřejmé, že další problém, který na matematiky čeká, je řešení kvintických rovnic. Příběh hledání vzorce pro řešení kvintické rovnice trval od smrti Cardana přibližně dalších 250 let. Tento problém byl však nesrovnatelně obtížnější. Na problému řešení kvintických rovnic pracovala v průběhu následujících století celá řada významných matematiků. Uveďme alespoň některé:

Rafael Bombelli	(1526–1572),
François Viète	(1540–1603),
Thomas Harriot	(1560–1621),
James Gregory	(1638–1675),
Ehrenfried Walther von Tschirnhaus	(1651–1708),
Étienne Bézout	(1730–1783),
Leonhard Paul Euler	(1777–1783),
Erland Samuel Bring	(1736–1798),
George Birch Jerrard	(1804–1863),
Alexandre–Théophile Vandermonde	(1735–1796),
Edward Waring	(1736–1798),
Joseph–Louis Lagrange	(1736–1813),
Johann Carl Friedrich Gauss	(1777–1855),
Paolo Ruffini	(1765–1822),
Niels Henrik Abel	(1802–1829),
Évariste Galois	(1811–1829).

Teprve objevy Abela a Galoise[2] uzavřely období velkého a marného úsilí nalézt řešení kvintické rovnice. Jejich objevy přinesly překvapující a znepokojivou odpověď. Žádný vzorec pro řešení kvintické rovnice, který by využíval pouze čtyři základní aritmetické operace a operaci odmocňování, nemůže existovat.

Důkaz, že kvintické rovnice není možné vyřešit podobným způsobem jako rovnice kubické a kvartické, ale neznamená, že by kvintické rovnice nemohly být řešeny pomocí jiných, složitějších metod, například pomocí eliptických funkcí. Touto problematikou se v následujícím období zabývali

Charles Hermite	(1922–1901),
Leopold Kronecker	(1823–1891),
Felix Christian Klein	(1849–1925).

Vývoj teorie rovnic od této chvíle pokračoval různými směry, v nichž hrála stále důležitější úlohu teorie grup. Vraťme se ale k problematice kubických rovnic. V roce 1940 Boris Nikolajevič Delone[3] (1890–1980) a Dmitrij Konstantinovič Faddějev (1907–1989) předložili následující problém:

Problém 1.1 (1940)**.** Nechť $D \in \mathbb{Z}$. Nalezněte metodu, která umožní určit všechny normované kubické polynomy s celočíselnými koeficienty mající diskriminant D.

Problém 1.1 byl poprvé publikován ve známé monografii [3, str. 313], která byla v roce 1964 přeložena do angličtiny. Pro zajímavost uveďme, že na anglickém překladu [4] se podstatně podílela Emma Lehmer (1906–2007). V [4] může čtenář nalézt Problém 1.1 na straně 412. Dále je vhodné poznamenat, že autorem Problému 1.1 je zřejmě pouze Boris Nikolajevič Delone, který se nalezením metody zabýval již před rokem 1928. Některé dílčí Deloneho výsledky, týkající se Problému 1.1,

[2]Tragické životní příběhy Abela a Galoise jsou podrobně popsány v kapitolách 4 a 5 v knize *Neřešitelná rovnice*.

[3]Delone publikoval některé články pod jménem Delaunay.

byly publikovány v článku [2]. V [2, str. 25] Delone nalezl všechny normované ireducibilní kubické polynomy s celočíselnými koeficienty pro 16 konkrétních hodnot diskriminantu D a sestavil jejich tabulku. Tato tabulka byla rovněž publikována v [3, str. 318] a [4, str. 418]. Metoda, kterou Delone k sestavení tabulky použil, byla založena na dvou podstatných předpokladech:

(i) Diskriminant D je záporný.
(ii) Polynomy jsou ireducibilní nad tělesem racionálních čísel $\mathbb{Q}$.

Deloneho postup tedy není možné aplikovat na případ diskriminantů $D \in \mathbb{Z}$, kde $D \geq 0$. Navíc, Deloneho postup neumožňuje určit kubické polynomy, které jsou reducibilní nad $\mathbb{Q}$. Obecná metoda, která je řešením Problému 1.1, byla poprvé publikována v roce 2021 v článku [20]. Tato metoda úzce souvisí s řešením diofantické rovnice

$$Y^2 = X^3 + k, \tag{1.1}$$

kde k je libovolné celé nenulové číslo. Rovnice (1) má velmi dlouhou a zajímavou historii, která sahá až do 17. století k práci francouzského matematika Gasparda Bacheta (1581–1638). Diofantická rovnice (1.1) se často nazývá Mordellova rovnice[4] na počest Louise Joela Mordella (1888–1972), který významně přispěl k objasnění některých vlastností této rovnice. Eliptická křivka odpovídající Mordellově rovnici se pak nazývá Mordellova křivka.

První objevy týkající se Mordellovy rovnice je možno nalézt v knize *History of the Theory of Numbers – Diophantine Analysis* [5, str. 533–539], jejímž autorem je americký matematik Leonard Eugene Dickson (1874–1954). Literatura týkající se Mordellovy rovnice je poměrně rozsáhlá. Čtenáři lze doporučit například publikace [1, 6, 11, 12, 19, 25, 26, 27, 28].

Důležitým výsledkem Louise Mordella je tvrzení, že každá rovnice (1.1) má nejvýše konečně mnoho celočíselných řešení. Je zřejmé, že je-li $[X_0, Y_0]$ je řešení rovnice (1.1), pak rovněž $[X_0, -Y_0]$ je řešení (1.1). Pro $Y_0 \neq 0$, budeme řešení $[X_0, Y_0]$ a $[X_0, -Y_0]$ považovat za různá. Konečně je vhodné připomenout, že v současné době existuje rozsáhlá literatura týkající se problematiky polynomů majících daný diskriminant. Významné výsledky v tomuto oboru dosáhli zejména maďarský matematik Kálmán Győry (*1940) a holandský matematik Jan–Hendrik Evertse (*1958). Z prací těchto autorů připomeňme alespoň publikace [7, 8, 9, 10, 13, 14, 15, 16, 17, 18].

V následující kapitole uvedeme hlavní výsledky dosažené v článku [20], které poskytují řešení Problému 1.1.

2. Řešení Deloneho problému kubických polynomů

Nechť $D \in \mathbb{Z}$ a nechť

$$C(D) = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x] : D(f) = D\},$$

kde $D(f) = a^2b^2 + 18abc - 4a^3c - 4b^3 - 27c^2$ je diskriminant $f(x)$. Je zřejmé, že problém určit množinu $C(D)$, pro dané $D \in \mathbb{Z}$, je ekvivalentní problému nalézt

[4] Rovnice (1.1) se někdy nazývá Bachetova rovnice.

všechna celočíselná řešení diofantické rovnice

$$a^2b^2 + 18abc - 4a^3c - 4b^3 - 27c^2 = D.$$

Řešení Deloneho problému můžeme rozdělit do několika částí.

2.1. Ekvivalence na množině $C(D)$

Nechť $f(x) = x^3 + ax^2 + bx + c \in C(D)$. Pro každé $w \in \mathbb{Z}$ definujme polynom $f_w(x) = f(x+w)$. Přímým výpočtem můžeme ověřit, že pro libovolné $w \in \mathbb{Z}$ platí

$$D(f_w) = D(f). \tag{2.1}$$

Z rovnosti (2.1) snadno plyne následující lemma.

Lemma 2.1. *Nechť $D \in \mathbb{Z}$. Je-li $C(D) \neq \emptyset$, pak množina $C(D)$ je nekonečná.*

Dále je možné dokázat, že pro polynomy $f_w(x)$ platí hezká a užitečná identita

$$f_w(x) = x^3 + \frac{f''(w)}{2!}x^2 + \frac{f'(w)}{1!}x + f(w), \tag{2.2}$$

ve které výrazy $f'(w)$ a $f''(w)$ označují první a druhou derivaci $f(x)$ v bodě w.

Nechť $C(D) \neq \emptyset$. Pro $f(x), g(x) \in C(D)$ položme

$$f(x) \sim g(x) \iff \exists\, w \in \mathbb{Z} : g(x) = f(x+w) = f_w(x).$$

Lemma 2.2. *Relace $\sim$ je ekvivalence na množině $C(D)$.*

Nechť $f(x) = x^3 + ax^2 + bx + c \in C(D)$. Pak existují jednoznačně určená čísla $w \in \mathbb{Z}$ a $e \in \{0, 1, 2\}$ tak, že $a = 3w + e$. Položme

$$r(x) = f(x-w) = x^3 + ex^2 + (b - 3w^2 - 2ew)x + 2w^3 + ew^2 - bw + c. \tag{2.3}$$

Polynom $r(x)$ budeme nazývat kanonický reprezentant třídy

$$[f(x)] = \{g(x) \in C(D) : g(x) \sim f(x)\} \in C(D)/\sim .$$

Bude užitečné zavést následující konvenci.

Konvence 2.3. Pro zápis polynomu $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ budeme rovněž požívat stručnější vyjádření ve tvaru uspořádané trojice koeficientů $[a, b, c]$.

Příklad 2.4. Nechť $f(x) = x^3 - 3x^2 - x + 6$. Protože $D(f) = 13$ je $C(13) \neq \emptyset$. Podle Lemma 2.1 je množina $C(13)$ nekonečná a z rovnosti (2.2) plyne, že polynomu $f(x)$ odpovídá třída rozkladu

$$[f(x)] = \{x^3 + (3w-3)x^2 + (3w^2 - 6w - 1)x + w^3 - 3w^2 - w + 6 : w \in \mathbb{Z}\}.$$

Aplikací vztahu (2.3) obdržíme, že kanonický reprezentant třídy $[f(x)]$ je polynom $r(x) = x^3 - 4x + 3$ a podle Konvence 2.3 můžeme $r(x)$ zapsat ve tvaru $[0, -4, 3]$.

Použití Konvence 2.3 může být také užitečné pro kratší formulace některých tvrzení.

Lemma 2.5. *Nechť $[a, b, c], [a', b', c'] \in C(D)$. Jestliže $[a, b, c] \sim [a', b', c']$, pak*

$$a \equiv a' \pmod 3.$$

Pomocí protipříkladu není obtížné dokázat, že opačná implikace neplatí. Zřejmě

$$[1,0,-1],[1,2,1] \in C(-23) \text{ a } [1,0,-1] \not\sim [1,2,1].$$

Následující Věta 2.6 má pro řešení Deloneho problému zásadní význam.

Věta 2.6. *Nechť $0 \neq D \in \mathbb{Z}$ a nechť $C(D) \neq \emptyset$. Pak $C(D)/\sim$ má konečně mnoho tříd.*

Věta 2.6 je důsledkem obecnějšího tvrzení, které dokázal v roce 1973 Kálmán Győry v článku [13, str. 419]. Viz také [8, str. 109] a [18, str. 475]. Alternativní důkaz Věty 2.6 může čtenář nalézt v článku [20, str. 107–108]. Tento důkaz je založen na následujícím významném výsledku Louise Mordella [27].

Věta 2.7 (L. J. Mordell, 1920)**.** *Nechť $0 \neq k \in \mathbb{Z}$. Pak Mordellova rovnice*

$$Y^2 = X^3 + k \tag{2.4}$$

má nejvýše konečně mnoho celočíselných řešení.

Pro nalezení všech celočíselných řešení rovnice (2.4) je možné použít metodu s níž se čtenář může podrobně seznámit v knize [30]. V současnosti je tato metoda implementována například v programech Magma a Sage.

Pro formulaci dalších výsledků budeme potřebovat několik označení. Předně, je-li A konečná množina, pak symbolem $\#A$ budeme označovat počet prvků množiny A. Dále, pro libovolné $0 \neq D \in \mathbb{Z}$, položme

$$c(D) = \begin{cases} \#C(D)/\sim, & \text{je-li } C(D) \neq \emptyset, \\ 0, & \text{je-li } C(D) = \emptyset. \end{cases}$$

Konečně, symbolem $R_C(D)$ označme množinu všech kanonických reprezentantů tříd rozkladu množiny $C(D)/\sim$. Množina $R_C(D)$ se nazývá úplný systém kanonických reprezentantů množiny $C(D)/\sim$. Je zřejmé, že platí

$$\#R_C(D) = \#C(D)/\sim = \ c(D).$$

Některé základní vlastnosti množiny $R_C(D)$ popisuje následující věta.

Věta 2.8. *Nechť $0 \neq D \in \mathbb{Z}$. Pak platí:*

(i) $[0,u,v] \in R_C(D)$ *právě tehdy, když* $[0,u,-v] \in R_C(D)$.
(ii) $[1,u,v] \in R_C(D)$ *právě tehdy, když* $[2,u+1,u-v] \in R_C(D)$.

Jestliže $v \neq 0$, pak v části (i) Věty 2.8 platí $[0,u,v] \not\sim [0,u,-v]$. Podobně v části (ii) platí $[1,u,v] \not\sim [2,u+1,u-v]$ pro libovolné u,v. Dále je možné dokázat, že část (ii) Věty 2.8 může být formulována v následujícím ekvivalentním tvaru

$$[2,r,s] \in R_C(D) \text{ právě tehdy, když } [1,r-1,r-s-1] \in R_C(D).$$

Je zřejmé, že vztahy (i) a (ii) uvedené ve Větě 2.8 mají praktický význam. Například, pokud víme, že $[1,-3077,64681] \in R_C(-76)$, pak také $[2,-3076,-67758] \in R_C(-76)$.

2.2. Případ množin $C(0)$ a $R_C(0)$

Množiny $C(0)$ a $R_C(0)$ tvoří výjimku celé teorie, kterou je nutné vyřešit samostatně. Úplný popis množin $C(0)$ a $R_C(0)$ uvedeme ve Větě 2.9.

Věta 2.9. *Nechť $f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]$. Pak $f(x) \in C(0)$ právě tehdy, když existují $e \in \{0,1,2\}$, $v, w \in \mathbb{Z}$ tak, že*

$$\begin{aligned} f(x) &= x^3 + (3w+e)x^2 + (3w^2+2ew-3v^2-2ev)x + w^3 + ew^2 \\ &\quad - (3v^2+2ev)w + 2v^3 + ev^2 \\ &= (x+w-v)^2(x+w+2v+e). \end{aligned}$$

Rozklad $C(0)/\sim$ má nekonečně mnoho tříd a množina všech kanonických reprezentantů $R_C(0)$ může být zapsána ve tvaru

$$R_C(0) = \{[e, -3v^2-2ev, 2v^3+ev^2] : e \in \{0,1,2\}, v \in \mathbb{Z}\}.$$

Důkaz Věty 2.9 lze nalézt v [20, str. 110].

2.3. Mordellova rovnice $Y^2 = X^3 - 432D$

Základní souvislost mezi množinou $C(D)$ a Mordellovou rovnicí $Y^2 = X^3 - 432D$ poskytuje Věta 2.10.

Věta 2.10. *Nechť $0 \neq D \in \mathbb{Z}$. Jestliže Mordellova rovnice*

$$Y^2 = X^3 + k, \quad \text{kde} \quad k = -432D = -2^4 3^3 D$$

nemá celočíselné řešení, pak $C(D) = \emptyset$.

Důkaz této věty lze nalézt v [20, str. 106].

Příklad 2.11. (i) Nechť $D \in \{-1,-2,-5,-6,-9,-10\}$. Pak žádná z Mordellových rovnic $Y^2 = X^3 - 432D$ nemá celočíselné řešení. Podle Věty 2.10 pak platí

$$C(-1) = C(-2) = C(-5) = C(-6) = C(-9) = C(-10) = \emptyset.$$

(ii) Nechť $D \in \{2,6,7,9,10\}$. Pak žádná z Mordellových rovnic $Y^2 = X^3 - 432D$ nemá celočíselné řešení. Podle Věty 2.10 pak platí

$$C(2) = C(6) = C(7) = C(9) = C(10) = C(11) = \emptyset.$$

Kombinací Lemma 2.1 a Příkladu 2.11 obdržíme Větu 2.12.

Věta 2.12. *Pro každé $D \in \mathbb{Z}$ nastane právě jedna z možností: množina $C(D)$ je buď prázdná, nebo nekonečná.*

Pro každé $0 \neq D \in \mathbb{Z}$ položme

$$M_C(D) = \{[X_0, Y_0] : X_0, Y_0 \in \mathbb{Z}, Y_0^2 = X_0^3 - 432D\} \text{ a } m_C(D) = \#M_C(D).$$

Zaměřme nyní krátce pozornost na aritmetické vlastnosti celočíselných řešení rovnice $Y^2 = X^3 - 432D$, kde $D \neq 0$. Speciální tvar koeficientu $-432D$ způsobuje, že rovněž celočíselná řešení této rovnice mají některé speciální vlastnosti. Například pro každé $[X_0, Y_0] \in M_C(D)$ platí $X_0 \equiv 0 \pmod 2$ právě tehdy, když $Y_0 \equiv 0 \pmod 2$. Můžeme tedy zavést následující definici.

(i) Řešení $[X_0, Y_0] \in M_C(D)$ budeme nazývat liché, když X_0 a Y_0 jsou lichá.
(ii) Řešení $[X_0, Y_0] \in M_C(D)$ budeme nazývat sudé, když X_0 a Y_0 jsou sudá

Zkoumání celkového počtu lichých a sudých řešení rovnice $Y^2 = X^3 - 432D$ odhalilo následující skutečnost. Nechť

$$G = \{D \in \mathbb{Z} : 0 \neq |D| \leq 1000\} \quad \text{a} \quad H = \bigcup_{D \in G} M_C(D).$$

Pak v množině H existuje přibližně 33% lichých řešení a 67% sudých řešení. Tento objev vede k zajímavé hypotéze, totiž že asymptotický poměr počtu lichých a sudých řešení Mordellovy rovnice $Y^2 = X^3 - 432D$ je roven $1/2$. Podrobnější informace může čtenář nalézt v [20, str. 112].

Při konstrukci množiny $C(D)$ hraje důležitou roli také Lemma 2.13.

Lemma 2.13. *Nechť $X_0, Y_0 \in \mathbb{Z}$. Pak existuje nejvýše jedno číslo $e \in \{0, 1, 2\}$ splňující soustavu kongruencí*

$$4e^2 - X_0 \equiv 0 \pmod{12}, \quad 4e^3 - 3eX_0 + Y_0 \equiv 0 \pmod{108}. \tag{2.5}$$

Pro formulaci Věty 2.14 bude vhodné zavést následující označení. Nechť

$$E_C(D) = \big\{[[X_0, Y_0], e] \in M_C(D) \times \{0, 1, 2\} : 4e^2 - X_0 \equiv 0 \pmod{12},\\ 4e^3 - 3eX_0 + Y_0 \equiv 0 \pmod{108}\big\}.$$

Věta 2.14. *Nechť $0 \neq D \in \mathbb{Z}$ a nechť $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$. Pak $f(x) \in C(D)$ právě tehdy, když existují $w \in \mathbb{Z}$ a $[[X_0, Y_0], e] \in E_C(D)$ tak, že*

$$a = 3w + e,$$
$$b = 3w^2 + 2ew + \frac{4e^2 - X_0}{12},$$
$$c = w^3 + ew^2 + \frac{4e^2 - X_0}{12}w + \frac{4e^3 - 3eX_0 + Y_0}{108}.$$

Navíc, pokud $f(x) \in C(D)$, pak

$$r(x) = f(x - w) = x^3 + ex^2 + \frac{4e^2 - X_0}{12}x + \frac{4e^3 - 3eX_0 + Y_0}{108}$$

je kanonický reprezentant třídy $[f(x)]$.

Z Věty 2.14 ihned plyne, že lichá řešení $[X_0, Y_0] \in M_C(D)$ nemohou splňovat podmínku $[[X_0, Y_0], e] \in E_C(D)$ pro žádné $e \in \{0, 1, 2\}$. V následujícím příkladu ukážeme, že i když množina $M_C(D)$ obsahuje sudá řešení, množina $C(D)$ může být prázdná.

Příklad 2.15. Uvažujme Mordellovu rovnici $Y^2 = X^3 - 432D$, kde $D = 33$. Pak $M_C(33) = \big\{[25, \pm 37], [36, \pm 180], [108, \pm 1116], [180, \pm 2412], [2113, \pm 97129]\big\}$ a $m_C(33) = 10$. Aplikací Věty 2.14 obdržíme, že $C(33) = \emptyset$ a $c(33) = 0$.

2.4. Metoda konstrukce množiny $C(D)$

Na základě předchozích výsledků můžeme vytvořit postup, pomocí kterého je možné určit množinu $C(D)$ pro libovolné $0 \neq D \in \mathbb{Z}$. Postup lze formálně rozdělit do čtyř následujících kroků:

1) Nechť $0 \neq D \in \mathbb{Z}$. Nejprve nalezneme množinu $M_C(D)$ všech celočíselných řešení $[X_0, Y_0]$ Mordellovy rovnice $Y^2 = X^3 - 432D$. Podle Věty 2.7 je množina $M_C(D)$ konečná. Je-li $M_C(D) = \emptyset$, pak výpočet končí. Z Věty 2.14 totiž plyne, že $C(D) = \emptyset$.
2) Předpokládejme, že $M_C(D) \neq \emptyset$. Ve druhém kroku určíme množinu $E_C(D)$. Pro každé $[X_0, Y_0] \in M_C(D)$ rozhodneme, zda existuje číslo $e \in \{0, 1, 2\}$, splňující soustavu kongruencí (2.5). Podle Lemma 2.13 vyhovuje této soustavě nejvýše jedno číslo $e \in \{0, 1, 2\}$. Protože $\#E_C(D) = \#C(D)/\!\sim$, platí, že $C(D) = \emptyset$ právě tehdy, když $E_C(D) = \emptyset$.
3) Předpokládejme, že $E_C(D) \neq \emptyset$. Ve třetím kroku určíme množinu $R_C(D)$, tj. úplný systém kanonických reprezentantů množiny $C(D)/\!\sim$. Vzhledem k Větě 2.14 platí

$$R_C(D) = \left\{ \left[e, \frac{4e^2 - X_0}{12}, \frac{4e^3 - 3eX_0 + Y_0}{108} \right] : [[X_0, Y_0], e] \in E_C(D) \right\}. \tag{2.6}$$

4) Ve čtvrtém, závěrečném kroku nalezneme množinu $C(D)$. Aplikací vzorce (2.2) pro všechna $r(x) \in R_C(D)$ obdržíme

$$C(D) = \bigcup_{r(x) \in R_C(D)} \left\{ x^3 + \frac{r''(w)}{2!}x^2 + \frac{r'(w)}{1!}x + r(w) : w \in \mathbb{Z} \right\}. \tag{2.7}$$

Výše uvedený postup budeme demonstrovat na Příkladu 2.16.

Příklad 2.16. Nechť $D = 29$. Nalezněte množinu $C(29)$.
Nejprve určíme množinu $M_C(29)$. Rovnice $Y^2 = X^3 - 12528$ má 10 řešení a

$$M_C(29) = \big\{[24, \pm 36], [33, \pm 153], [112, \pm 1180], [384, \pm 7524], [528, \pm 12132]\big\}.$$

Dále, pro každé $[X_0, Y_0] \in M_C(29)$ nalezneme řešení soustavy kongruencí (2.5) a určíme množinu $E_C(29)$.

$$E_C(29) = \big\{[[112, -1180], 1], [[112, 1180], 2]\big\}.$$

Aplikací vztahu (2.6) obdržíme množinu $R_C(29)$, tj. úplný systém kanonických reprezentantů množiny $C(29)/\!\sim$.

$$R_C(29) = \{x^3 + x^2 - 9x - 14,\ x^3 + 2x^2 - 8x + 5\}.$$

Odtud plyne, že $c(29) = \#C(29)/\!\sim\ = \#R_C(29) = 2$. Podle Konvence 2.3 můžeme množinu $R_C(29)$ zapsat stručně ve tvaru $R_C(29) = \big\{[1, -9, -14], [2, -8, 5]\big\}$. Konečně aplikací vzorce (2.7) nalezneme

$$\begin{aligned} C(29) = \{&x^3 + (3w+1)x^2 + (3w^2 + 2w - 9)x + w^3 + w^2 - 9w - 14 : w \in \mathbb{Z}\} \cup \\ &\{x^3 + (3w+2)x^2 + (3w^2 + 4w - 8)x + w^3 + 2w^2 - 8w + 5 : w \in \mathbb{Z}\}. \end{aligned}$$

2.5. Tabulky kanonických reprezentantů tříd rozkladu množiny $C(D)/\sim$

V roce 2022 byla metoda konstrukce množiny $C(D)$ použita pro sestavení tabulek kanonických reprezentantů tříd rozkladu množiny $C(D)/\sim$ pro všechna $D \in \mathbb{Z}$, kde $1 \leq |D| \leq 1000$. Dosažené výsledky byly prezentovány v publikaci [21]. V roce 2023 se podařilo tabulky [21] rozšířit pro všechna $D \in \mathbb{Z}$, kde $1 \leq |D| \leq 10000$. Rozšířená verze tabulek byla publikována v [23].

3. Problém kvartických polynomů a jeho řešení

Je zřejmé, že analogický problém k Problému 1.1 je možné formulovat také pro případ kvartických polynomů. Pro libovolné $D \in \mathbb{Z}$ definujme množinu

$$Q(D) = \big\{f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x] : D(f) = D\big\},$$

kde $D(f)$ označuje diskriminant polynomu $f(x)$. Je dobře známo, že pomocí koeficientů a, b, c, d lze diskriminant $D(f)$ vyjádřit ve tvaru

$$\begin{aligned} D(f) = {} & a^2b^2c^2 - 4a^2b^3d - 4a^3c^3 + 18a^3bcd - 27a^4d^2 - 4b^3c^2 \\ & + 16b^4d + 18abc^3 - 80ab^2cd - 6a^2c^2d + 144a^2bd^2 \\ & - 27c^4 + 144bc^2d - 128b^2d^2 - 192acd^2 + 256d^3. \end{aligned} \tag{3.1}$$

Problém 3.1 (2022)**.** Nechť $D \in \mathbb{Z}$. Nalezněte metodu, která umožní určit všechny normované kvartické polynomy s celočíselnými koeficienty mající diskriminant D.

Je zřejmé, že problém určit množinu $Q(D)$ je ekvivalentní problému nalézt všechna celočíselná řešení diofantické rovnice $D(f) = D$. Hlavním cílem této kapitoly je poskytnout čtenáři základní informace o řešení Problému 3.1, které bylo nalezeno v článku [22].

3.1. Ekvivalence na množině $Q(D)$

Nechť $f(x) = x^4 + ax^3 + bx^2 + cx + d \in Q(D)$. Pro každé $w \in \mathbb{Z}$ definujme polynom $f_w(x) = f(x+w)$. Podobně, jako v případě kubických polynomů, můžeme ověřit, že pro libovolné $w \in \mathbb{Z}$ platí rovnost $D(f_w) = D(f)$, jejímž důsledkem je Lemma 3.2.

Lemma 3.2. *Nechť $D \in \mathbb{Z}$. Je-li $Q(D) \neq \emptyset$, pak množina $Q(D)$ je nekonečná.*

Dále je možné dokázat, že pro polynomy $f_w(x)$ platí identita

$$f_w(x) = x^4 + \frac{f'''(w)}{3!}\,x^3 + \frac{f''(w)}{2!}\,x^2 + \frac{f'(w)}{1!}\,x + f(w), \tag{3.2}$$

ve které výrazy $f'(w)$, $f''(w)$ a $f'''(w)$ označují první, druhou a třetí derivaci $f(x)$ v bodě w. Nechť $Q(D) \neq \emptyset$. Pro $f(x), g(x) \in Q(D)$ položme

$$f(x) \sim g(x) \iff \exists\, w \in \mathbb{Z} : g(x) = f(x + w).$$

Lemma 3.3. *Relace $\sim$ je ekvivalence na množině $Q(D)$.*

Nechť $f(x) = x^4 + ax^3 + bx^2 + cx + d \in Q(D)$. Pak existují jednoznačně určená čísla $w \in \mathbb{Z}$ a $e \in \{0, 1, 2, 3\}$ tak, že $a = 4w + e$. Položme $r(x) = f(x - w) =$

$$x^4+ex^3+(b-6w^2-3ew)x^2+(c+8w^3+3ew^2-2bw)+d-3w^4-ew^3+bw^2-cw. \quad (3.3)$$

Polynom $r(x)$ budeme nazývat kanonický reprezentant třídy

$$[f(x)] = \{g(x) \in Q(D) : g(x) \sim f(x)\} \in Q(D)/\sim .$$

Konvence 3.4. Pro zápis kvartického polynomu $f(x) = x^4+ax^3+bx^2+cx+d \in \mathbb{Z}[x]$ budeme používat stručnější vyjádření ve tvaru uspořádané čtveřice koeficientů $[a, b, c, d]$.

Příklad 3.5. Nechť $f(x) = x^4 - x^3 + 2x^2 - x + 1$. Z (3.1) plyne, že $D(f) = 12$, a tedy $Q(12) \neq \emptyset$. Podle Lemma 3.2 je množina $Q(12)$ nekonečná a třída rozkladu obsahující polynom $f(x)$ je tvaru $[f(x)] = \{x^4 + (4w - 1)x^3 + (6w^2 - 3w + 2)x^2 + (4w^3 - 3w^2 + 4w - 1)x + w^4 - w^3 + 2w^2 - w + 1 : w \in \mathbb{Z}\}$. Aplikací vztahu (3.3) obdržíme, že kanonický reprezentant třídy $[f(x)]$ je polynom $r(x) = x^4 + 3x^3 + 5x^2 + 4x + 2$ a podle Konvence 3.4 můžeme $r(x)$ zapsat ve tvaru $[3, 5, 4, 2]$.

Lemma 3.6. *Nechť* $[a, b, c, d], [a', b', c', d'] \in Q(D)$. *Jestliže platí* $[a, b, c, d] \sim [a', b', c', d']$, *pak*

$$a \equiv a' \pmod 4.$$

Pomocí protipříkladu není obtížné dokázat, že opačná implikace neplatí. Zřejmě

$$[1, -5, 4, -1], [1, -6, -3, 10] \in Q(-23) \quad \text{a} \quad [1, -5, 4, -1] \not\sim [1, -6, -3, 10].$$

Následující věta má pro řešení problému kvartických polynomů zásadní význam.

Věta 3.7. *Nechť* $0 \neq D \in \mathbb{Z}$ *a nechť* $Q(D) \neq \emptyset$. *Pak* $Q(D)/\sim$ *má konečně mnoho tříd.*

Věta 3.7 je rovněž důsledkem obecnějšího tvrzení, které dokázal Kálmán Győry v článku [13, str. 419]. Alternativní důkaz Věty 3.7 může čtenář nalézt v [22, str. 42]. Důkaz prezentovaný v [22] využívá podstatného rozšíření Mordellova výsledku formulovaného ve Větě 2.7. Toto rozšíření provedl v roce 1929 německý matematik Carl Ludwig Siegel (1896–1981) v článku [29]. Speciálním případem Siegelova výsledku je Věta 3.8.

Věta 3.8 (C. L. Siegel, 1929)**.** *Nechť* $\alpha, \beta \in \mathbb{Z}$ *a nechť* $4\alpha^3 + 27\beta^2 \neq 0$. *Pak eliptická rovnice*

$$\eta^2 = \xi^3 + \alpha\xi + \beta \quad (3.4)$$

má nejvýše konečně mnoho celočíselných řešení.

Pro nalezení všech celočíselných řešení rovnice (3.4) je možné použít, podobně jako v případě Mordellovy rovnice (2.4), metodu popsanou v knize [30] a implementovanou v programech Magma a Sage.

Pro formulaci dalších výsledků budeme potřebovat následující označení. Pro libovolné $0 \neq D \in \mathbb{Z}$, položme

$$q(D) = \begin{cases} \#Q(D)/\sim, & \text{je-li } Q(D) \neq \emptyset, \\ 0, & \text{je-li } Q(D) = \emptyset, \end{cases}$$

a symbolem $R_Q(D)$ označme množinu všech kanonických reprezentantů tříd rozkladu množiny $Q(D)/\sim$. Množinu $R_Q(D)$ budeme nazývat úplný systém kanonických reprezentantů množiny $Q(D)/\sim$. Je zřejmé, že $\#R_Q(D) = \#Q(D)/\sim = q(D)$.

3.2. Souvislost mezi Mordellovou rovnicí a množinou $Q(D)$

Základním objevem, který umožňuje určit všechny prvky množiny $Q(D)$ je nalezení souvislosti mezi množinou $Q(D)$ a Mordellovou rovnicí (1.1) pro speciální hodnotu koeficientu k. Tuto souvislost popisuje následující věta.

Věta 3.9. *Nechť $0 \neq D \in \mathbb{Z}$. Jestliže Mordellova rovnice*

$$Y^2 = X^3 + k, \quad kde \quad k = -1769472D = -2^{16}3^3D \tag{3.5}$$

nemá celočíselné řešení, pak $Q(D) = \emptyset$.

Pro každé $0 \neq D \in \mathbb{Z}$ položme

$$M_Q(D) = \left\{[X_0, Y_0] : X_0, Y_0 \in \mathbb{Z}, Y_0^2 = X_0^3 - 2^{16}3^3D\right\} \quad \text{a} \quad m_Q(D) = \#M_Q(D).$$

Je možné dokázat, že opačná implikace k Větě 3.9 neplatí. Z předpokladu $M_Q(D) \neq \emptyset$ tedy obecně neplyne $Q(D) \neq \emptyset$.

Příklad 3.10.
(i) Nechť $D = 2$. Pak $M_Q(2) = \emptyset$ a podle Věty 3.9 platí, že $Q(2) = \emptyset$.
(ii) Nechť $D = -7$. Pak $M_Q(-7) = \{[-192, \pm 2304], [16, \pm 3520], [960, \pm 29952]\}$, a tedy $m_Q(-7) = 6$. Přesto ale $Q(-7) = \emptyset$. Skutečnost, že $Q(-7) = \emptyset$ je možné dokázat pomocí Věty 3.12, která bude uvedena v následujícím odstavci.

3.3. Eliptická rovnice $\eta^2 = \xi^3 - 108X_0\xi + 432Y_0$

Při konstrukci množiny $Q(D)$ hraje důležitou roli Lemma 3.11.

Lemma 3.11. *Nechť $\xi_0, \eta_0 \in \mathbb{Z}$. Pak existuje nejvýše jedno číslo $e \in \{0, 1, 2, 3\}$ splňující soustavu kongruencí $\xi_0 \equiv 36e^2 \pmod{96}$, $\eta_0 \equiv 9e\xi_0 - 108e^3 \pmod{1728}$.*

Následující Věta 3.12 je nejdůležitějším tvrzením celé teorie. Poskytuje nutnou a postačující podmínku pro $Q(D) \neq \emptyset$. Věta 3.12 má konstruktivní charakter, tj. umožňuje určit konkrétní tvary kanonických reprezentantů množiny $Q(D)/\sim$.

Věta 3.12. *Nechť $0 \neq D \in \mathbb{Z}$ a nechť $M_Q(D) \neq \emptyset$. Pak $Q(D) \neq \emptyset$ právě tehdy, když existuje $[X_0, Y_0] \in M_Q(D)$ tak, že eliptická rovnice*

$$\eta^2 = \xi^3 - 108X_0\xi + 432Y_0 \tag{3.6}$$

má aspoň jedno celočíselné řešení $[\xi_0, \eta_0]$ splňující soustavu kongruencí

$$36e^2 - \xi_0 \equiv 0 \pmod{96}, \tag{3.7}$$

$$108e^3 - 9e\xi_0 + \eta_0 \equiv 0 \pmod{1728}, \tag{3.8}$$

$$432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0 \equiv 0 \pmod{110592} \tag{3.9}$$

pro nějaké $e \in \{0,1,2,3\}$. *Pak polynom*

$$r(x) = x^4 + ex^3 + \frac{36e^2 - \xi_0}{96}\,x^2 + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}\,x + \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592}$$

leží v množině $Q(D)$.

Nechť $0 \neq D \in \mathbb{Z}$ a nechť $M_Q(D) \neq \emptyset$. Pak pro každé $[X_0, Y_0] \in M_Q(D)$ definujeme množinu $\mathscr{E}(D, X_0, Y_0) = \{[X_0, Y_0, \xi_0, \eta_0] : \xi_0, \eta_0 \in \mathbb{Z}, \eta_0^2 = \xi_0^3 - 108X_0\xi_0 + 432Y_0\}$ a klademe $e(D, X_0, Y_0) = \#\mathscr{E}(D, X_0, Y_0)$. Dále položme

$$\mathscr{E}(D) = \bigcup_{[X_0,Y_0]\in M_Q(D)} \mathscr{E}(D, X_0, Y_0), \quad e(D) = \#\mathscr{E}(D),$$

$$E_Q(D) = \big\{[[X_0, Y_0, \xi_0, \eta_0], e] \in \mathscr{E}(D) \times \{0,1,2,3\} : e \in \{0,1,2,3\} \text{ splňuje pro } [X_0, Y_0, \xi_0, \eta_0] \text{ soustavu kongruencí (3.7)–(3.9)}\big\}.$$

Věta 3.13 je důsledkem Věty 3.12.

Věta 3.13. *Nechť* $0 \neq D \in \mathbb{Z}$ *a nechť* $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$. *Pak* $f(x) \in Q(D)$ *právě tehdy, když existují* $[[X_0, Y_0, \xi_0, \eta_0], e] \in E_Q(D)$ *a* $w \in \mathbb{Z}$ *tak, že*

$$\begin{aligned} a &= 4w + e, \\ b &= 6w^2 + 3ew + \frac{36e^2 - \xi_0}{96}, \\ c &= 4w^3 + 3ew^2 + \frac{36e^2 - \xi_0}{48}w + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}, \\ d &= w^4 + ew^3 + \frac{36e^2 - \xi_0}{96}\,w^2 + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}\,w \\ &\quad + \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592}. \end{aligned}$$

3.4. Metoda určení množiny $Q(D)$

Na základě teoretických výsledků prezentovaných v předchozích odstavcích můžeme vytvořit postup umožňující určit množinu $Q(D)$ pro každé $0 \neq D \in \mathbb{Z}$. Tento postup může být formálně rozdělen do pěti následujících kroků.

1) Nechť $0 \neq D \in \mathbb{Z}$. Nejprve nalezneme množinu $M_Q(D)$ všech celočíselných řešení $[X_0, Y_0]$ Mordellovy rovnice $Y^2 = X^3 - 2^{16}3^3D$. Podle Věty 2.7 je $M_Q(D)$ konečná množina a podle Věty 3.9 platí, že pokud $M_Q(D) = \emptyset$, pak $Q(D) = \emptyset$.
2) Nechť $M_Q(D) \neq \emptyset$. Pro každé $[X_0, Y_0] \in M_Q(D)$ sestavíme eliptickou rovnici $\eta^2 = \xi^3 - 108X_0\xi + 432Y_0$ a určíme množinu $\mathscr{E}(D, X_0, Y_0)$. Z Věty 3.8 plyne, že $\mathscr{E}(D, X_0, Y_0)$ je konečná množina pro každé $[X_0, Y_0] \in M_Q(D)$.

Sjednocením všech množin $\mathscr{E}(D, X_0, Y_0)$ obdržíme množinu $\mathscr{E}(D)$. Je-li $\mathscr{E}(D) = \emptyset$, pak $Q(D) = \emptyset$.

3) Nechť $\mathscr{E}(D) \neq \emptyset$. Pro každou čtveřici $[X_0, Y_0, \xi_0, \eta_0] \in \mathscr{E}(D)$ provedeme test, zda existuje číslo $e \in \{0, 1, 2, 3\}$ splňující soustavu kongruencí (3.7)–(3.9). Na základě těchto testů určíme množinu $E_Q(D)$. Je-li $E_Q(D) = \emptyset$, pak $Q(D) = \emptyset$.

4) Nechť $E_Q(D) \neq \emptyset$ a $\#E_Q(D) = n$. Každému prvku $\big[[X_0, Y_0, \xi_0, \eta_0], e\big] \in E_Q(D)$ přiřadíme polynom

$$\begin{aligned} r(x) &= x^4 + ex^3 + \frac{36e^2 - \xi_0}{96}x^2 + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}x \\ &\quad + \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592} \\ &= \left[e, \frac{36e^2 - \xi_0}{96}, \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}, \right. \\ &\qquad \left. \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592}\right] \end{aligned} \tag{3.10}$$

Podle Věty 3.12 leží polynom $r(x)$ v množině $R_Q(D)$ a přiřazení je bijektivním zobrazením mezi množinami $E_Q(D)$ a $R_Q(D)$. Tímto způsobem obdržíme úplný systém kanonických reprezentantů množiny $Q(D)/\!\sim$. Nechť $R_Q(D) = \{r_1(x), \ldots, r_n(x)\}$.

5) V závěrečném kroku konstrukce množiny $Q(D)$ přiřadíme každému $r_i(x) \in R_Q(D)$ třídu $[r_i(x)] = \{r_i(x + w) : w \in \mathbb{Z}\}$. Podle (3.2) platí, že

$$\begin{aligned} [r_i(x)] &= \left\{x^4 + \frac{r_i'''(w)}{3!}x^3 + \frac{r_i''(w)}{2!}x^2 + \frac{r_i'(w)}{1!}x + r_i(w) : w \in \mathbb{Z}\right\} \\ &= \left\{\left[\frac{r_i'''(w)}{3!}, \frac{r_i''(w)}{2!}, \frac{r_i'(w)}{1!}, r_i(w)\right] : w \in \mathbb{Z}\right\}. \end{aligned} \tag{3.11}$$

Sjednocením všech tříd $[r_i(x)]$ obdržíme množinu $Q(D)$.

$$Q(D) = \bigcup_{i=1}^{n} [r_i(x)] = \bigcup_{i=1}^{n}\left\{\left[\frac{r_i'''(w)}{3!}, \frac{r_i''(w)}{2!}, \frac{r_i'(w)}{1!}, r_i(w)\right] : w \in \mathbb{Z}\right\}.$$

Výše uvedený postup budeme demonstrovat na dvou příkladech.

Příklad 3.14. Nechť $D = 5$. Pak Mordellova rovnice (3.5) má tvar $Y^2 = X^3 - 8847360$. Tato rovnice má 6 celočíselných řešení

$$M_Q(5) = \{[256, \pm 2816], [384, \pm 6912], [5136, \pm 368064]\} \quad \text{a} \quad m_Q(5) = 6.$$

Ke každému ze šesti prvků množiny $M_Q(5)$ sestavíme odpovídající eliptickou rovnici (3.6) a tu vyřešíme. Řešením eliptických rovnic obdržíme následující množiny:

$$\mathscr{E}(5, 256, -2816) = \{[256, -2816, -48, 0]\},$$

$$\begin{aligned}
\mathscr{E}(5,256,2816) &= \{[256,2816,-96,\pm 1728],[256,2816,48,0],\\
&\qquad [256,2816,192,\pm 1728]\}\\
\mathscr{E}(5,384,-6912) &= \{[384,-6912,-144,0]\},\\
\mathscr{E}(5,384,6912) &= \{[384,6912,0,\pm 1728],[384,6912,144,0]\},\\
\mathscr{E}(5,5136,-368064) &= \{[5136,-368064,-432,0],[5136,-368064,-428,\pm 8],\\
&\qquad [5136,-368064,864,\pm 2592],\\
&\qquad [5136,-368064,103897,\pm 33488317]\},\\
\mathscr{E}(5,5136,368064) &= \{[5136,368064,432,0]\}.
\end{aligned}$$

Odtud plyne, že

$$\begin{aligned}
\mathscr{E}(5) = \{&[256,-2816,-48,0],[256,2816,-96,\pm 1728],[256,2816,48,0],\\
&[256,2816,192,\pm 1728],[384,-6912,-144,0],[384,6912,0,\pm 1728],\\
&[384,6912,144,0],[5136,-368064,-432,0],[5136,-368064,-428,\pm 8],\\
&[5136,-368064,864,\pm 2592],[5136,-368064,103897,\pm 33488317],\\
&[5136,368064,432,0]\},
\end{aligned}$$

a tedy, $e(5) = \#\mathscr{E}(5) = 18$. Dále, pro každý z osmnácti prvků množiny $\mathscr{E}(5)$ provedeme test, zda existuje číslo $e \in \{0,1,2,3\}$ splňující soustavu kongruencí (3.7)–(3.9). Na základě těchto testů zjistíme, že soustavě vyhovují pouze tři prvky množiny $\mathscr{E}(5)$. Z těchto prvků sestavíme množinu $E_Q(5)$.

$$\begin{aligned}
E_Q(5) = \{&[[256,2816,192,-1728],0],[[256,2816,192,1728],0],\\
&[[384,6912,144,0],0]\}.
\end{aligned}$$

Každému prvku množiny $E_Q(5)$ nyní přiřadíme uspořádanou čtveřici čísel definovanou vztahem (3.10). Tímto způsobem vytvoříme množinu $R_Q(5)$.

$$R_Q(5) = \{[2,0,-1,0],[0,-2,-1,0],[0,-2,1,0]\}.$$

Na základě Konvence 3.4 můžeme každou uspořádanou čtveřici ležící v množině $R_Q(5)$ interpretovat jako polynom. Platí tedy, že $R_Q(5) = \{r_1(x), r_2(x), r_3(x)\}$, kde

$$r_1(x) = x^4 + 2x^3 - x, \quad r_2(x) = x^4 - 2x^2 - x, \quad r_3(x) = x^4 - 2x^2 + x.$$

Polynomy $r_1(x)$, $r_2(x)$, $r_3(x)$ tvoří úplný systém kanonických reprezentantů množiny $Q(5)/\sim$. Platí tedy, že $\#R_Q(5) = \#Q(5)/\sim\, = q(5) = 3$. V závěrečném kroku postupu aplikujeme vztah (3.11), pomocí kterého každému reprezentantu $r_i(x) \in R_Q(5)$ přiřadíme třídu rozkladu $[r_i(x)]$. Sjednocením všech tříd $[r_i(x)]$ pak obdržíme množinu $Q(5)$.

$$\begin{aligned}
Q(5) = \{&[4w, 6w^2+3, 4w^3+6w-1, w^4+2w^3-w],\\
&[4w, 6w^2-2, 4w^3-4w-1, w^4-2w^2-w],\\
&[4w, 6w^2-2, 4w^3-4w+1, w^4-2w^2+w] : w \in \mathbb{Z}\}.
\end{aligned}$$

Příklad 3.15. Nechť $D = -87$. Pak Mordellova rovnice (3.5) má tvar $Y^2 = X^3 + 153944064$. Tato rovnice má 6 celočíselných řešení.

$$M_Q(-87) = \{[-320, \pm 11008], [-92, \pm 12376], [448, \pm 15616]\}.$$

Ke každému prvku množiny $M_Q(-87)$ sestavíme odpovídající eliptickou rovnici (3.6) a tu vyřešíme. Řešením těchto eliptických rovnic obdržíme následující množiny:

$$\begin{aligned}
\mathscr{E}(-87, -320, 11008) &= \{[-320, 11008, -80, \pm 1216], [-320, 11008, -48, \pm 1728], \\
&\quad [-320, 11008, 240, \pm 5184], [-320, 11008, 384, \pm 8640], \\
&\quad [320, 11008, 8592, \pm 796608]\}, \\
\mathscr{E}(-87, -320, -11008) &= \emptyset, \\
\mathscr{E}(-87, -92, 12376) &= \{[-92, 12376, -156, 0]\}, \\
\mathscr{E}(-87, -92, -12376) &= \{[-92, -12376, 156, 0]\}, \\
\mathscr{E}(-87, 448, 15616) &= \{[448, 15616, -156, \pm 3240], [448, 15616, 96, \pm 1728]\}, \\
\mathscr{E}(-87, 448, -15616) &= \emptyset.
\end{aligned}$$

Odtud plyne, že $e(-87) = \#\mathscr{E}(-87) = 16$. Pro každý z prvků množiny $\mathscr{E}(-87)$ provedeme test, zda existuje číslo $e \in \{0, 1, 2, 3\}$ splňující soustavu kongruencí (3.7)–(3.9). Na základě těchto testů zjistíme, že soustavě vyhovují pouze čtyři prvky množiny $\mathscr{E}(-87)$. Z těchto prvků sestavíme množinu $E(-87)$.

$$\begin{aligned}
E_Q(-87) = \{&[[-320, 11008, 240, 5184], 2], [[-320, 11008, 240, -5184], 2], \\
&[[448, 15616, -156, -3240], 1], [[448, 15616, -156, 3240], 3]\}.
\end{aligned}$$

Každému prvku množiny $E_Q(-87)$ přiřadíme uspořádanou čtveřici čísel definovanou vztahem (3.10). Tímto způsobem vytvoříme množinu

$$R_Q(-87) = \{[2, -1, 1, 0], [2, -1, -5, -3], [1, 2, -1, 0], [3, 5, 6, 3]\}.$$

Na základě Konvence 3.4 můžeme každou uspořádanou čtveřici ležící v množině $R_Q(-87)$ interpretovat jako polynom. Platí tedy, že

$$R_Q(-87) = \{r_1(x), r_2(x), r_3(x), r_4(x)\},$$

kde

$$\begin{aligned}
r_1(x) &= x^4 + 2x^3 - x^2 + x, \quad r_2(x) = x^4 + 2x^3 - x^2 - 5x - 3, \\
r_3(x) &= x^4 + x^3 + 2x^2 - x, \quad r_4(x) = x^4 + 3x^3 + 5x^2 + 6x + 3.
\end{aligned}$$

Polynomy $r_1(x), r_2(x), r_3(x), r_4(x)$ tvoří úplný systém kanonických reprezentantů množiny $Q(-87)/\!\sim$. Odtud plyne, že $\#R_Q(-87) = \#Q(-87)/\!\sim = q(-87) = 4$. V závěrečném kroku postupu aplikujeme vztah (3.11), pomocí kterého každému reprezentantu $r_i(x) \in R_Q(-87)$ přiřadíme třídu rozkladu $[r_i(x)]$. Sjednocením všech tříd $[r_i(x)]$ pak obdržíme množinu

$$\begin{aligned}
Q(-87) = \big\{&[4w + 2, 6w^2 + 6w - 1, 4w^3 + 6w^2 - 2w + 1, w^4 + 2w^3 - w^2 + w], \\
&[4w + 2, 6w^2 + 6w - 1, 4w^3 + 6w^2 - 2w - 5,
\end{aligned}$$

$$w^4 + 2w^3 - w^2 - 5w - 3],$$
$$[4w + 1, 6w^2 + 3w + 2, 4w^3 + 3w^2 + 4w - 1, w^4 + w^3 + 2w^2 - w],$$
$$[4w + 3, 6w^2 + 9w + 5, 4w^3 + 9w^2 + 10w + 6,$$
$$w^4 + 3w^3 + 5w^2 + 6w + 3] : w \in \mathbb{Z}\big\}.$$

3.5. Tabulky kanonických reprezentantů tříd rozkladu množiny $Q(D)/\sim$

V roce 2024 byla metoda konstrukce množiny $Q(D)$ použita pro sestavení tabulek kanonických reprezentantů tříd rozkladu množiny $Q(D)/\sim$ pro všechna $D \in \mathbb{Z}$, kde $1 \leq |D| \leq 1000$. Dosažené výsledky byly prezentovány v publikaci [24].

3.6. Sudá a lichá řešení Mordellovy rovnice $Y^2 = X^3 - 2^{16}3^3D$

V následujícím lemmatu uvedeme některé základní vlastnosti celočíselných řešení Mordellovy rovnice $Y^2 = X^3 - 2^{16}3^3D$.

Lemma 3.16. *Nechť $0 \neq D \in \mathbb{Z}$ a nechť $[X_0, Y_0] \in M_Q(D)$. Pak platí:*

(i) *Jestliže $2|X_0$, pak $4|X_0$, $8|Y_0$.*
(ii) *Jestliže $2|Y_0$, pak $4|X_0$, $8|Y_0$.*
(iii) *Jestliže $3|X_0$, pak $9|Y_0$.*
(iv) *Jestliže $3|Y_0$, pak $3|X_0$, $9|Y_0$.*

Kombinací vlastností (i) a (ii) obdržíme, že $X_0 \equiv 0 \pmod 2 \iff Y_0 \equiv 0 \pmod 2$. Je tedy přirozené zavést, podobně jako v případě kubických polynomů, následující definice:

Řešení $[X_0, Y_0] \in M_Q(D)$ se nazývá sudé, když X_0 a Y_0 jsou sudá čísla.
Řešení $[X_0, Y_0] \in M_Q(D)$ se nazývá liché, když X_0 a Y_0 jsou lichá čísla.

Dále, pro každé $0 \neq D \in \mathbb{Z}$ položme

$$\mathcal{E}(D) = \{[X_0, Y_0] \in M_Q(D) : X_0 \equiv Y_0 \equiv 0 \pmod 2\},$$
$$\mathcal{O}(D) = \{[X_0, Y_0] \in M_Q(D) : X_0 \equiv Y_0 \equiv 1 \pmod 2\}.$$

Pak $\mathcal{E}(D) \cap \mathcal{O}(D) = \emptyset$ a $\mathcal{E}(D) \cup \mathcal{O}(D) = M(D)$. Konečně pro každé přirozené číslo n definujme

$$\varepsilon(n) = \sum_{D=1}^{n} \#\mathcal{E}(D), \quad \varepsilon(-n) = \sum_{D=-1}^{-n} \#\mathcal{E}(D),$$
$$o(n) = \sum_{D=1}^{n} \#\mathcal{O}(D), \quad o(-n) = \sum_{D=-1}^{-n} \#\mathcal{O}(D).$$

Výpočet hodnot čísel $\varepsilon(n)$, $\varepsilon(-n)$, $o(n)$ a $o(-n)$ prezentovaný v článku [22, str. 46] odhalil následující významný rozdíl mezi počtem sudých a lichých řešení:

$$\varepsilon(-1000) = 1572, \quad \varepsilon(1000) = 1090, \quad o(-1000) = 100, \quad o(1000) = 44.$$

Z uvedených hodnot plyne, že existuje přibližně 95% sudých a pouze 5% lichých řešení Mordellovy rovnice $Y^2 = X^3 - 2^{16}3^3D$ pro $0 \neq |D| \leq 1000$. Tato překvapující skutečnost se stala inspirací k podrobnějšímu studiu sudých řešení. Hlavním dosaženým výsledkem je tvrzení, že pro každé sudé řešení Mordellovy rovnice může být odpovídající eliptická rovnice (3.6) nahrazena eliptickou rovnicí (3.13), jejíž celočíselné koeficienty jsou v absolutní hodnotě podstatně menší, než koeficienty v rovnici (3.6) .

Věta 3.17. *Nechť $0 \neq D \in \mathbb{Z}$ a nechť $[X_0, Y_0] \in \mathcal{E}(D)$.*

(i) *Jestliže kongruence $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{27}$ neplatí pro žádné $\alpha \in \{0, 1, 2\}$, pak soustava diofantických rovnic*

$$R^2 + 3T = X_0, \quad R^3 - 9RT + 108S^2 = Y_0 \tag{3.12}$$

není řešitelná v oboru celých čísel.

(ii) *Jestliže kongruence $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{27}$ platí pro nějaké $\alpha \in \{0, 1, 2\}$, pak α je jednoznačně určeno, $X_0 - 4\alpha^2 \equiv 0 \pmod{12}$, $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{108}$ a množina K všech celočíselných řešení soustavy (3.12) může být získána z množiny L všech celočíselných řešení eliptické rovnice*

$$\eta^2 = \xi^3 - \alpha\xi^2 - \frac{X_0 - 4\alpha^2}{12}\,\xi + \frac{3\alpha X_0 + Y_0 - 4\alpha^3}{108}\,. \tag{3.13}$$

Navíc mezi množinami L a K existuje vzájemně jednoznačné zobrazení $\varphi : L \to K$ definované vztahem

$$\varphi(\xi_0, \eta_0) = \left[-3\xi_0 + \alpha, \eta_0, 2\alpha\xi_0 - 3\xi_0^2 + \frac{X_0 - \alpha^2}{3}\right] = [R_0, S_0, T_0] \in K. \tag{3.14}$$

(iii) *Nechť $[R_0, S_0, T_0] \in K$ a nechť*

$$g(x) = x^4 + \frac{R_0}{8}\,x^2 + \frac{S_0}{8}\,x + \frac{T_0}{256} \in \mathbb{Q}[x].$$

Dále nechť $e \in \{0, 1, 2, 3\}$ a $g_e(x) = g(x + e/4) \in \mathbb{Q}[x]$. Pak $D(g) = D(g_e) = D$ a

$$g_e(x) \in R_Q(D) \Longleftrightarrow g_e(x) \in \mathbb{Z}[x]. \tag{3.15}$$

Postup nalezení množiny $R_Q(D)$ v případě sudých řešení Mordellovy rovnice budeme demonstrovat na následujícím příkladu.

Příklad 3.18. Nechť $D = -87$. Pak $[X_0, Y_0] = [-320, 11008] \in \mathcal{E}(-87)$ a pro $\alpha = 1$ platí $3\alpha X_0 + Y_0 - 4\alpha^3 = 10044 \equiv 0 \pmod{27}$. Podle Věty 3.17 můžeme množinu K všech celočíselných řešení systému diofantických rovnic

$$R^2 + 3T = -320, \quad R^3 - 9RT + 108S^2 = 11008$$

získat pomocí množiny L všech celočíselných řešení eliptické rovnice

$$\eta^2 = \xi^3 - \xi^2 + 27\xi + 93.$$

Protože

$$L = \{[-1, \pm 8], [7, \pm 24], [11, \pm 40], [239, \pm 3688]\},$$

aplikací zobrazení (3.14) obdržíme, že

$$K = \{[4, \pm 8, -112], [-20, \pm 24, -240], [-32, \pm 40, -448], [-716, \pm 3688, -170992]\}.$$

Dále aplikací vztahu (3.15) zjistíme, že pouze dva prvky ležící v množině K vedou k polynomům s celočíselnými koeficienty. Z trojice $[-20, -24, -240]$ obdržíme pro $e = 2$ polynom $[2, -1, -5, -3] \in R_Q(-87)$ a trojice $[-20, 24, -240]$ vede pro $e = 2$ k polynomu $[2, -1, 1, 0] \in R_Q(-87)$. Všechny prvky množiny $R_Q(-87)$ získáme analogickým postupem, který aplikujeme na zbývající řešení $[X_0, Y_0] \in \mathcal{E}(-87) = M_Q(-87)$. Viz Příklad 3.15.

Na závěr poznamenejme, že množina K může být určena také pomocí množiny

$$H = \{[-80, \pm 1216], [-48, \pm 1728], [240, \pm 5184], [384, \pm 8640], [8592, \pm 796608]\}$$

všech celočíselných řešení eliptické rovnice (3.6), tj. rovnice

$$\eta^2 = \xi^3 + 34560\xi + 4755456.$$

Množinu K nalezneme tak, že každému prvku $[\xi_0, \eta_0] \in H$ přiřadíme trojici

$$\left[-\frac{\xi_0}{12}, \frac{\eta_0}{216}, \frac{144X_0 - \xi_0^2}{432}\right]$$

a ze všech získaných trojic vybereme pouze ty, které mají všechny souřadnice celočíselné.

3.7. Nové hypotézy týkající se Mordellovy rovnice

Nechť $0 \neq D \in \mathbb{Z}$ a nechť

$$\mu(D) = \begin{cases} 0, & \text{když } M_Q(D) = \emptyset, \\ 1, & \text{když } M_Q(D) \neq \emptyset. \end{cases}$$

Dále pro každé přirozené číslo n položme

$$\sigma(n) = \sum_{D=1}^{n} \mu(D) \quad \text{a} \quad \sigma(-n) = \sum_{D=-1}^{-n} \mu(D).$$

Výpočtem hodnot $\sigma(n)$ a $\sigma(-n)$ pro $n \leq 1000$ bylo v [22, str. 48] zjištěno, že

$$\frac{\sigma(1000)}{1000} = \frac{280}{1000} = 0{,}280, \quad \frac{\sigma(-1000)}{1000} = \frac{426}{1000} = 0{,}426, \quad \frac{\sigma(1000)}{\sigma(-1000)} = \frac{280}{426} \approx 0{,}657.$$

Uvedené výsledky mohou vést k následujícím hypotézám:

$$\begin{gathered} \lim_{n\to\infty} \frac{\sigma(n)}{n} = \frac{2}{7} \approx 0{,}286, \quad \lim_{n\to\infty} \frac{\sigma(-n)}{n} = \frac{3}{7} \approx 0{,}429, \\ \lim_{n\to\infty} \frac{\sigma(n)}{\sigma(-n)} = \frac{2}{3} \approx 0{,}667. \end{gathered} \tag{3.16}$$

Domněnky prezentované v (3.16) vedou k další zajímavé otázce, totiž zda podobné hypotézy mohou být formulovány také pro případ obecné Mordellovy rovnice. Je zřejmé, že ke stanovení takových hypotéz bude zapotřebí mnoha výpočtů na počítači. Díky výpočtům, které provedli Michael A. Bennett a Amir Ghadermarzi v článku [1], jsou známa všechna celočíselná řešení Mordellovy rovnice

$Y^2 = X^3 + k$ pro každé $k \in \mathbb{Z}$, kde $0 \neq |k| \leq 10^7$. Na základě výsledků těchto autorů mohou být formulovány nové hypotézy.

Pro každé $0 \neq k \in \mathbb{Z}$ nechť $\mathbb{M}(k)$ označuje množinu všech celočíselných řešení Mordellovy rovnice $Y^2 = X^3 + k$ a nechť

$$\nu(k) = \begin{cases} 0, & \text{když } \mathbb{M}(k) = \emptyset, \\ 1, & \text{když } \mathbb{M}(k) \neq \emptyset. \end{cases}$$

Dále, pro každé přirozené číslo n položme

$$s(n) = \sum_{k=1}^{n} \nu(k) \quad \text{a} \quad s(-n) = \sum_{k=-1}^{n} \nu(-k).$$

Z Tabulky 1 a Tabulky 2, které jsou prezentovány v článku [1, str. 642–643] obdržíme, že

$$\frac{s(10^7)}{10^7} = \frac{1332934}{10^7} \approx 0{,}133, \quad \frac{s(-10^7)}{10^7} = \frac{834604}{10^7} \approx 0{,}083,$$
$$\frac{s(-10^7)}{s(10^7)} = \frac{834604}{1332934} \approx 0{,}626.$$

Uvedené výsledky mohou vést k následujícím hypotézám:

$$\lim_{n\to\infty} \frac{s(n)}{n} = \frac{2}{15} = 0{,}1\bar{3}, \quad \lim_{n\to\infty} \frac{s(-n)}{n} = \frac{1}{12} = 0{,}08\bar{3},$$
$$\lim_{n\to\infty} \frac{s(-n)}{s(n)} = \frac{5}{8} = 0{,}625. \tag{3.17}$$

Domněnky (3.16) a (3.17) byly předloženy v článku [22, str. 49] ve formě problému: Dokažte nebo vyvraťte hypotézy (3.16) a (3.17).

4. Perspektivy dalšího výzkumu

Předně tabulky uvedené v publikacích [21] a [23] mohou poskytnout důležitá vodítka pro další výzkum obtížné problematiky týkající se zákona zachování rozkladu kubických polynomů nad konečnými tělesy $\mathbb{F}_p$, kde p je prvočíslo. Odkazy na literaturu týkající se tohoto problému může čtenář nalézt například v [21, str. 46]. Rovněž tabulky prezentované v [24] mohou sehrát důležitou roli při studiu analogického problému pro kvartické polynomy.

Dále je možné soustředit pozornost na nalezení důkazů hypotéz uvedených v článku [22, str. 48–49]. Tyto hypotézy se týkají asymptotického poměru počtu řešitelných a neřešitelných Mordellových rovnic. Volným pokračováním této studie by mohlo být určení asymptotického poměru počtu lichých a sudých řešení Mordellovy rovnice $Y^2 = X^3 + k$, kde $k = -432D$ a $k = -1769472D$. Některé dílčí výsledky týkající se tohoto problému byly publikovány v článcích [20, str. 112] a [22, str. 46].

Jiný možný směr výzkumu může souviset s revizí výsledků, které se týkají struktury množiny $Q(D)/\sim$. Revize by měla vést k přesnější a ucelenější představě o

počtu tříd množiny $Q(D)/\sim$ a k podrobnějšímu popisu vztahů mezi reprezentanty těchto tříd.

Konečně je možné zaměřit pozornost na popis podobností a odlišností struktur množin $C(D)/\sim$ a $Q(D)/\sim$. Lze očekávat, že důležitou roli v této otázce budou hrát Mordellovy rovnice $Y^2 = X^3 - 432D$ a $Y^2 = X^3 - 1769472D$.

Vyřešení uvedených problémů by mohlo být další částí pokračujícího příběhu kubických a kvartických rovnic.

Reference

[1] M. A. Bennett, A. Ghadermarzi: *Mordell's equation: a classical approach*, LMS Journal of Computation and Mathematics **18.1** (2015), 633–646.

[2] B. N. Delone: *Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante*, Mathematische Zeitschrift **31** (1930), 1–26.

[3] B. N. Delone, D. K. Faddeev: *Těorija irracionalnostěj tretěj stěpeni*, Trudy Matematičeskogo Instituta imeni V. A. Steklova XI, Moskva–Leningrad, 1940.

[4] B. N. Delone, D. K. Faddeev: *The Theory of Irrationalities of the Third Degree*, Translations of Mathematical Monographs 10, AMS providence, 1964.

[5] L. E. Dickson: *History of the Theory of Numbers – Diophantine Analysis*, Volume II, Chelsea, New York, (1952).

[6] W. J. Ellison, F. Ellison, J. Pesek, C. E. Stahl, D. S. Stall: *The diophantine equation* $y^2+k = x^3$, Journal of Number Theory **4** (1972), 107–117.

[7] J.-H. Evertse: *On the representation of integers by binary cubic forms of positive discriminant*, Inventiones mathematicae, **73** (1983), 117–138.

[8] J.-H. Evertse, K. Győry: *Discriminant Equations in Diophantine Number Theory*, New Mathematical Monographs 32, Cambridge University Press, 2016.

[9] J.-H. Evertse, K. Győry: *Unit Equations in Diophantine Number Theory*, Cambridge Studies in Advanced Mathematics **146**, Cambridge University Press, 2016.

[10] J.-H. Evertse, K. Győry: *Effective Results and Methods for Diophantine Equations over Finitely Generated Domains*, London Mathematical Society Lecture Note Series **475**, 2022.

[11] S. Gauthier, F. Lê: *On the youthful writings of Louis J. Mordell on the Diophantine equation* $y^2 - k = x^3$, Archive for History of Exact Sciences **73** (2019), 427–468.

[12] J. Gebel, A. Pethö, G. H. Zimmer: *On Mordell's equation*, Compositio Mathematica **110** (1998), 335–367.

[13] K. Győry: *Sur les polynômes à coefficients entiérs et de discriminant donné*, Acta Arithmetica **23** (1973), 419–426.

[14] K. Győry: *Sur les polynômes à coefficients entiérs et de discriminant donné* II, Publicationes Mathematicae Debrecen **21** (1974), 125–144.

[15] K. Győry: *Sur les polynômes à coefficients entiérs et de discriminant donné* III, Publicationes Mathematicae Debrecen **23** (1976), 141–165.

[16] K. Győry: *Sur les polynômes à coefficients entiérs et de discriminant donné* IV, Publicationes Mathematicae Debrecen **25** (1978), 155–167.

[17] K. Győry: *On polynomials with integer coefficients and given discriminant* V, p-adic generalizations, Acta Mathematica Academiae Scientiarum Hungaricae **32** (1978), 175–190.

[18] K. Győry: *Polynomials and binary forms with given discriminant*, Publicationes Mathematicae Debrecen **69.4** (2006), 473–499.

[19] O. Hemer: *On the Diophantine Equation* $y^2 - k = x^3$, Uppsala (1952).

[20] J. Klaška: *On cubic polynomials with a given discriminant*, Mathematics for Applications **10** (2021), 103–113.

[21] J. Klaška: *Tabulky reprezentantů kubických polynomů s daným diskriminantem*, Akademické nakladatelství CERM, Brno, 2022.

[22] J. Klaška: *Quartic polynomials with a given discriminant*, Mathematica Slovaca **72.1** (2022), 35–50.
[23] J. Klaška: *The Full Systems of Canonical Representatives of Cubic Polynomials with a Given Discriminant*, Akademické nakladatelství CERM, Brno, 2023.
[24] J. Klaška: *Tabulky reprezentantů kvartických polynomů s daným diskriminantem*, Akademické nakladatelství CERM, Brno, 2024.
[25] J. London, M. Finkelstein: *On Mordell's Equation* $y^2-k=x^3$, Bowling Green, Ohio Bowling Green State University, 1973.
[26] L. J. Mordell: *The diophantine equation* $y^2-k=x^3$, Proceedings of the London Mathematical Society **13** (1913), 60–80.
[27] L. J. Mordell: *A statement by Fermat*, Proceedings of the London Mathematical Society, 2nd ser. **18** (1920), pp. v–vi.
[28] L. J. Mordell: *Diophantine Equations*, Pure and Applied Mathematics **30**, Academic Press, London–New York, 1969.
[29] C. L. Siegel: *Über einige Anwendungen diophantischer Approximationen*, Abhandlungen der Preußischer Akademie der Wissenschaften. Physikalisch–mathematische Klasse, 1–41, 1929.
[30] N. P. Smart: *The Algorithmic Resolution of Diophantine Equations*, Cambridge University Press, 1998.

Jiří Klaška, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 61669 Brno, Česká republika,
e-mail: klaska@fme.vutbr.cz