ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ
KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

# KLASICKÉ I MODERNÍ FAKTORIZAČNÍ ALGORITMY

BAKALÁŘSKÁ PRÁCE

**Petra Pojarová**

*B1001 Přírodovědná studia, obor Matematická studia*

Vedoucí práce: doc. RNDr. Jaroslav Hora, CSc.

**Plzeň 2020**

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, 30. června 2020

.....

vlastnoruční podpis

Poděkování

Ráda bych poděkovala svému vedoucímu bakalářské práce doc. RNDr. Jaroslavu Horovi, CSc. za odborné vedení, věcné připomínky a zejména za vstřícný přístup při zpracování této práce. Dále bych ráda poděkovala své rodině a přátelům za veškerou podporu ve studiu.

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta pedagogická
Akademický rok: 2019/2020

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

| | |
|---|---|
| Jméno a příjmení: | **Petra POJAROVÁ** |
| Osobní číslo: | **P19B0056P** |
| Studijní program: | **B1001 Přírodovědná studia** |
| Studijní obor: | **Matematická studia** |
| Téma práce: | **Klasické i moderní faktorizační algoritmy.** |
| Zadávající katedra: | **Katedra matematiky, fyziky a technické výchovy** |

## Zásady pro vypracování

1. Rozklad přirozeného čísla v součin prvočísel. Metoda opakovaného dělení.
2. Fermatova faktorizační metoda.
3. Eulerova faktorizační metoda.
4. Pollardova p-1 metoda. Metoda kvadratického síta – příklad.

Rozsah bakalářské práce: **30 – 50**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

Childs, L. N. A Concrete Introduction to Higher Algebra. 2. ed., Springer, 1996.
Crandall, R., Pomerance, C. Prime Numbers. A Computational Perspective. Second Edition, Springer, 2005.
Gathen von zur, J., Gerhard, J. Modern Computer Algebra, 3. vydání, Cambridge Univ. Press, 2013.
Wagstaff, S. The Joy of Factoring, American Mathematical Society, 2013.

Vedoucí bakalářské práce: **Doc. RNDr. Jaroslav Hora, CSc.**
Katedra matematiky, fyziky a technické výchovy

Datum zadání bakalářské práce: **1. října 2019**
Termín odevzdání bakalářské práce: **30. června 2020**

Západočeská univerzita v Plzni
Fakulta pedagogická
6

L.S.

v z.

**Doc. RNDr. Pavel Mentlík, Ph.D.**
děkan

**Prof. PaedDr. Jarmila Honzíková, Ph.D.**
vedoucí katedry

V Plzni dne 17. října 2019

# OBSAH

# SEZNAM ZKRATEK A SYMBOLŮ

NSD – největší společný dělitel

NSN – nejmenší společný násobek

$a|b$ – číslo $b$ je dělitelné číslem $a$ beze zbytku, tedy existuje číslo $c = b/a$

$\lfloor N \rfloor$ – hodnota celého čísla $N$

$\mathbb{Z}_{\varphi_{(n)}}$ – množina zbytkových tříd pro $\varphi_{(n)}$

$\equiv$ – je kongruentní s (modulo)

$\not\equiv$ – není kongruentní s

$\wedge$ – a zároveň

$=$ – rovná se

$\neq$ – nerovná se

$\leq$ – je menší nebo roven

$<$ – je menší než

$\Longrightarrow$ – implikuje; vyplývá

# ÚVOD

Tématem této bakalářské práce jsou „Klasické i moderní faktorizační algoritmy“. V bakalářské práci jsou podrobně rozebrány metody rozkladu čísel, tedy zejména algoritmy, kterými se faktorizují velká čísla. Během studia se studenti zabývají především jednoduchými postupy rozkladu čísel, jako je například zkusmé dělení. Tato práce přispěje k prohloubení dosavadních znalostí a představí další možné postupy pro faktorizaci čísel. Problematika samotné faktorizace je rozsáhlejší než samotné nahodilé nebo záměrné dělení čísel. Přestože se nejedná o složitou problematiku, jde o matematickou operaci, která je časově a paměťově velmi náročná.

Pro faktorizaci malých čísel stačí základní matematické znalosti. Již na základní škole se faktorizace používá pro nalezení největšího společného dělitele a nejmenšího společného násobku dvou nebo více čísel. Pokud bychom se pokoušeli faktorizovat větší čísla je možné využít stejných postupů, ale časová náročnost je pro ně příliš vysoká. S nástupem počítačů se proces faktorizace urychlil, ale pro vysoká čísla v řádu několika tisíců cifer, ani za využití počítače nelze provést faktorizaci v přijatelném čase.

V bakalářské práci je uvedeno shrnutí základních i pokročilejších algoritmů. Ke každému faktorizačnímu algoritmu je podrobně vysvětlen postup a uveden alespoň jeden řešený příklad pro srozumitelnější pochopení jednotlivých metod a algoritmů.

Obsahem první kapitoly je seznámení se základními matematickými pojmy, které jsou důležité pro faktorizaci, jsou jimi například prvočíslo, složené číslo, čtvercové číslo atd. Dále je zde podrobněji vysvětlen proces faktorizace a jeho využití v matematice a šifrování.

V druhé kapitole jsou uvedeny základní postupy pro testování prvočíselnosti. Testování prvočíselnosti lze využít tak, abychom zbytečně neprováděli faktorizaci vysokých čísel, která jsou prvočísly, u kterých tedy nejde nalézt jejich faktory.

Hlavním cílem této práce je seznámení s vybranými klasickými i moderními faktorizačními metodami a jejich podrobnější popis, kterým se věnují poslední dvě kapitoly této práce. Ve třetí kapitole jsou rozepsány klasické faktorizační algoritmy. Poslední čtvrtá kapitola se zabývá moderními faktorizačními algoritmy.

# 1 ÚVOD DO FAKTORIZACE

Tato kapitola je zaměřená na vysvětlení základních matematických pojmů, jako jsou například prvočíslo, složené číslo, nesoudělná čísla atd. Pro pochopení faktorizačních algoritmů je nutné nejprve vysvětlit, co znamená pojem faktorizace.

## 1.1 FAKTORIZACE

Faktorizace představuje proces rozkladu libovolného čísla $N$ na součin menších čísel, v ideálním případě na součin prvočísel. Proces faktorizace má význam pro nalezení vlastního dělitele nebo při hledání největšího společného dělitele a nejmenšího společného násobku dvou čísel. [1]

## 1.2 ZÁKLADNÍ POJMY VE FAKTORIZACI

V následující kapitole budou shrnuty základní pojmy a matematické procesy, které se v rámci faktorizačních metod používají a které je třeba znát pro jejich rychlejší a správné pochopení.

**Prvočísla**

Za prvočíslo je možné označit takové přirozené číslo, které je větší než 1, a zároveň je beze zbytku dělitelné pouze jedničkou a sebou samým. Z tohoto tvrzení lze odvodit, že libovolné přirozené číslo větší než 2 je číslem složeným nebo prvočíslem. [2], [24]

Výčet prvočísel od 1 do 100: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

**Složené číslo**

Za složené číslo se označuje přirozené číslo, které má alespoň jednoho přirozeného dělitele různého od jedničky a sebe samého. Složené číslo lze tedy beze zbytku dělit minimálně třemi čísly, tyto tři dělitele mají především čísla, která jsou tvořena mocninami prvočísla, ostatní složená čísla mají čtyři a více dělitelů. Každé složené číslo lze zapsat jako součin dvou menších čísel. Nejmenším složeným číslem je číslo 4, jelikož je dělitelné jedničkou, samo sebou a dvojkou. [3]

**Prvočíselný rozklad**

Jedná se o matematický pojem, který charakterizuje vyjádření přirozeného čísla jako součin mocnin prvočísel. Nechť je $N$ libovolné přirozené číslo větší než 1, potom je jeho prvočíselný rozklad roven $p_1^{s_1} \cdot p_2^{s_2} \cdot p_3^{s_3} \cdot \ldots \cdot p_n^{s_n}$, kde $p_i$ je prvočíslem. Rozklad musí splňovat dvě základní podmínky. První podmínkou je, že exponenty $s_i$ jsou nenulová kladná celá čísla. Druhá podmínka je vzájemná různost prvočísel seřazených podle velikosti.

Příklad prvočíselného rozkladu se může ukázat na číslech 24 nebo 8 400, obě tato čísla jsou čísly složenými, tudíž je lze zapsat jako součin prvočísel. Číslo 24 se může faktorizovat na: $24 = 2^3 \cdot 3^1$ druhé číslo $8\,400$ se může rozložit na součin: $8\,400 = 2^4 \cdot 3^1 \cdot 5^2 \cdot 7^1$.

**Čtvercové číslo**

Pojmem čtvercové číslo nebo čtverec se označuje takové celé číslo, které lze zapsat jako druhou mocninu celého čísla. Například čísla 49 a 121 jsou čtvercovým číslem, protože mohou být zapsána jako $7^2$ a $11^2$. [4]

**Čísla soudělná**

Čísla soudělná znamenají taková čísla, která mají alespoň jednoho společného dělitele s výjimkou čísla 1. Například čísla 21 a 18 jsou čísla soudělná, protože jejich společným dělitelem je číslo 3.

**Čísla nesoudělná**

Čísla nesoudělná nemají jiného společného dělitele než číslo 1. Například čísla 15 a 23 jsou čísla nesoudělná, jelikož pro ně nelze nalézt jiného společného dělitele než 1. [5]

## 1.3 VYUŽITÍ FAKTORIZACE V MATEMATICE

Proces rozkládání přirozených čísel na součin prvočísel se učí děti již v 6. třídě základní školy. V matematice se faktorizace přirozených čísel využívá především pro nalezení nejmenšího společného násobku (NSN) a největšího společného dělitele (NSD) dvou či více čísel. Pro daná čísla se určí součin prvočísel odpovídající jejich hodnotě, ze kterého se následně získá NSD a NSN.

### 1.3.1 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL

Pro nalezení nevětšího společného dělitele a nejmenšího společného násobku je možné využít následující postup. Jednotlivá přirozená čísla se rozepíší na součin prvočísel. Pro určení největšího společného dělitele je třeba nalézt součin čísel, který je shodný v obou rozkladech. Například pro čísla 60 a 5 544, která se dají rozepsat jako součin prvočísel $2 \cdot 2 \cdot 3 \cdot 5$ a $2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7 \cdot 11$, lze určit jejich největší společný dělitel jako $2 \cdot 2 \cdot 3 = 12$.

Pokud neexistuje shodný součin nebo alespoň jedno společné číslo v obou rozkladech, znamená to, že čísla nemají žádného společného dělitele kromě 1, jsou tedy nesoudělná. Například čísla 209 a 135, čísla se dají rozložit na 11·19 a 5·3·3·3. V těchto rozkladech nelze najít shodný součin a ani jedno společné číslo.

Naopak pokud první rozklad obsahuje celý součin druhého rozkladu, znamená to, že první číslo je násobkem druhého. Toto platí například pro čísla 75 867 a 2 299, která se dají rozložit na 19·11·11·11·3 a 19·11·11.

### 1.3.2 NEJMENŠÍ SPOLEČNÝ NÁSOBEK

Pro hledání nejmenšího společného násobku lze opět využít rozkladu na součin prvočísel. V postupu se využije celý součin jednoho z rozkladů, ke kterému je doplněn součin čísel, která jsou obsažena v rozkladu druhém, ale zároveň nejsou již obsažena v prvním vybraném rozkladu.

Pro znázornění lze využít opět čísla 60 a 5 544. Vybere se jeden z rozkladů, například $2 \cdot 2 \cdot 3 \cdot 5$, ke kterému se doplní součin čísel $2 \cdot 3 \cdot 7 \cdot 11$. Tímto se získá nejmenší společný násobek $2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 27\,720$.

Uvedené postupy je možné využít při hledání NSD a NSN i pro více čísel. Při hledání NSD se opět hledá společná část obsažená ve všech prvočíselných rozkladech. Pro získání NSN se k vybranému rozkladu postupně přidává součin chybějících čísel obsažených ve zbývajících rozkladech.

## 1.4 VYUŽITÍ FAKTORIZACE V ŠIFROVÁNÍ

Samotné šifrování zpráv bylo již vynalezeno před stovkami let. Uvádí se, že Gaius Julius Caesar užíval jednoduchou šifru, v níž při šifrování bylo každé písmeno nahrazené jiným písmenem. Je zřejmé, že v dnešní době by nebylo dešifrování této metody příliš složité. Dnešní šifrovací metody musejí být podstatně sofistikovanější, jelikož je zapotřebí počítat s tím, že existuje vyspělá výpočetní technika, která tyto jednoduché metody šifrování snadno rozluští. [9]

### 1.4.1 ŠIFROVACÍ METODA RSA

Šifrovací metodu RSA navrhli roku 1978 matematici Ronald Rivest, Adi Shamir a Leonard Adleman. Jedná se o šifru s jedním veřejným šifrovacím klíčem $(e, N)$ a jedním soukromým dešifrovacím klíčem $(d, N)$. Název šifrovací metody vychází z prvních písmen příjmení autorů. [10]

Pro šifrování pomocí RSA je nutné mít dvě různě velká náhodná prvočísla $p$ a $q$. Vynásobením těchto dvou čísel dostaneme tzv. modul $N = p \cdot q$. Dalším krokem je získání hodnoty Eulerovy funkce $\varphi_{(N)}$, která se vypočte podle následujícího vztahu:

$$\varphi_{(N)} = (p-1) \cdot (q-1)$$

Eulerova funkce $\varphi_{(N)}$ vyjadřuje počet všech celých čísel $k$ v rozsahu $1 \leq k \leq N$, která jsou taková, že platí $NSD(k, N) = 1$. [11]

Po výpočtu $\varphi_{(N)}$ zvolíme číslo $e$, pro které platí: $e < \varphi_{(N)} \wedge NSD\left(e, \varphi_{(N)}\right) = 1$. Posledním krokem je získání hodnoty $d$, kterou lze získat pomocí rozšířeného Eukleidova algoritmu. Podrobnější popis algoritmu je v kapitole 1.5.

$$\varphi_{(N)} = e \cdot n_1 + z_1$$

$$e = z_1 \cdot n_2 + z_2$$

Tabulka 1 – Rozšířený Eukleidův algoritmus

| | | | |
|---|---|---|---|
| | $\varphi_{(N)}$ | $\alpha_1 = 1$ | $\beta_1 = 0$ |
| | $e$ | $\alpha_2 = 0$ | $\beta_2 = 1$ |
| $n_1$ | $z_1$ | $\alpha_3 = \alpha_1 - \alpha_2 \cdot n_1$ | $\beta_3 = \beta_1 - \beta_2 \cdot n_1$ |
| … | … | … | … |
| $n_n$ | $z_n = 1$ | $\alpha_n = \alpha_{n-2} - \alpha_{n-1} \cdot n_n$ | $\beta_n = \beta_{n-2} - \beta_{n-1} \cdot n_n$ |

Číslo $\beta_n$ je multiplikativní inverzí čísla $e$ v $\mathbb{Z}_{\varphi_{(N)}}$, tedy nalezne se takové číslo $d$ pomocí kterého můžeme zprávu rozšifrovat.

$$d = \beta_n$$

Pro zašifrování zprávy $m$, kterou chceme poslat je třeba znát šifrovací exponent $e$ a modul $n$, pomocí kterých se vytvoří zašifrovaná zpráva $c$.

$$c = m^e \ (mod\ N)$$

Pro dešifrování přijaté zprávy $c$ je třeba znát dešifrovací exponent $d$ a modul $n$, pomocí kterých se zpráva uvede do původní podoby $m$.

$$m = c^d \ (mod\ N)$$

**Příklad 1: Šifrovací metoda RSA**

Za pomoci šifrování RSA zašifrujte a dešifrujte zprávu $m = 100$, pro šifrování zvolte prvočísla $p = 13$ a $q = 29$.

**Řešení**: V prvním kroku vypočteme modul $N$: $N = p \cdot q = 13 \cdot 29 = 377$.

Druhým krokem je získání hodnoty Eulerovy funkce: $\varphi_{(N)} = (p-1) \cdot (q-1) = (13-1) \cdot (29-1) = 12 \cdot 28 = 336$.

Předposledním krokem, než se bude moci zpráva $m$ zašifrovat, je zvolení si hodnoty $e$ pro kterou bude platit: $e < \varphi_{(N)} \wedge NSD(e, \varphi_{(N)}) = 1$. V tomto případě se zvolí číslo $e = 13$, pro které je předchozí podmínka splněna.

Posledním krokem pro nastavení šifrovacího systému je získání hodnoty $d$. Tato hodnota se zjistí pomocí Bézoutovy rovnosti jejíž výpočet je uveden v následující tabulce:

Tabulka 2 – Šifrovací metoda RSA – příklad

| | $\varphi_{(N)} = 336$ | 1 | 0 |
|---|---|---|---|
| | $e = 13$ | 0 | 1 |
| $n_1 = 25$ | $z_1 = 11$ | $1 - 0 \cdot 25 = 1$ | $0 - 1 \cdot 25 = -25$ |
| $n_2 = 1$ | $z_2 = 2$ | $0 - 1 \cdot 1 = -1$ | $1 - (-25) \cdot 1 = 26$ |
| $n_3 = 5$ | $z_3 = 1$ | $1 - (-1) \cdot 5 = 6$ | $-25 - 26 \cdot 5 = -155$ |

Pomocí rozšířeného Euklidova algoritmu se získala hodnota $d = -155$. Tato hodnota se může upravit, jelikož se počítá v modu 336, na $d = -155 + 336 = 181$.

Nyní se může zašifrovat zadaná zpráva $m = 100$, jelikož už známe šifrovací exponent $e = 13$ a modul $N = 377$, pomocí kterých se vytvoří zašifrovaná zpráva $c$.

$$c = m^e \ (mod\ N)$$

Dosazením do rovnice se získá:

$c = 100^{13}\ (mod\ 377)$

Protože by vycházeli vysoké hodnoty, které nemusejí být ani za pomoci výpočetní techniky zvladatelné, lze postup umocnění upravit. Mocninu 13 můžeme rozložit na součet čísel 1, 4 a 8.

$c = 100^{1+4+8}\ (mod\ 377) = 100^1 \cdot 100^4 \cdot 100^8\ (mod\ 377)$

Nyní stačí získat hodnotu mocniny pro daný součin čísel. Abychom nemuseli počítat s čísli s velkým množstvím cifer, lze každé číslo upravit do modulu 377.

$100^1 = 100\ (mod\ 377)$

Je zbytečné v každém kroku počítat mocninu z celého čísla zprávy $m$, postačí spočítat druhou mocninu zbytku z předchozího kroku.

$100^2 = 198\ (mod\ 377)$

$100^4 = 373\ (mod\ 377)$

$100^8 = 16\ (mod\ 377)$

Pro získání zprávy c je dostačující provést součin zbytků příslušných mocnin.

$c = 100 \cdot 373 \cdot 16\ (mod\ 377)$

$c = 596\,800\ (mod\ 377) = 9\ (mod\ 377)$

Za pomoci veřejného klíče se provedlo zašifrování zprávy $m$ do podoby $c$.

$m = 100 \implies c = 9$

Výpočtem bylo zjištěno, že zadaná zpráva $m = 100$ se zakóduje do podoby $c = 9$.

Pro dešifrování přijaté zprávy $c$ je třeba znát dešifrovací exponent $d$ a modul $N$, pomocí kterých se zpráva uvede do původní podoby $m$.

$$m = c^d \ (mod\ N)$$

Dosazením do rovnice se získá:

$m = 9^{181}\ (mod\ 377)$

Umocnění zašifrované zprávy $c$ se upraví na součet čísel 1, 4, 16, 32 a 128.

$m = 9^{1+4+16+32+12}\ \ (mod\ 377) = 9^1 \cdot 9^4 \cdot 9^{16} \cdot 9^{32} \cdot 9^{128} (mod\ 377)$

Opět se získá hodnota pro jednotlivé mocniny v modulu 377.

$9^1 = 9\ (mod\ 377)$

$9^4 = 152\ (mod\ 377)$

$9^{16} = 139\ (mod\ 377)$

$9^{32} = 94\ (mod\ 377)$

$9^{128} = 81\ (mod\ 377)$

Zpráva se dešifruje provedením součinu zbytků příslušných mocnin v modulu 377.

$m = 9 \cdot 152 \cdot 139 \cdot 94 \cdot 81\ (mod\ 377)$

$m = 1\ 447\ 817\ 328\ (mod\ 377) = 100\ (mod\ 377)$

Pomocí soukromého klíče se provedlo dešifrování zašifrované zprávy $c$ do původní podoby zprávy $m$.

$c = 9 \Longrightarrow m = 100$

Tento příklad využívá malých prvočísel $p$ a $q$ pro názorné představení postupu šifrování a dešifrování zprávy metodou RSA, takto malá čísla by byla velmi snadno rozluštitelná. V praxi by tato čísla měla tisíce až miliónů řádů cifer, postup metody je však totožný.

### 1.4.2 VÝZNAM PRVOČÍSEL V ŠIFROVACÍCH SYSTÉMECH

RSA je šifra, která je založena na veřejném klíči, jeho část se tvoří součinem dvou prvočísel $N = p \cdot q$. Jedná se o systém, který je možné použít jak pro šifrování zpráv, tak i pro elektronický podpis. Celý systém bezpečnosti systému RSA je postaven na

předpokladu, že je velmi obtížné, respektive v rozumném čase nemožné číslo $N$, které je součástí veřejného klíče, rozložit na původní faktory $p$ a $q$.

Pokud by byl vytvořen algoritmus, který by dokázal faktorizovat v reálném čase opravdu velká čísla (v řádu milionů cifer), tak by systém RSA byl snadno prolomitelný. Proto s délkou klíče stoupá obtížnost prolomení šifry a tím stoupá bezpečnost šifrování. Protože po získání faktorů $p$ a $q$ je relativně jednoduché získat i neveřejný klíč $(d, N)$ a zašifrovanou zprávu dešifrovat. Bezpečnost systémů šifrování, které jsou založeny na číslech složených z prvočísel, je přímo úměrná schopnosti faktorizace velkých čísel. [12]

## 1.5 ALGORITMY VYUŽÍVANÉ PŘI FAKTORIZACI

V této kapitole jsou uvedeny základní algoritmy, které se využívají jako pomocné nebo doplňkové k samotným algoritmům faktorizace.

### 1.5.1 EUKLIDŮV ALGORITMUS

Euklidův algoritmus je jeden z nejstarších algoritmů. Tímto algoritmem lze určit největšího společného dělitele dvou přirozených čísel, tedy takové největší přirozené číslo, kterým lze dělit obě přirozená čísla beze zbytku. Byl pojmenován podle řeckého matematika Euklida, který jej uvedl ve svém díle Základy, a to již ve 4. století př.n.l. [6],[7]

Existují dvě přirozená čísla $a$ a $b$, pro která když aplikujeme Euklidův algoritmus, se nalezne číslo $z$, které je jejich NSD. Postup hledání NSD pomocí Euklidova algoritmu je následující:

Vyšší číslo $a$ se vydělí číslem $b$, výsledek tohoto celočíselného dělení je číslo $n_1$ a číslo $z_1$ představuje zbytek po dělení.

$$a = b \cdot n_1 + z_1$$

Protože $NSD(a, b)$ musí být faktorem čísla $b$ a zároveň celá pravá strana musí být tímto faktorem dělitelná, je zjevné že bude dělitelný i zbytek. Je možné rovnici upravit a hledat $NSD(b,\ z_1)$. [8]

$$b = z_1 \cdot n_2 + z_2$$

Pokud po provedení tohoto úkonu není nalezen nulový zbytek, celý proces se opakuje s čísli $z_1$ a $z_2$, při kterých vznikne celočíselný zbytek $z_3$.

$$z_1 = z_2 \cdot n_3 + z_3$$

$$z_2 = z_3 \cdot n_4 + z_4$$

$$\dots$$

$$z_{n-2} = z_{n-1} \cdot n_n + z_n$$

$$z_{n-1} = z_n \cdot n_{n+1} + 0$$

Algoritmus se provádí do té doby, než se zbytek rovná nule. Výsledkem algoritmu je poté číslo $z_n$, které představuje NSD čísel $a$ a $b$. V případě, že výsledkem metody je číslo $z_n = 1$, znamená to, že čísla $a$ a $b$ jsou nesoudělná. [25]

**Příklad 2: Euklidův algoritmus**

Pomocí Euklidova algoritmu najděte NSD čísel $a = 91\,333$ a $b = 16\,093$.

**Řešení**: V prvním kroku se větší číslo vydělí menším číslem, při kterém se získá n-násobek čísla $b$. Sestaví se následující rovnice, ve které se větší číslo $a$ rovná součtu n-násobku čísla $b$ a zbytku $z_1$.

$a = b \cdot n_1 + z_1 \Longrightarrow 91\,333 = 16\,093 \cdot 5 + 10\,868$

Protože zbytek $z_1 \neq 0$ je nutné v algoritmu pokračovat s čísli 16 093 a 10 868. A tento postup opakovat do té doby, než se $z_i = 0$.

$b = z_1 \cdot n_2 + z_2 \Longrightarrow 16\,093 = 10\,868 \cdot 1 + 5\,225$

$z_1 = z_2 \cdot n_3 + z_3 \Longrightarrow 10\,868 = 5\,225 \cdot 2 + 418$

$z_2 = z_3 \cdot n_4 + z_4 \Longrightarrow 5\,225 = 418 \cdot 12 + 209$

$z_3 = z_4 \cdot n_5 + z_5 \Longrightarrow 418 = 209 \cdot 2 + 0$

Použitím Euklidova algoritmu bylo zjištěno, že největším společným dělitelem čísel $a = 91\,333$ a $b = 16\,093$ je číslo 209. Výsledek je možné ověřit pomocí metody rozkladu na součin prvočísel, kdy $a = 11^1 \cdot 19^2 \cdot 23^1$ a $b = 7^1 \cdot 11^2 \cdot 19^1$, největším společným dělitelem opět vychází číslo $11 \cdot 19 = 209$. U vyšších čísel je složité nalezení tohoto rozkladu, proto je výhodnější použití Euklidova algoritmu.

### 1.5.2 ROZŠÍŘENÝ EUKLIDŮV ALGORITMUS

Rozšířený Euklidův algoritmus vychází z Euklidova algoritmu, pomocí něhož je možné získat nejen největší společný dělitel čísel $a$ a $b$, ale i spočítat Bézoutovu rovnost, která říká, že NSD dvou přirozených čísel $a$ a $b$ je možné zapsat jako lineární kombinaci $a$ a $b$ s koeficienty $\alpha$ a $\beta$, které jsou celými čísly. [8]

$$\alpha \cdot a + \beta \cdot b = NSD(a, b)$$

Pomocí rozšířeného Euklidova algoritmu lze nalézt multiplikativní inverzi na tělese $\mathbb{Z}_p$, kde $p$ je prvočíslo.

Ze základního Euklidova algoritmu víme, že číslo $a$ lze napsat jako násobek $n_1$ čísla $b$ se zbytkem $z_1$. V rámci rozšířeného algoritmu se postupuje shodně se základním algoritmem, který je doplněn o výpočet Bézoutových koeficientů $\alpha$ a $\beta$.

$$a = b \cdot n_1 + z_1$$
$$b = z_1 \cdot n_2 + z_2$$

Tabulka 3 – Rozšířený Euklidův algoritmus

| | | | |
|---|---|---|---|
| | $a$ | $\alpha_1 = 1$ | $\beta_1 = 0$ |
| | $b$ | $\alpha_2 = 0$ | $\beta_2 = 1$ |
| $n_1$ | $z_1$ | $\alpha_3 = \alpha_1 - \alpha_2 \cdot n_1$ | $\beta_3 = \beta_1 - \beta_2 \cdot n_1$ |
| $n_2$ | $z_2$ | $\alpha_4 = \alpha_2 - \alpha_3 \cdot n_2$ | $\beta_4 = \beta_2 - \beta_3 \cdot n_2$ |
| … | … | … | … |
| $n_n$ | $z_n$ | $\alpha_n = \alpha_{n-2} - \alpha_{n-1} \cdot n_n$ | $\beta_n = \beta_{n-2} - \beta_{n-1} \cdot n_n$ |

Z předchozí rozepsané tabulky lze získat lineární kombinace čísel $a$ a $b$ v následujícím tvaru:

$$a = \alpha_1 \cdot a + \beta_1 \cdot b$$

$$b = \alpha_2 \cdot a + \beta_2 \cdot b$$

$$z_n = \alpha_{n+2} \cdot a + \beta_{n+2} \cdot b$$

Pokud jsou čísla $a$ a $b$ nesoudělná je číslo $\beta_n$ multiplikativní inverzní čísla $b$ v $\mathbb{Z}_a$.

**Příklad 3: Euklidův rozšířený algoritmus**

Pomocí Euklidova rozšířeného algoritmu najděte NSD čísel $a = 91\,333$ a $b = 16\,093$ a určete koeficienty $\alpha$ a $\beta$, tak aby se lineární kombinace čísel $a$ a $b$ rovnala $NSD(a, b)$ a nule.

**Řešení**: V první části výpočtu se postupuje podle základního Euklidova algoritmu. Větší číslo se vydělí menším číslem, při kterém se získá n-násobek a zbytek $z$ viz předchozí příklad.

Tabulka 4 - Rozšířený Euklidův algoritmus – příklad

| | | | |
|---|---|---|---|
| | $a = 91\,333$ | $\alpha_1 = 1$ | $\beta_1 = 0$ |
| | $b = 16\,093$ | $\alpha_2 = 0$ | $\beta_2 = 1$ |
| $n_1 = 5$ | $z_1 = 10\,868$ | $\alpha_3 = \alpha_1 - \alpha_2 \cdot n_1$<br>$\alpha_3 = 1 - 0 \cdot 5 = 1$ | $\beta_3 = \beta_1 - \beta_2 \cdot n_1$<br>$\beta_3 = 0 - 1 \cdot 5 = -5$ |
| $n_2 = 1$ | $z_2 = 5\,225$ | $\alpha_4 = \alpha_2 - \alpha_3 \cdot n_2$<br>$\alpha_4 = 0 - 1 \cdot 1 = -1$ | $\beta_4 = \beta_2 - \beta_3 \cdot n_2$<br>$\beta_4 = 1 - (-5) \cdot 1 = 6$ |
| $n_3 = 2$ | $z_3 = 418$ | $\alpha_5 = \alpha_3 - \alpha_4 \cdot n_3$<br>$\alpha_5 = 1 - (-1) \cdot 2 = 3$ | $\beta_5 = \beta_3 - \beta_4 \cdot n_3$<br>$\beta_5 = -5 - 6 \cdot 2 = -17$ |
| $n_4 = 12$ | $z_4 = 209$ | $\alpha_6 = \alpha_4 - \alpha_5 \cdot n_4$<br>$\alpha_6 = -1 - 3 \cdot 12 = -37$ | $\beta_6 = \beta_4 - \beta_5 \cdot n_4$<br>$\beta_6 = 6 - (-17) \cdot 12$<br>$= 210$ |
| $n_5 = 2$ | $z_5 = 0$ | $\alpha_7 = \alpha_5 - \alpha_6 \cdot n_5$<br>$\alpha_7 = 3 - (-37) \cdot 2 = 77$ | $\beta_7 = \beta_5 - \beta_6 \cdot n_5$<br>$\beta_7 = -17 - 210 \cdot 2$<br>$= -437$ |

Za použití rozšířeného Euklidova algoritmu byl určen největší společný násobek čísel $a = 91\,333$ a $b = 16\,093$, kterým je $z_4 = 209$. Dále byly zjištěny koeficienty $\alpha_6 = -37$ a $\beta_6 = 210$ pro které platí následující rovnost:

$$\alpha \cdot a + \beta \cdot b = NSD(a, b)$$

$$-37 \cdot 91\,333 + 210 \cdot 16\,093 = NSD(91\,333, 16\,093)$$

Pomocí algoritmu byly také zjištěny koeficienty $\alpha_7 = 77$ a $\beta_7 = -437$, pro které platí:

$$\alpha \cdot a + \beta \cdot b = 0$$

$77 \cdot 91\,333 + (-437) \cdot 16\,093 = 0$

Užitím těchto koeficientů se lineární kombinace $a$ a $b$ rovná nule.

**Příklad 4: Euklidův rozšířený algoritmus**

Prostřednictvím Euklidova rozšířeného algoritmu najděte multiplikativní inverzi čísla b na tělese $\mathbb{Z}_a$, $a = 53$ a $b = 13$.

**Řešení**: Opět se postupuje dle algoritmu a hledá se $NSD(a, b)$, který musí být roven 1 jinak by multiplikativní inverze neexistovala.

Tabulka 5 - Rozšířený Euklidův algoritmus – příklad

| | | | |
|---|---|---|---|
| | $a = 53$ | $\alpha_1 = 1$ | $\beta_1 = 0$ |
| | $b = 13$ | $\alpha_2 = 0$ | $\beta_2 = 1$ |
| $n_1 = 4$ | $z_1 = 1$ | $\alpha_3 = \alpha_1 - \alpha_2 \cdot n_1$<br>$\alpha_3 = 1 - 0 \cdot 4 = 1$ | $\beta_3 = \beta_1 - \beta_2 \cdot n_1$<br>$\beta_3 = 0 - 1 \cdot 4 = -4$ |

Podle Bézoutovy rovnosti platí následující vztah:

$$\alpha \cdot a + \beta \cdot b = 1$$

V tomto případě lze dosadit:

$1 \cdot 53 - 4 \cdot 13 = 1$

Protože se pohybujeme v $\mathbb{Z}_a$ jsou všechny násobky $a = 53$ rovny nule, předchozí vztah lze upravit do následující podoby:

$4 \cdot 13 \equiv 1\ (mod\ 53)$

Lze tedy říct, že číslo 4 je multiplikativní inverzí čísla 13 v $\mathbb{Z}_{53}$.

# 2 TESTOVÁNÍ PRVOČÍSELNOSTI

Protože faktorizace je proces rozkladu složených čísel na jejich faktory, v ideálním případě na součin prvočísel, je vhodné před zahájením faktorizace zjistit, zda zadané číslo není prvočíslem, u kterého faktorizaci nelze provést.

## 2.1 JEDNODUCHÉ ALGORITMY PRO TESTOVÁNÍ PRVOČÍSELNOSTI

V první části druhé kapitoly jsou uvedeny základní algoritmy pro testování prvočíselnosti. Tyto metody jsou praktické zejména pro menší čísla, u větších čísel narůstá jejich časová a paměťová náročnost.

### 2.1.1 ZKUSMÉ DĚLENÍ

Testování pomocí zkusmého dělení je jedna z nejjednodušších metod. Základním principem této metody je, že se číslo $N$ postupně zkouší dělit náhodnými čísly. Pokud je nalezen podíl roven celému číslu, znamená to, že byly nalezeny faktory čísla $N$, tedy se nejedná o prvočíslo. Princip této metody se využívá i při hledání samotných faktorů čísel. Podrobněji vysvětleno v kapitole 3.1 Metoda pokusného dělení.

### 2.1.2 ERATOSTHENOVO SÍTO

Z dalších algoritmů pro vyhledávání prvočísel se může využít algoritmus, který byl pojmenován po řeckém matematikovi Eratosthénovi z Kyrény. Eratosthenovo síto je jednoduchý algoritmus pro vyhledávání prvočísel ležících ve zvoleném intervalu (v intervalu od čísla 2 do zvoleného čísla).

Princip algoritmu je založen na vyškrtávání násobků jednotlivých čísel v tomto intervalu. Nejdříve je vytvořen seznam přirozených čísel jdoucí postupně od 2 do zadaného čísla. První zapsané číslo v seznamu se označí jako prvočíslo, a poté se následně vyškrtne ze seznamu. Postupně se vyškrtávají i všechny jeho násobky. V dalším kroku se opět vezme první číslo ze seznamu, opět se označí jako prvočíslo a stejně jako v předchozím kroku se provede vyškrtnutí čísla a jeho násobků. Tento postup se opakuje, dokud nejsou vyškrtána všechna čísla ze seznamu. Pokud je dosaženo poloviny intervalu, je možné označit všechna zbývající čísla jako prvočísla. Jelikož při překročení poloviny intervalu jsou násobky nevyškrtaných čísel již mimo

hledaný interval, a tedy zbývající čísla již nemohou být násobkem jiného čísla v seznamu. [10]

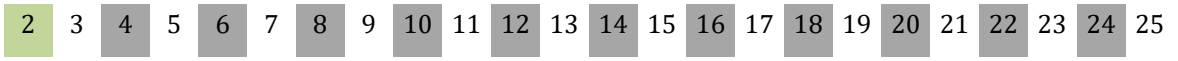
**Příklad 5: Eratosthenovo síto**

Pomocí algoritmu Erathosthenova síta najděte všechna prvočísla v daném intervalu <2;25>.

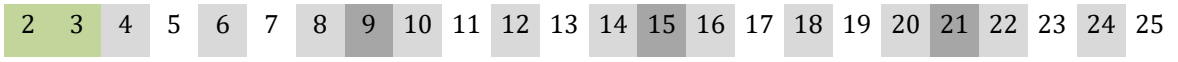
**Řešení**: Nejprve se vytvoří seznam přirozených čísel od 2 do 25.

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

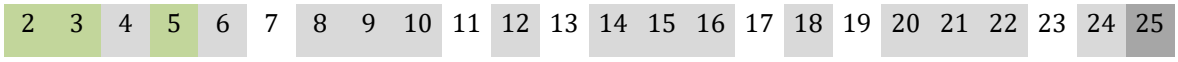
Dále si označíme první číslo ze seznamu jako prvočíslo a postupně se ze seznamu vyškrtají všechny násobky toho čísla.



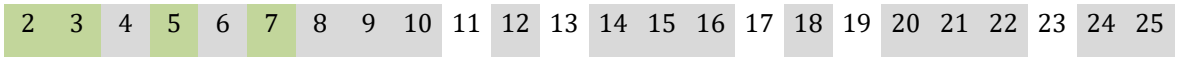
Prvním číslem v seznamu bylo číslo 2, které je prvním prvočíslem na daném intervalu. Ze seznamu byly vyškrtnuty všechny násobky čísla 2 (2; 4; 6; 8; 10; 12; 14; 16; 18; 20; 22; 24). V dalším kroku se postup opakuje.



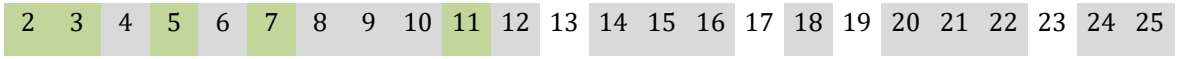
V tomto kroku bylo prvním číslem v seznamu číslo 3, číslo 3 je tedy druhým prvočíslem na daném intervalu. Opět byly vyškrtnuty všechny násobky tohoto čísla, které v seznamu zůstaly z předchozího kroku (3; 9; 15; 21).



V dalším kroku bylo označeno jako prvočíslo číslo 5 a ze seznamu byly vyškrtnuty jeho zbývající násobky (5 a 25).



V následujících krocích byla označena a vyškrtnuta čísla 7 a 11, jejich násobky byly již vyškrtnuty v předchozích krocích.



Veškerá zbývající nevyškrtnutá čísla lze označit jako prvočísla daného intervalu, protože jejich násobky jsou již mimo zadaný interval.

V tomto příkladě jsou zbývajícími prvočísly čísla 13; 17; 19 a 23.

Pomocí algoritmu Erathosthenova síta byla nalezena všechna prvočísla v intervalu od 2 do 25, kterými jsou čísla: 2; 3; 5; 7; 11; 13; 17; 19 a 23. [13]

## 2.2 OBECNÉ ALGORITMY PRO TESTOVÁNÍ PRVOČÍSELNOSTI

V druhé části druhé kapitoly jsou uvedeny obecné algoritmy pro testování prvočíselnosti. Na rozdíl od metod v předchozí kapitole následující metody umožňují snadněji testovat i vysoká čísla.

### 2.2.1 FERMATŮV TEST

Fermatův test prvočíselnosti je založen na Malé Fermatově větě, tedy že pro každé prvočíslo platí:

$$a^{p-1} \equiv 1 \ (mod\ p)$$

Neplatí-li pro testované číslo $p$ tato rovnost, číslo $p$ určitě není prvočíslem. Pokud tvrzení platí, dané číslo je možná prvočíslem. Slovo možná je zde uvedeno, protože pro Fermatův test existují tzv. Fermatova pseudoprvočísla. Pro tato čísla vychází Fermatův test prvočíselnosti jako pozitivní, i přesto že jsou to čísla složená. Z tohoto důvodu není v praxi Fermatův test příliš používán. [14]

### 2.2.2 MILLER-RABINŮV TEST

V praxi je více využívaný Miller-Rabinův test prvočíselnosti, který také využívá Malou Fermatovu větu doplněnou o následující vztah:

$$p - 1 = 2^b \cdot m$$

Kde $m$ je liché číslo. Kombinací těchto dvou vztahů lze získat následující vztah:

$$a^{2^b \cdot m} - 1 \equiv 0 \ (mod\ p)$$

Při ověřování prvočíselnosti čísla $N$ se ověřuje, zda platí výrazy z předchozích vztahů. Pokud je z podmínek alespoň jedna splněna, dá se říci, že číslo $N$ je s pravděpodobností 75 % prvočíslem. Pokud podmínky nejsou splněny, jedná se o složené číslo. [15]

# 3 KLASICKÉ FAKTORIZAČNÍ METODY

Obsahem této kapitoly jsou vybrané metody, které lze označit jako klasické metody faktorizace. Daly by se charakterizovat jako jednoduché metody se snadným postupem výpočtu. Jejich výhodou a zároveň jejich nevýhodou je, že jsou vytvořeny pro čísla určitého charakteru, což jim umožňuje tato čísla rychle faktorizovat, a však pro ostatní čísla mohou být tyto metody zdlouhavé nebo nevhodné.

## 3.1 METODA POKUSNÉHO DĚLENÍ

Metoda pokusného dělení je jednou z nejstarších a nejjednodušších metod faktorizace. Základním principem této metody je, že se faktorizované číslo $N$ postupně zkouší dělit prvočísly, která jsou menší než číslo $N$. Pokud se nalezne nějaké prvočíslo, které dělí $N$, tak se jednak našel prvočíselný faktor $N$ a jednak se dokázalo, že $N$ je složené číslo. Chceme-li číslo $N$ touto metodou faktorizovat úplně, musí se tak $N$ tímto prvočíslem dělit, dokud se dá dělit beze zbytku. Dále se pokračuje tak, že se vezme další prvočíslo a postup se opakuje.

Je dobré si uvědomit, že pro nalezení faktoru čísla $N$ nebo pro jeho úplnou faktorizaci, postačuje vyzkoušet pouze všechna prvočísla menší než $\lfloor\sqrt{N}\rfloor$.

Pro každé složené číslo, jehož jeden z faktorů je větší než $\sqrt{N}$, musí existovat faktor menší než $\sqrt{N}$. Pokud neexistuje faktor menší než $\sqrt{N}$, nemůže existovat ani faktor větší než $\sqrt{N}$, mimo případu, kdy je jedním faktorem samotné číslo $N$ a druhým faktorem je číslo 1. [16]

Tento fakt lze ověřit na jednoduchém příkladu, kdy se hledají faktory čísla 21. Prvním prvočíslem, kterým lze dělit číslo 21 beze zbytku, je číslo 3. Číslo 21 se tedy může rozdělit na faktory 3 a 7. Pokud by se hledaly faktory vyšší než $\sqrt{21}$ nalezl by se opět faktor 7, ke kterému náleží druhý faktor číslo 3. Tato dvojice faktorů byla nalezena již v intervalu od 2 do $\sqrt{21}$. V rámci metody je dostačující hledat faktory pouze v intervalu od 2 do $\sqrt{N}$.

**Příklad 6: Metoda pokusného dělení**

Pomocí metody pokusného dělení zjistěte faktory čísla 1 176.

**Řešení**: V prvním kroku se zkusí číslo 1 176 vydělit prvním prvočíslem, kterým je číslo 2. Po vydělení vyjde celočíselný zbytek 588. Toto číslo lze opět dělit prvočíslem 2. Po druhém vydělení se dostane celočíselný zbytek 294. Tento postup se opakuje, dokud je zbytkem dělení celé číslo. Pro tento případ je to třetí dělení, kdy se dostane zbytek číslo 147, které dále nejde dělit beze zbytku.

V následujícím kroku zbytek číslo 147 se vydělí dalším prvočíslem, kterým je číslo 3. Po vydělení se získá zbytek číslo 49, které už není možné dělit číslem 3 beze zbytku. Dalším prvočíslem je číslo 5. Tímto prvočíslem dělit zbytek číslo 49 beze zbytku nelze, proto se musí pokračovat v dělení s jiným prvočíslem. Následujícím prvočíslem je číslo 7, tímto prvočíslem lze vydělit zbytek číslo 49. Po vydělení zůstane zbytek číslo 7, které je samotné prvočíslem.

Číslo 1 176 lze faktorizovat na $2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 \cdot 7$.

**Příklad 7: Metoda pokusného dělení**

Pomocí metody pokusného dělení zjistěte faktory čísla 98 325.

**Řešení**: V prvním kroku se číslo 98 325 vydělí prvním prvočíslem, jelikož je zadané číslo liché, je zřejmé že, prvním prvočíslem, kterým je číslo 2 vydělit beze zbytku nepůjde. Proto číslo 98 325 vydělíme dalším prvočíslem což je číslo 3. Po vydělení vyjde celočíselný zbytek 32 775. Tento celočíselný zbytek lze opět dělit prvočíslem 3. Po druhém vydělení se dostane zbytek 10 925, který již nelze dále dělit číslem 3 beze zbytku. V dalším kroku zbytek 10 925 se vydělí následujícím prvočíslem, kterým je číslo 5. Po vydělení se získá zbytek 2 185, který lze vydělit ještě jednou prvočíslem 5. Po druhém vydělení se získá hodnota zbytku rovna číslu 437, která již není beze zbytku dělitelná číslem 5.

Jelikož číslo 437 není dělitelné beze zbytku následujícími prvočísly 7, 11, 13 a 17, musí se vydělit dalším prvočíslem 19. Po vydělení se získá zbytek číslo 23, které je samotné prvočíslem.

Číslo 98 325 lze faktorizovat na $3 \cdot 3 \cdot 5 \cdot 5 \cdot 19 \cdot 23$.

Použití metody pokusného dělení je výhodné pro menší čísla, protože u větších čísel je tato metoda zdlouhavá, tedy časově náročná. Například pro číslo 988 027, které má faktory 991 a 997 by bylo nutné projít všechny prvočísla nižší než 991, kterých je už pro tento případ 166.

## 3.2 POLYNOMICKÁ FAKTORIZACE

Polynomická faktorizace je založena na principu, kdy existuje polynom $P(x)$ stupně $n$, jehož faktorem je polynom $Q(x)$ menšího stupně než $n$, který je možné vynásobit polynomem $R(x)$ menšího stupně než $n$, tak aby vznikl polynom $P(x)$.

$$P(x) = Q(x) \cdot R(x)$$

Pro faktorizaci celých čísel lze upravit rovnici do základní podoby:

$$N = x^2 = x \cdot x$$

Ve specifických případech, pokud je číslo $N$ čtvercem, tak na základě rovnice vyplývá, že výslednými faktory čísla $N$ jsou hodnoty odmocniny $N$. Příkladem může být číslo $N = 36 \Rightarrow N = 6 \cdot 6$.

Pro čísla, která nejsou čtvercem, lze využít následující rovnici:

$$N = x^2 - 1 = (x + 1) \cdot (x - 1)$$

Tato rovnice lze využít v případě, kdy zadané číslo $N$ je menší o hodnotu 1 od čtverce. Tedy odmocnina výrazu $N + 1$ je celým číslem. Příkladem může být číslo $N = 143$.

$$x^2 = N + 1 = 143 + 1 = 144 \Rightarrow x = 12 \Rightarrow N = (12 + 1) \cdot (12 - 1) = 13 \cdot 11$$

Za předpokladu použití všeobecného vzorce, lze vytvořit metodu, která bude hledat, takové číslo $y$, aby vznikl čtverec čísla $x$.

$$A^2 - B^2 = (A - B) \cdot (A + B) \Rightarrow N = x^2 - y^2 = (x - y) \cdot (x + y)$$

V prvním kroku se zvolí $y = 1$ a zjišťuje se zda $x^2$ je čtvercovým číslem.

$$y = 1: N = x^2 - 1 \Rightarrow x^2 = N + 1 \Rightarrow x = \sqrt{N + 1}$$

Pokud bylo nalezeno čtvercové číslo, tak faktory čísla $N$ se stanoví:

$$x \equiv 0 \ (mod\ 1) \Rightarrow N = (x - y) \cdot (x + y)$$

Pokud čtvercové číslo nebylo nalezeno, provede se zvětšení hodnoty $y$ a postup se opakuje do té doby, než je nalezen čtverec nebo je dosažená stanovená mez. [17]

$$x \not\equiv 0\ (mod\ 1) \Rightarrow y\ zvětším\ o\ 1$$

**Příklad 8: Polynomická faktorizace**

Pomocí metody polynomické faktorizace určete faktory čísla $N = 475$.

**Řešení**: V prvním kroku se zvolí $y = 1$ a zjišťuje se zda $x^2$ je čtvercovým číslem.

$y = 1$: $N = x^2 - 1 \Rightarrow x^2 = N + 1 \Rightarrow x = \sqrt{N+1} = \sqrt{475+1} = \sqrt{476} \doteq 21{,}817$

Pro $y = 1$ není $x^2$ čtvercovým číslem, proto se pokračuje v postupu, kde se provede zvětšení $y$ o 1.

$y = 2$: $N = x^2 - 4 \Rightarrow x^2 = N + 4 \Rightarrow x = \sqrt{N+4} = \sqrt{475+4} = \sqrt{479} \doteq 21{,}886$

$x \not\equiv 0\ (mod\ 1) \Rightarrow y\ zvětší\ o\ 1$

$y = 3$: $N = x^2 - 9 \Rightarrow x^2 = N + 9 \Rightarrow x = \sqrt{N+9} = \sqrt{475+9} = \sqrt{484} = 22$

$x \equiv 0\ (mod\ 1) \Rightarrow N = (x-y)\cdot(x+y) = (22-3)\cdot(22+3) = 19 \cdot 25$

Pomocí polynomické faktorizace se určily faktory čísla $N = 475$, kterými jsou čísla 19 a 25.

## 3.3 FERMATOVA FAKTORIZAČNÍ METODA

Fermatova faktorizační metoda patří také mezi základní metody faktorizace, byla pojmenovaná po francouzském matematikovi Pierrovi de Fermatovi. Metoda pochází ze 17. století a je druhou nejstarší metodou pro faktorizaci daného celého čísla.

Principem metody je, že každé liché číslo $N$ se dá zapsat jako rozdíl dvou čtverců, a to třeba i několika způsoby. Pro vysvětlení budeme předpokládat čtverce $s^2$ a $t^2$ a budeme hledat faktory $a$ a $b$.

$$N = s^2 - t^2 = (s-t)\cdot(s+t) = a \cdot b \qquad (1)$$

Z předchozí rovnosti lze odvodit závislost faktorů $a$ a $b$ na odmocninách čtverců.

$$a = s - t\ ;\ b = s + t \qquad (2)$$

Po vyjádření a dosazení do rovnice (1) se dostane:

$$s = a + t \ \wedge \ s = b - t \Longrightarrow t = \frac{b-a}{2} \ \wedge \ s = \frac{b+a}{2}$$

$$N = s^2 - t^2 = \left(\frac{b+a}{2}\right)^2 - \left(\frac{b-a}{2}\right)^2$$

Na základě rovnice (1) lze určit triviální případ, kdy $a = 1$ tudíž $b = N$. A proto pro každé číslo $N$ lze nalézt i triviální rozklad:

$$N = \left(\frac{N+1}{2}\right)^2 - \left(\frac{N-1}{2}\right)^2$$

K nalezení ostatních čtverců je třeba využít metody Fermatovy faktorizace, s následujícím algoritmem:

1) Určí se hodnota čísla $s$, která se bude rovnat hodnotě celého čísla odmocniny čísla $N$ zvětšenou o hodnotu 1; $s = \lfloor\sqrt{N}\rfloor + 1$.
2) V dalším kroku se určí hodnota $t$, která se na základě rovnice (1) určí jako: $t = \sqrt{-N + s^2}$, pokud výraz $-N + s^2$ není roven druhé mocnině, provede se zvýšení hodnoty $s$; $s = s + 1$.
3) Postup se opakuje, dokud výraz $-N + s^2$ není roven druhé mocnině.
4) Po získání hodnot $s$ a $t$, se určí hodnoty $a, b$ na základě rovnice (2). [18]

**Příklad 9: Fermatova faktorizační metoda**

Pomocí Fermatovy faktorizační metody najděte faktory čísla $N = 27$.

**Řešení**: Příklad vypočteme pomocí algoritmu, který byl popsán o odstavec výše. Tedy nejdříve vypočteme hodnoty $s$ a $t$.

$s = \lfloor\sqrt{N}\rfloor + 1 = \lfloor\sqrt{27}\rfloor + 1 = 6$

$t = \sqrt{-N + s^2} = \sqrt{-27 + 6^2} = \sqrt{9} = 3$

Hned po prvním výpočtu jsme získali výraz $-N + s^2$ roven druhé mocnině. Můžeme tedy pokračovat ve výpočtu hodnot $a$ a $b$.

$a = s - t = 6 - 3 = 3$

$b = s + t = 6 + 3 = 9$

Výsledkem příkladu jsou faktory $a = 3; b = 9$.

Výpočet faktorů čísla 27 byl jednoduchý, jelikož v tomto případě nebylo nutné pro výpočet faktorů využít zvyšování hodnoty o jednu větší. Výsledek se získal ihned v prvním kroku Fermatovy faktorizační metody.

**Příklad 10: Fermatova faktorizační metoda**

Za pomoci Fermatovy faktorizační metody najděte faktory čísla $N = 799$.

**Řešení**: Příklad se vypočte pomocí stejného algoritmu jako v předchozím příkladě.

$s = \left[\sqrt{N}\right] + 1 = \left[\sqrt{799}\right] + 1 = 29$

$t = \sqrt{-N + s^2} = \sqrt{-799 + 29^2} = \sqrt{42} \doteq 6{,}48$

Zde se výraz $-N + s^2$ nerovná druhé mocnině, proto se musí hodnosta $s$ zvětšit o 1 a pokračovat tímto způsobem do té doby, dokud se nezíská výraz roven druhé mocnině.

$s \leftarrow s + 1 = 29 + 1 = 30$

$t = \sqrt{-N + s^2} = \sqrt{-799 + 30^2} = \sqrt{101} \doteq 10{,}05$

$s \leftarrow s + 1 = 30 + 1 = 31$

$t = \sqrt{-N + s^2} = \sqrt{-799 + 31^2} = \sqrt{162} \doteq 12{,}73$

$s \leftarrow s + 1 = 31 + 1 = 32$

$t = \sqrt{-N + s^2} = \sqrt{-799 + 32^2} = \sqrt{225} = 15$

Po třetím zvětšení se získal výsledek roven druhé mocnině, a proto se může pokračovat ve výpočtu hodnot $a$ a $b$.

$a = s - t = 32 - 15 = 17$

$b = s + t = 32 + 15 = 47$

Výsledkem příkladu jsou faktory $a = 17; b = 47$.

V tomto případě bylo třeba ve výpočtu faktorů čísla 799 použít postup, při kterém se zvětšuje hodnota $s$ o jednu větší, tím se stal výpočet delším a pracnějším.

**Příklad 11: Fermatova faktorizační metoda**

Pomocí Fermatovy faktorizační metody najděte faktory čísla $N = 1\,003$.

**Řešení**: Příklad se vypočítá pomocí stejného algoritmu jako u předchozích příkladů.

$s = \left[\sqrt{N}\right] + 1 = \left[\sqrt{1\,003}\right] + 1 = 32$

$t = \sqrt{-N + s^2} = \sqrt{-1\,003 + 32^2} = \sqrt{21} \doteq 4{,}58$

V tomto případě se výraz $-N + s^2$ nerovná druhé mocnině. Proto se musí hodnosta $s$ zvětšit o 1 a pokračovat tímto způsobem do té doby, dokud se nezíská výraz roven druhé mocnině.

$s \leftarrow s + 1 = 32 + 1 = 33$

$t = \sqrt{-N + s^2} = \sqrt{-1\,003 + 33^2} = \sqrt{86} \doteq 9{,}27$

$s \leftarrow s + 1 = 33 + 1 = 34$

$t = \sqrt{-N + s^2} = \sqrt{-1\,003 + 34^2} = 3\sqrt{17} \doteq 12{,}37$

$s \leftarrow s + 1 = 34 + 1 = 35$

$t = \sqrt{-N + s^2} = \sqrt{-1\,003 + 35^2} = \sqrt{222} \doteq 14{,}9$

$s \leftarrow s + 1 = 35 + 1 = 36$

$t = \sqrt{-N + s^2} = \sqrt{-1\,003 + 36^2} = \sqrt{293} \doteq 17{,}12$

$s \leftarrow s + 1 = 36 + 1 = 37$

$t = \sqrt{-N + s^2} = \sqrt{-1\,003 + 37^2} = \sqrt{366} \doteq 19{,}13$

$s \leftarrow s + 1 = 37 + 1 = 38$

$t = \sqrt{-N + s^2} = \sqrt{-1\,003 + 38^2} = \sqrt{441} = 21$

Po šestém zvětšení se získala hodnota druhé mocniny, a proto se může pokračovat ve výpočtu hodnot $a$ a $b$.

$a = s - t = 38 - 21 = 17$

$b = s + t = 38 + 21 = 59$

Výsledkem příkladu jsou faktory $a = 17; b = 59$.

Porovnáním předchozích výpočtů, se zjistilo, že tato metoda je pro každé číslo jinak časově náročná a pracná. Například u čísla 27 bylo zapotřebí jen jednoho kroku výpočtu pro zjištění faktorů, naopak u čísla 799 se muselo využít opakovaného přidávání hodnoty 1, aby byly získány jeho faktory. U čísla 1 003 se musela dokonce 6krát přičítat hodnota 1, aby byla získána druhá mocnina.

### 3.3.1 PIERRE DE FERMAT – ŽIVOTOPIS

Pierre de Fermat byl francouzský právník a vládní úředník, který měl záliby v matematice. Narodil se 17. srpna 1601 v Beaumont de Lomagne a zemřel 12. ledna 1665 v Castres ve Francii. Spolu s Descartem byl považován za jednoho předního matematika první poloviny 17. století.

**Fermatova rodina**

Otec Pierra Fermata byl bohatým obchodníkem s kůží a druhým konzulem Beaumont-Lomange. Jeho matka byla Claire de Long. Pierre měl bratra a dvě sestry. Byl vychováván ve městě jeho narození, tedy v Beaumont de Lomange, kde chodil do školy.

**Studia a vzdělání**

Fermat navštěvoval univerzitu v Toulouse. V druhé polovině roku 1620 se přestěhoval do Bordeaux. Zde zahájil své první seriózní matematické výzkumy. Setkal se zde s Beaugrandem, francouzským matematikem, který publikoval práce o geostatice a matematice. V této době vytvořil práci pojednávající o maximech a minimech.

Obrázek 1- Pierre de Fermat (zdroj: Wikimedia)

Z Bordeaux Fermat odešel do Orléans, kde studoval právo na univerzitě. Titul získal v oboru občanského práva. V roce 1631 se Fermat stal právníkem a vládním úředníkem v Toulouse. Kvůli úřadu, který zde zastával, měl právo změnit své jméno z Pierra Fermata na Pierra de Fermata. Téhož roku se oženil s Louise de Longovou, čtvrtou sestřenicí své matky. Spolu měli osm dětí, z nichž se pět dožilo dospělého věku.

Po zbytek svého života žil v Toulouse, ale také pracoval v jeho rodném městě Beaumont de Lomange a v nedalekém městě Castres. Od svého jmenování v roce 1631 Fermat pracoval v dolní komoře parlamentu, o sedm let později byl jmenován do vyšší komory, poté byl v roce 1652 povýšen na nejvyšší úroveň u trestního soudu. Jeho postup v kariéře byl ovlivněn nejen jeho výsledky, ale i výskytem moru, který zasáhl oblast v 50. letech 17. století (velmi mnoho starších mužů v tento čas zemřelo). Během morové epidemie byl Fermat vyhlášen za mrtvého.

Fermat se samozřejmě pořád během života zabýval matematikou. Po přestěhování do Toulouse si udržel matematické přátelství s Beaugrandem, také získal nového matematického přítele Pierra de Carcavi, se kterým se podílel o lásku k matematice. V roce 1636 navázal Carcavi v Paříži kontakt s Mersennem a dalšími vědci. Carcaviho popis Fermatových objevů vzbudil natolik Mersennův zájem, že Fermatovi napsal dopis. Fermat na něj odpověděl a kromě toho, že řekl Mersennemu o chybách, které Galileo udělal ve svém popisu volného pádu, také se zmínil Mersennemu o jeho práci na spirálách a jeho navrácení Apolloniusových rovinných lokusů.

V období od 1643 do 1654 byl Fermat v kontaktu se svými vědeckými kolegy v Paříži. Práci mu komplikovali úřední povinnosti, také se konala občanská válka ve Francii, kterou byla Toulouse velmi zasažena. Během této doby Fermat pracoval na teorii čísel.

Fermat významně přispěl k rozvoji matematiky, v oblastech analytické geometrie, pravděpodobnosti, teorii čísel a matematické analýzy. Během života se zabýval i problémy ve fyzice zejména v optice, kde se zaobíral zákony lomu a odrazu světla. Jeho matematické práce byly vydány tiskem až po jeho smrti v roce 1679. [19]

## 3.4 EULEROVA FAKTORIZAČNÍ METODA

Tato metoda faktorizace je pojmenována po švýcarském matematikovi a fyzikovi Leonhardu Paulu Eulerovi. Eulerova faktorizační metoda je postup pro hledání faktoru daného přirozeného čísla $N$, které se dá zapsat jako součet čtverců, a to dvěma různými způsoby. Například číslo $N = 500$ lze rozepsat jako součet dvou čtverců dvojic čísel 22 a 4 nebo čísel 20 a 10. Číslo 500 je zde uvedeno jako příklad, jelikož je sudé, lze najít jednoduší metodu pro získání jeho faktorů.

Eulerova faktorizace je založená na předpokladu, že $N = a^2 + b^2 = c^2 + d^2$, tato rovnici se může upravit do podoby: $a^2 - c^2 = d^2 - b^2$. Další možnou úpravou se získá rovnice ve tvaru:

$$(a - c) \cdot (a + c) = (d - b) \cdot (d + b) \qquad (3)$$

Pokud platí že $k$ se rovná NSD výrazů $(a - c)$ a $(d - b)$ a $n$ se rovná NSD výrazů $(a + c)$ a $(d + b)$, tak musejí existovat konstanty $l, m$ a $p, q$:

$(a - c) = kl$

$(d - b) = km$

$NSD(l, m) = 1$; pokud by čísla $l, m$ byla dělitelná libovolným číslem jiným od 1, znamenalo by to, že $k$ není NSD pro výrazy $(a - c)$ a $(d - b)$.

$(a + c) = nq$

$(d + b) = np$

$NSD(q, p) = 1$

Pokud se dosadí do (3) rovnice dostane se $klnq = kmnp$. Po úpravě rovnice se získá $lq = mp$. Z této rovnice lze určit, že $l = p$ a $m = q$, protože čísla $l$ a $m$ jsou nesoudělná.

Nyní se tedy dostanou rovnice:

$(a - c) = kl$

$(d - b) = km$

$(a + c) = nm$

$(d + b) = nl$

Na základě získaných rovností lze vyjádřit $2a = (a - c) + (a + c) = kl + nm$ a $2b = (d + b) - (d - b) = nl - km$. Po dosazení do rovnice $N = a^2 + b^2 = c^2 + d^2$ lze vyjádřit hodnotu čísla $N$ jako:

$$N = a^2 + b^2 = \left(\frac{kl + nm}{2}\right)^2 + \left(\frac{nl - km}{2}\right)^2 = \frac{1}{4} \cdot [(k^2 + n^2) \cdot (l^2 + m^2)]$$

Z vyjádřených rovnice lze pomocí Eulerovy faktorizační metody získat faktory libovolného přirozeného čísla $N$, pro které jsou známé dvě možnosti součtu čtverců. Princip metody lze dokázat na následujících příkladech.

**Příklad 12: Eulerova faktorizační metoda**

Pomocí Eulerovy faktorizační metody určete faktory pro číslo $N = 793$.

**Řešení**: Číslo 793 lze rozepsat jako součet dvou čtverců dvojic čísel 27 a 8 nebo čísel 28 a 3. Tímto rozkladem se získají hodnoty $a, b, c$ a $d$.

$N = 793 = 28^2 + 3^2 = 27^2 + 8^2$

$a = 28; b = 3; c = 27; d = 8$

Nyní se dosadí tyto čtyři hodnoty do získaných rovnic.

$a - c = 28 - 27 = 1$

$a + c = 28 + 27 = 55$

$d - b = 8 - 3 = 5$

$d + b = 8 + 3 = 11$

Poté se vypočtou největší společní dělitelé.

$k = NSD(a - c; d - b) = NSD(1; 5) = 1$

$l = NSD(a - c; d + b) = NSD(1; 11) = 1$

$m = NSD(a + c; d - b) = NSD(55; 5) = 5$

$NSD(l, m) = 1$

$n = NSD(a + c; d + b) = NSD(55; 11) = 11$

Nyní jsou vypočteny všechny potřebné neznámé, které se dosadí do rovnice $N = \frac{1}{4} \cdot (k^2 + n^2) \cdot (l^2 + m^2)$ a získají se tím faktory čísla $N$.

$$N = \frac{1}{4} \cdot (k^2 + n^2) \cdot (l^2 + m^2) = \frac{1}{4} \cdot (1^2 + 11^2) \cdot (1^2 + 5^2) = 793$$

Číslo 793 lze faktorizovat na součin $\frac{1}{4} \cdot (1^2 + 11^2) \cdot (1^2 + 5^2) = \frac{1}{4} \cdot 122 \cdot 26$, ze kterého se získájí faktory 61 a 13.

**Příklad 13: Eulerova faktorizační metoda**

Pomocí Eulerovy faktorizační metody určete faktory pro číslo $N = 71\,721$.

**Řešení**: Číslo 71 721 lze rozepsat jako součet dvou čtverců dvojic čísel 264 a 45 nebo čísel 261 a 60. Tímto rozkladem se získají hodnoty $a, b, c$ a $d$.

$$N = 71\,721 = 264^2 + 45^2 = 261^2 + 60^2$$

$$a = 264; b = 45; c = 261; d = 60$$

Opět se tyto hodnoty dosadí do získaných rovnic.

$$a - c = 264 - 261 = 3$$

$$a + c = 264 + 261 = 525$$

$$d - b = 60 - 45 = 15$$

$$d + b = 60 + 45 = 105$$

Dále se vypočítají největší společní dělitelé.

$$k = NSD(a - c; d - b) = NSD(3; 15) = 3$$

$$l = NSD(a - c; d + b) = NSD(3; 105) = 3$$

$$m = NSD(a + c; d - b) = NSD(525; 15) = 15$$

$$NSD(l, m) = 1 \Longrightarrow l = 1; m = 5$$

$$n = NSD(a + c; d + b) = NSD(525; 105) = 105$$

Nyní jsou vypočteny všechny potřebné neznámé, které se dosadí do rovnice $N = \frac{1}{4} \cdot (k^2 + n^2) \cdot (l^2 + m^2)$ a získají se faktory čísla $N$.

$$N = \frac{1}{4} \cdot (k^2 + n^2) \cdot (l^2 + m^2) = \frac{1}{4} \cdot (3^2 + 105^2) \cdot (1^2 + 5^2) = 71\,721$$

Číslo 71 721 lze faktorizovat na součin $\frac{1}{4} \cdot (3^2 + 105^2) \cdot (1^2 + 5^2) = \frac{1}{4} \cdot 11\,034 \cdot 26$, ze kterého se získají faktory 5 517 a 13.

**Příklad 14: Eulerova faktorizační metoda**

Pomocí Eulerovy faktorizační metody určete faktory pro číslo $N = 1\,000\,009$.

**Řešení**: Číslo 1 000 009 lze rozepsat jako součet dvou čtverců dvojic čísel 1000 a 3 nebo čísel 972 a 235. Tímto rozkladem se získají hodnoty $a, b, c$ a $d$.

$N = 1\,000\,009 = 1000^2 + 3^2 = 972^2 + 235^2$

$a = 1000; b = 3; c = 972; d = 235$

Opět se tyto hodnoty dosadí do získaných rovnic.

$a - c = 1\,000 - 972 = 28$

$a + c = 1\,000 + 972 = 1\,972$

$d - b = 235 - 3 = 232$

$d + b = 235 + 3 = 238$

Znovu se vypočítají největší společní dělitelé.

$k = NSD(a - c; d - b) = NSD(28; 232) = 4$

$l = NSD(a - c; d + b) = NSD(28; 238) = 14$

$m = NSD(a + c; d - b) = NSD(1\,972; 232) = 116$

$NSD(l, m) = 1 \Longrightarrow l = 7; m = 58$

$n = NSD(a + c; d + b) = NSD(1\,972; 238) = 34$

Nyní jsou vypočteny všechny potřebné neznámé, které se dosadí do rovnice $N = \frac{1}{4} \cdot (k^2 + n^2) \cdot (l^2 + m^2)$ a získají se faktory čísla $N$.

$N = \frac{1}{4} \cdot (k^2 + n^2) \cdot (l^2 + m^2) = \frac{1}{4} \cdot (4^2 + 34^2) \cdot (7^2 + 58^2) = 1\,000\,009$

Číslo 1 000 009 lze faktorizovat na součin $\frac{1}{4} \cdot (4^2 + 34^2) \cdot (7^2 + 58^2)$, ze kterého se získají faktory 293 a 3 413.

### 3.4.1 LEONHARD EULER – ŽIVOTOPIS

Leonhard Euler byl průkopnický švýcarský matematik a fyzik. Je považován za nejlepšího matematika 18. století a za jednoho z nejlepších matematiků vůbec. Narodil se 15. dubna 1707 v Basileji ve Švýcarsku a zemřel 18. září 1783 v Petrohradě.

**Eulerova rodina**

Otcem Leonarda Eulera byl Paul Euler, který vystudoval teologii na Basilejské univerzitě, kde se zúčastnil matematických přednášek Jacoba Bernoulliho. Během života se Paul Euler stal protestanským pastorem a oženil se s Margaretou Bruckerovou, matkou Leonarda Eulera. Když byl Leonhardu jeden rok, rodina se přestěhovala do Riehenu, kde byl vychováván babičkou.

**Studia a matematické vzdělání**

Ve škole v Basileji se Leonhard o matematice mnoho nedověděl. Jelikož Paul Euler, jeho otec, měl jakési matematické vzdělání, mohl tedy sám vyučovat svého syna v elementární matematice. Otcův výklad vzbudil natolik Eulerův zájem o matematiku, že začal sám číst matematické texty a hledat cesty k dalšímu vzdělání. Eulerův otec si přál, aby ho syn následoval a stal se pastorem jako on. Proto v roce 1720 Leonhard Euler začal studovat, jako 14letý, na universitě v Basileji. Nejprve aby získal všeobecné vzdělání a pak mohl nastoupit na teologickou fakultu. Otcův přítel, Johann Bernoulli, při soukromých lekcích, které navrhl samotný Leonardo, brzy zjistil, že Euler má obrovské matematické nadání. Sám Euler to popsal takto:

*"…Brzy jsem našel příležitost být představen slavnému profesoru Johanu Bernoulliovi … pravda, měl málo času, a tak hned odmítal dávat mi soukromé hodiny. Ale dal mi mnohem cennější radu, abych začal sám studovat obtížnější matematické knihy, a to tak pilně, jak to jen půjde. A kdybych narazil na nějakou obtíž nebo překážku, že za ním mohu každé nedělní odpoledne přijít, a on mi vysvětlí, co jsem nepochopil..." [20]*

V roce 1723 dokončil magisterské studium a na podzim téhož roku podle přání svého otce začal studium na teologické fakultě. Bohužel nemohl najít takové nadšení pro studium teologie, řečtiny a hebrejštiny jaké našel ve studiu matematiky. Po přímluvách Johanna Bernoulliho, který byl přítelem Paula Eulera, otec nakonec souhlasil, aby se Leonhard zaměřil na matematiku. Své studium na universitě ukončil v roce 1726, během studia prostudoval mnoho matematických prací. Téhož roku byla otištěna jeho

první krátká práce pojednávající o izochronních křivkách v odporujícím médiu. O rok později, tedy kdy mu bylo 20 let, publikoval další práci o vzájemných trajektoriích. Také zaslal do soutěže o Velkou cenu pařížské akademii soutěžní příspěvek, na téma: nejlepší umístění stožárů na plachetnici, za který získal 2. místo.

Obrázek 2 - Leonhard Euler (zdroj: Mendeleu)

**Práce na akademii v Petrohradě**

V roce 1726, po smrti Nicolause Bernoulliho, bylo Eulerovi nabídnuto místo vyučujícího matematiky a mechaniky ve fyziologii. Euler tuto pozici přijal s tím, že do Ruska pojede až na jaře příštího roku. Potřeboval čas na studium témat týkajících se jeho nového postu a jednak měl naději, že na universitě v Basileji získá místo po nedávno zemřelém profesoru fyziky. V konečném rozhodnutí, však nebyl přijat na katedru fyziky. Jakmile se Euler dověděl tuto negativní zprávu, odjel z Basileje.

Roku 1727 přijel do Petrohradu, kde nastoupil do Petrohradské akademie věd, založenou o dva roky dříve Kateřinou I. (manželka Petra Velikého). Na základě žádostí Daniela Bernouliho a Jakoba Hermanna byl Euler jmenován do matematicko-fyzikální sekce akademie místo do fyziologického postu, který mu byl původně nabídnut. V Petrohradě měl Euler mnoho kolegů, skupinu eminentních vědců, kteří vytvářeli výjimečně příznivé badatelské prostředí v oblasti analýzy a geometrie. Do skupiny patřili jeho příbuzní Jakob Hermann a Daniel Bernoulli, dále mnohostranný učenec Christian Goldbach, s nímž Euler diskutoval o mnoha problémech analýzy, teorii čísel a další významní vědci. [20]

V letech 1727 až 1730 sloužil Euler jako lékařský poručník v ruském námořnictvu. V roce 1730 se stal na akademii profesorem fyziky, což mu umožnilo stát se řádným členem akademie a opustit tak ruské námořnictvo. Poté co Daniel Bernoulli opustil

Petrohrad a vrátil se zpět do Basileje, bylo Eulerovi přiděleno jeho místo na akademii. Finanční vylepšení, které vyplynulo z tohoto jmenování umožnilo Eulerovi se oženit. Jeho ženou se stala Katharina Gsell, dcera malíře ze švýcarské rodiny. Měli celkem 13 dětí, i když pouze pět z nich přežilo své dětství.

Euler sepsal knihu Mechanica, ve které podrobně popisuje Newtonovu dynamiku ve formě matematické analýzy. Po publikaci této knihy a mnoha dalších článků se mu otevřela cesta k práci na větších matematických dílech.

Eulerovy zdravotní problémy začaly v roce 1735, kdy měl těžkou horečku a téměř přišel o život. Ve svých autobiografických spisech Euler tvrdí, že jeho problémy se zrakem začaly v roce 1738 přetížením kvůli kartografické práci. Nejdříve přišel o zrak v pravém oku, později osleplo i levé oko ze šedého zákalu.

**Přestěhování do Berlína**

Euler měl velmi vysokou reputaci již ve 33 letech. V roce 1738 a 1740 získal Velkou cenu pařížské akademie. Vynikající pověst mu přinesla nabídku do Berlína. Euler nejdříve dával přednost pobytu v Petrohradě, pozdější politické nepokoje v Rusku však ztížily postavení cizinců a přispěly k tomu, aby Euler změnil svůj názor. Poté přijal nabídku od Fridricha Velikého, odjel do Berlína, kde měla být Společnost věd nahrazena Akademií věd. Prezidentem berlínské akademie byl po jejím založení v roce 1744 Pierre Louis Maupertuis. Euler se stal ředitelem matematické sekce a zastupoval Maupertuise v době jeho nepřítomnosti na akademii. Oba se stali velkými přáteli. V této době měl Euler mnoho povinností. Působil ve výboru akademie zabývajícím se knihovnou a vědeckými publikacemi, také působil jako poradce vlády pro státní loterie, pojištění atd. Jeho vědecký výstup v tomto období byl fenomenální.

Během dvaceti pěti let strávených v Berlíně napsal Euler kolem 380 článků. Psal knihy o variačním počtu; o výpočtu planetárních drah; o dělostřelectvu a balistice; o stavbě a navigaci lodí; přednášky o diferenciálním počtu atd. Také napsal populární vědeckou publikaci: Dopisy německé princezně, které vyšly ve třech svazcích. V roce 1759 Maupertuis zemřel a Euler převzal vedení berlínské akademie. Dřívější přátelství a dobré vztahy s králem Fridrichem vystřídala nepřízeň, díky které Euler nebyl jmenován předsedou akademie. Tato pozice byla v roce 1763 nabídnuta d'Alembertovi, se kterým Euler v některých vědeckých otázkách nesouhlasil, D'Alembert místo na

akademii nepřijal. Neustálé zasahování Fridricha do činnosti akademie nakonec Eulera donutilo k jejímu úplnému opuštění. [20]

**Návrat do Petrohradu**

V roce 1766 se Euler vrátil do Petrohradu, brzy po návratu do Ruska Euler onemocněl a stal se téměř úplně slepým. V roce 1771 byl jeho dům zničen ohněm, Euler byl schopný zachránit jen svůj život a jeho matematické rukopisy. V tom samém roce byl Euler operován na šedý zákal. Jeho zrak se mu na krátkou dobu vrátil, zanedbáním nutné ochrany a nešetřením zraku, ale oslepl definitivně. Díky jeho pozoruhodné paměti byl schopný pokračovat ve své vědecké práci. Je fascinující, že po svém návratu do Petrohradu (59 let) navzdory úplné ztrátě zraku napsal téměř polovinu z celkového počtu svých vědeckých prací. Samozřejmě, že Euler nemohl vytvořit tolik prací bez cizí pomoci. Pomáhali mu jeho synové, Johann Albrecht Euler a Christoph Euler, dva členové akademie, W. L. Krafft a A. J. Lexell, a mladý matematik N. Fuss. Po Eulerově smrti Petrohradská akademie začala vydávat Eulerovy nepublikované písemnosti, pokračovala s tím dalších 50 let.

Euler byl asi nejplodnějším matematikem všech dob. Napsal kolem 880 článků, desítky knih a tisíce vědeckých sdělení ve formě dopisů. Posunul hranice analytické geometrie a trigonometrie, kde jako první uvažoval o sinu, kosinu atd. jako o funkcích. Položil základy analytické mechaniky. Všichni vědci si Eulera vážili a jeho díla byla inspirací pro celé generace matematiků. [20]

# 4 MODERNÍ FAKTORIZAČNÍ METODY

Moderní faktorizační algoritmy jsou oproti klasickým faktorizačním metodám v principu složitější. Narozdíl od metod, které jsou vedeny v předchozí kapitole, nejsou u těchto metod určeny podmínky na podobu faktorizovaného čísla.

## 4.1 POLLARDOVA METODA P-1

Jednou z moderních faktorizačních metod je Pollardova p-1 metoda, kterou uvedl britský matematik John Pollard v roce 1974. Metoda slouží k rozložení složených čísel na jejich prvočíselný rozklad. Algoritmus vytvořený na základě této metody je vhodný především pro čísla, jejichž faktor bez jedné je hladké nebo téměř hladké číslo. O celkové složitosti metody nerozhoduje velikost faktorizovaného čísla $N$, ale hladkost jeho faktoru. Číslo je možné označit jako B-hladké, pokud žádný z jeho prvočíselných dělitelů není vetší než $B$. Například číslo 10 500 má prvočíselný rozklad $2^2 \cdot 3^1 \cdot 5^3 \cdot 7^1$, je tedy 7-hladké, jelikož žádný z jeho prvočíselných dělitelů není větší než 7.

Podstatou algoritmu je princip vycházející z Malé Fermatovy věty, tedy že pro libovolné prvočíslo $p$ a libovolné s ním nesoudělné číslo $a$ platí, že výraz $a^p - a$ je dělitelný prvočíslem $p$.

$$a^p \equiv a \; mod \; p$$

Pokud zároveň $a$ a $p$ jsou čísla nesoudělná, tak lze výraz upravit na tvar:

$$a^{p-1} \equiv 1 \; mod \; p, tedy \; a^{p-1} - 1 \equiv 0 \; mod \; p$$

Výraz $(a^{p-1} - 1)$ je stejně jako číslo $N$ dělitelné p. Možným způsobem, jak jej nalézt je určení největšího společného dělitele výrazu $(a^{p-1} - 1)$ a $N$. Protože p je neznámé a zkoušet, že pro náhodné p platí $NSD(a^{p-1} - 1; N) > 1$ by bylo časově náročné, je nutné nalézt takové číslo, které ověří více hodnot najednou.

Protože předešlý výraz je pravdivý i pokud číslo $a$ umocníme libovolným $k$ násobkem výrazu $p - 1$, je možné na základě tohoto tvrzení zapsat výraz jako:

$$a^{k(p-1)} \equiv 1 \; mod \; p$$

Neboť platí tvrzení, že je výraz pravdivý pro jakékoliv $k \neq 0$, je možné tento princip použít v kombinaci s Malou Fermatovou větou, kdy je možné nalézt takové číslo $M$, pro které bude platit $(p-1)|M$, tedy číslo $M$ je dělitelné výrazem $p - 1$. V ideálním případě

takové číslo $M$, které bude součinem možných prvočísel a jejich mocnin. Pro pokrytí co největšího počtu prvočísel se určí hranice, do které budou vyhledána všechna prvočísla a jejich mocniny. Dále se hledá nejmenší společný násobek všech prvočísel i jejich mocnin, takových, že ${p_i}^{e_i} \leq B$, kde $e_i \geq 1$. Po provedení těchto operací bude číslo $M$ zcela jistě B-hladké a zároveň pro každé prvočíslo $p_i$ bude platit $(p_i - 1)|M$. Zvyšováním hranice $B$ se zvyšuje i šance pro nalezení netriviálního dělitele čísla $N$. [10]

Tato metoda může selhat v případě, že hranice $B$ je zvolena nízká, tedy že $NSD(a^M - 1; N) = 1$. Nalezená prvočísla a jejich mocniny nemohou dělit číslo $N$ beze zbytku. Je možné hranici zvýšit, ale s každým zvýšením roste i složitost metody. Teoreticky je možné využít Pollardovu p-1 metodu s hranicí $B = \sqrt{N}$, ale z důvodu složitosti se používá pouze jako zkusmá rychlá metoda pro nízkou hranici, jinak se přechází na jinou metodu. Pollardova metoda může selhat také v případě, že výrazy $a^M - 1$ lze beze zbytku dělit číslem $N$, tedy $NSD(a^M - 1; N) = N$. [21], [24]

**Příklad 15: Pollardova p-1 faktorizační metoda**

Pomocí algoritmu Pollardovy metody proveďte faktorizaci čísla $N = 357$.

**Řešení**: V prvním kroku se zvolí libovolná mez neboli číslo $B$.

$B = 3$

Pro tuto mez byla vyhledána všechna prvočísla a jejich mocniny.

$M = 2^1 \cdot 3^1 = 6$

Dále se zvolí libovolné celé číslo $a$.

$a = 2$

Vypočte se největší společný dělitel výrazu $a^M - 1$ a $N$, čímž se získá jeden z faktorů čísla $N$.

$q = NSD(a^M - 1; N) = NSD(2^6 - 1; 357) = NSD(63; 357) = 21$

Druhý faktor se získá vydělením zadaného čísla $N$ získaným faktorem $q$.

$p = \frac{357}{21} = 17$

$N = p \cdot q = 17 \cdot 21$

Použitím algoritmu Pollardovy p-1 metody byly získány faktory 17 a 21.

**Příklad 16: Pollardova p-1 faktorizační metoda**

Pomocí algoritmu Pollardovy metody proveďte faktorizaci čísla $N = 5\,001$.

**Řešení**: V prvním kroku se zvolí libovolná mez neboli číslo $B$.

$B = 3$

Pro tuto mez byla vyhledána všechna prvočísla a jejich mocniny.

$M = 2^1 \cdot 3^1 = 6$

Dále se zvolí libovolné celé číslo $a$.

$a = 2$

Vypočte se největší společný dělitel výrazu $a^M - 1$ a $N$, čímž se získá jeden z faktorů čísla $N$.

$q = NSD(a^M - 1; N) = NSD(2^6 - 1; 5\,001) = NSD(63; 5\,001) = 3$

Druhý faktor se získá vydělením zadaného čísla $N$ získaným faktorem $q$.

$p = \frac{5\,001}{3} = 1\,667$

$N = p \cdot q = 1\,667 \cdot 3$

Použitím algoritmu Pollardovy p-1 metody byly získány faktory 1 667 a 3.

## 4.2 METODA KVADRATICKÉHO SÍTA

Algoritmus metody kvadratického síta je v praxi druhá nejrychlejší metoda faktorizace. Je stále nejrychlejší metodou pro čísla do stého řádu. Obtížnost této metody závisí na velikosti faktorizovaného čísla více než na struktuře čísla a jeho vlastnostech. Tato metoda byla objevena Carlem Pomerancem v roce 1981, jako vylepšení Schroepplova lineárního síta.

Algoritmus vychází ze vzorce $N = x^2 - y^2$, tedy hledají se dvě taková čísla, pro něž platí, že rozdíl jejich druhých mocnin se rovná zadanému číslu $N$. Faktory čísla $N$ se stanoví na základě vzorce:

$$N = (x + y) \cdot (x - y);\ x \neq \pm y$$

V rámci metody se hledá takový čtverec $x^2$, aby existoval čtverec druhý $y^2$, který je z výchozí rovnice stanoven jako: $y^2 = x^2 - N$. Hodnotu většího čtverce $x^2$ je možné

stanovit jako $\left(\lfloor\sqrt{N}\rfloor + k\right)^2$, kde se bude hledat takové $k$, aby platila výše zmíněná rovnice, $k = 1; 2; 3 \dots n$. Je možné stanovit hranici B, ve které se bude hledat $k \leq B$. [22], [24]

$$y^2 = \left(\lfloor\sqrt{N}\rfloor + k\right)^2 - N$$

$$x^2 \equiv y^2 (mod\ N) \Rightarrow \left(\lfloor\sqrt{N}\rfloor + k\right)^2 = y^2\ (mod\ N)$$

**Příklad 17: Metoda kvadratického síta**

Pomocí metody kvadratického síta proveďte faktorizaci čísla $N = 481$.

**Řešení**: V prvním kroku se vypočítá odmocnina čísla N, které se zaokrouhlí na celé číslo.

$\sqrt{N} \doteq 21{,}932 \Rightarrow \lfloor\sqrt{N}\rfloor = 21$

Dále se dosadí do vzorce $y^2 = \left(\lfloor\sqrt{N}\rfloor + k\right)^2 - N$, stanoví se koeficient $k = 1$ a hledá se čtverec $y^2$.

$y^2 = (21 + 1)^2 - 481 = 3;\ \sqrt{3} \not\equiv 0\ (mod\ 1)$

Pokud po odmocnění získaného čtverce $y^2$ se $y$ rovná celému číslu je nalezen jeden z faktorů čísla $N$. Pro tento případ, kdy $k = 1$ není odmocnina čísla 3 celočíselným číslem ($\sqrt{3} \doteq 1{,}732$) a proto se musí pokračovat v dalším kroku, kde $k = 2$.

$y^2 = (21 + 2)^2 - 481 = 48;\ \sqrt{48} \not\equiv 0\ (mod\ 1)$

Opět se získá výsledek, který po odmocnění není celým číslem. Z tohoto důvodu se pokračuje ve stejném postupu, dokud se nezíská celočíselná odmocnina.

$k = 3$: $y^2 = (21 + 3)^2 - 481 = 95;\ \sqrt{95} \not\equiv 0\ (mod\ 1)$

$k = 4$: $y^2 = (21 + 4)^2 - 481 = 144;\ \sqrt{144} \equiv 0\ (mod\ 1)$

Číslo 144 lze odmocnit beze zbytku ($\sqrt{144} = 12$) .

Po dosazení do rovnice $N = (x + y) \cdot (x - y) = (25 + 12) \cdot (25 - 12)$ se získají faktory čísla $N$, kterými jsou čísla 37 a 13.

**Příklad 18: Metoda kvadratického síta**

Pomocí metody kvadratického síta proveďte faktorizaci čísla $N = 2\,673$.

**Řešení**: V prvním kroku se opět vypočítá odmocnina čísla N, které se zaokrouhlí na celé číslo.

$\sqrt{N} \doteq 51{,}701 \Rightarrow \lfloor \sqrt{N} \rfloor = 51$

V druhém kroku se dosadí do vzorce $y^2 = \left(\lfloor \sqrt{N} \rfloor + k\right)^2 - N$, stanoví se koeficient $k = 1$ a hledá se čtverec $y^2$.

$y^2 = (51+1)^2 - 2\,673 = 31;\ \sqrt{31} \not\equiv 0\ (mod\ 1)$

Pokud po odmocnění získaného čtverce $y^2$ se $y$ rovná celému číslu je nalezen jeden z faktorů čísla $N$. Pro tento případ, kdy $k = 1$ není odmocnina čísla 31 celočíselným číslem ($\sqrt{31} \doteq 5{,}568$) a proto se musí pokračovat v dalším kroku, kde $k = 2$.

$y^2 = (51+2)^2 - 2\,673 = 136;\ \sqrt{136} \not\equiv 0\ (mod\ 1)$

Opět se získá výsledek, který po odmocnění není celým číslem ($\sqrt{136} \doteq 11{,}662$), a proto se pokračuje ve stejném postupu, dokud se nezíská celočíselná odmocnina.

$k = 3: y^2 = (51+3)^2 - 2\,673 = 243;\ \sqrt{243} \not\equiv 0\ (mod\ 1)$

$k = 4: y^2 = (51+4)^2 - 2\,673 = 352;\ \sqrt{352} \not\equiv 0\ (mod\ 1)$

$k = 5: y^2 = (51+5)^2 - 2\,673 = 463;\ \sqrt{463} \not\equiv 0\ (mod\ 1)$

$k = 6: y^2 = (51+6)^2 - 2\,673 = 576;\ \sqrt{576} \equiv 0\ (mod\ 1)$

Číslo 576 lze odmocnit beze zbytku ($\sqrt{576} = 24$). Nyní se dá dosadit do rovnice pro získání faktorů čísla $N$.

Po dosazení do rovnice $N = (x+y)\cdot(x-y) = (57+24)\cdot(57-24)$ se získají faktory čísla $N$, kterými jsou čísla 81 a 33.

## 4.3 SHANKSOVA ČTVERCOVÁ FAKTORIZAČNÍ METODA (SQUFOF)

Jedná se o moderní faktorizační metodu představenou Danielem Shanksem v roce 1975. Originálním názvem Shanks´s method Square Forms Factorization do češtiny přeloženo jako Shanksova faktorizační metoda čtvercových rozkladů. Vychází z Fermatovy faktorizační metody s využitím binární kvadratické formy, tyto formy se využívají v řadě moderních metod faktorizace.

$$q(x, y) = ax^2 + bxy + cy^2$$

Jako základní myšlenku tato metoda používá vztah:

$$N = x^2 - y^2$$

Upravený na tvar:

$$x^2 \equiv y^2 (mod\ N)$$

Od Fermatovy faktorizační metody se liší postupem získání čísel $x$ a $y$. Číslo $N$ je základním vstupem do Shankseova algoritmu, existují rozšířené verze, které počítají i s malými koeficientem $k$. Číslo $N$, které chceme faktorizovat nesmí pro tento algoritmus být prvočíslem ani druhou mocninou celého čísla. Pro hledání faktorů je potřeba nejprve určit několik proměnných.

$$P_0 = \lfloor \sqrt{N} \rfloor \tag{4}$$

$$Q_0 = 1 \tag{5}$$

$$Q_1 = N - P_0^2 \tag{6}$$

Pro další kroky se opakují následující vztahy:

$$b_i = \left\lfloor \frac{\lfloor \sqrt{N} \rfloor + P_{i-1}}{Q_i} \right\rfloor \tag{7}$$

$$P_i = b_i \cdot Q_i - P_{i-1} \tag{8}$$

$$Q_{i+1} = Q_{i-1} + b_i \cdot (P_{i-1} - P_i) \tag{9}$$

Postup se opakuje do té doby, dokud není dosaženo čtvercového čísla $Q_i$. Následně se opět určí základní hodnoty proměnných $b_0, P_0, Q_0$ a $Q_1$ na základě získaného indexu $i$.

$$b_0 = \left\lfloor \frac{\lfloor \sqrt{N} \rfloor - P_{i-1}}{\sqrt{Q_i}} \right\rfloor \tag{10}$$

$$P_0 = b_0 \sqrt{Q_i} + P_{i-1} \tag{11}$$

$$Q_0 = \sqrt{Q_i} \tag{12}$$

$$Q_1 = \frac{N - P_0^2}{Q_0} \tag{13}$$

Poté výpočet pokračuje opětovným dosazováním do rovnic (7), (8) a (9), do té doby, než je nalezeno takové $P_i = P_{i-1}$. Faktor čísla $N$ se poté nalezne jako největší společný dělitel čísel $P_i$ a $N$. [23]

$$N = p \cdot q \ \wedge p = NSD(P_i, N)$$

**Příklad 19: Shanksova čtvercová faktorizační metoda**

Pomocí Shanksovy metody proveďte faktorizaci čísla $N = 3\,021$.

**Řešení**: V prvním kroku se vypočítá odmocnina čísla N, které se zaokrouhlí na celé číslo. Hodnota $Q_0$ je rovna 1.

$P_0 = \lfloor \sqrt{N} \rfloor = \lfloor \sqrt{3\,021} \rfloor = 54$

$Q_0 = 1$

Z následujícího stavu se určí hodnota pro $Q_1$.

$Q_1 = N - P_0^2 = 3\,021 - 54^2 = 105$

Dosazením do rovnice (7), kde za $i$ se dosazuje číslo 1 se získá hodnota $b_1$. Stejným způsobem se určí hodnoty pro $P_1$ a $Q_2$ dosazením do rovnic (8) a (9).

$$b_1 = \left\lfloor \frac{\lfloor \sqrt{N} \rfloor + P_0}{Q_1} \right\rfloor = \left\lfloor \frac{\lfloor \sqrt{3\,021} \rfloor + 54}{105} \right\rfloor = \left\lfloor \frac{54 + 54}{105} \right\rfloor = \left\lfloor \frac{108}{105} \right\rfloor = 1$$

$P_1 = b_1 \cdot Q_1 - P_0 = 1 \cdot 105 - 54 = 51$

$Q_2 = Q_0 + b_1 \cdot (P_0 - P_1) = 1 + 1 \cdot (54 - 51) = 1 + 3 = 4$

Tento postup by se opakoval do té doby, než se získá hodnota $Q_i$ rovna čtvercovému číslu. V tomto případě vyšlo čtvercové číslo hned v druhém kroku výpočtu.

Nyní se proces otočí a z následujících rovnic, na základě získaného čísla $Q_2$, se vypočte faktor čísla $N$. Do rovnic (10), (11) a (12) se dosadí index $i$, který byl získán v první části výpočtu. V tomto případě se získal index $i = 2$.

$$b_0 = \left\lfloor \frac{\lfloor \sqrt{N} \rfloor - P_{2-1}}{\sqrt{Q_2}} \right\rfloor = \left\lfloor \frac{\lfloor \sqrt{3\,021} \rfloor - 51}{\sqrt{4}} \right\rfloor = \left\lfloor \frac{54 - 51}{\sqrt{4}} \right\rfloor = \left\lfloor \frac{3}{2} \right\rfloor = 1$$

$$P_0 = b_0\sqrt{Q_2} + P_{2-1} = 1\sqrt{4} + 51 = 2 + 51 = 53$$

$$Q_0 = \sqrt{Q_2} = \sqrt{4} = 2$$

Po získání těchto hodnot je možno dosadit do rovnice (13).

$$Q_1 = \frac{N - P_0^2}{Q_0} = \frac{3\,021 - 53^2}{2} = \frac{3\,021 - 2\,809}{2} = \frac{212}{2} = 106$$

Postupně se dosazuje do rovnic (7), (8) a (9), a hledá se takové $P_i$, které se rovná $P_{i-1}$.

$$b_1 = \left\lfloor \frac{\lfloor \sqrt{N} \rfloor + P_{1-1}}{Q_1} \right\rfloor = \left\lfloor \frac{54 + 53}{106} \right\rfloor = \left\lfloor \frac{107}{106} \right\rfloor = 1$$

$$P_1 = b_1 \cdot Q_1 - P_{1-1} = 1 \cdot 106 - 53 = 53$$

Hned v prvním kroku se hodnota $P_1$ rovná $P_0$. Jeden z faktorů čísla $N$ se získá vyhledáním největšího společného dělitele čísel $N$ a $P_1$.

$$N = p \cdot q \ \wedge p = NSD(53, 3\,021) = 53$$

Druhý faktor se získá vydělením čísla $N$ prvním faktorem.

$$N = 3\,021 = 53 \cdot 57$$

Číslo $N$ lze rozdělit na součin dvou čísel 53 a 57.

**Příklad 20: Shanksova čtvercová faktorizační metoda**

Pomocí Shanksovy metody proveďte faktorizaci čísla $N = 13\,930\,021$.

**Řešení**: V prvním kroku se určí hodnoty $P_0, Q_0 \; a \; Q_1$ dosazením do rovnic (4), (5) a (6).

Tabulka 6 – Shanksova metoda – příklad (a)

| $i$ | $P_i$ | $Q_i$ | $b_i$ |
|---|---|---|---|
| 0 | 3732 | 1 | |
| 1 | 2859 | 2197 | 3 |
| 2 | 2381 | 2620 | 2 |
| 3 | 772 | 3153 | 1 |
| 4 | 3457 | 4229 | 1 |
| 5 | 3563 | 468 | 15 |
| 6 | 1715 | 2639 | 2 |
| 7 | 2449 | 4164 | 1 |
| 8 | 3266 | 1905 | 3 |
| 9 | 3586 | 1713 | 4 |
| 10 | 3289 | 625 | 11 |

Čtvercové číslo se získalo v desátém kroku, kde $Q_{10} = 625$. Nyní pomocí indexu $i = 10$ se opět určí hodnoty $P_0, b_0, Q_0 \; a \; Q_1$ pomocí rovnic (10), (11), (12) a (13). Následným dosazováním do rovnic (7), (8) a (9) se hledají hodnoty $P_i$ a $P_{i-1}$ takové které jsou si rovny.

Tabulka 7 – Shanksova metoda – příklad (b)

| $i$ | $P_i$ | $Q_i$ | $b_i$ |
|---|---|---|---|
| 0 | 3711 | 25 | 5 |
| 1 | 2629 | 6340 | 1 |
| 2 | 2906 | 1107 | 5 |
| 3 | 2049 | 4955 | 1 |
| 4 | 1879 | 1964 | 2 |
| 5 | 3416 | 5295 | 1 |
| 6 | 3416 | 427 | 16 |

Stejných dvou hodnot bylo dosaženo v šestém kroku, hodnota $P_6$ se rovná hodnotě $P_5$. Jeden z faktorů se získá nalezením NSD čísel $P_6$ a $N$.

$N = p \cdot q \ \wedge p = NSD(3\,416, 13\,930\,021) = 427$

$N = 13\,930\,021 = 427 \cdot 32\,623$

Faktory čísla $N$ se pomocí Shanksovy metody určily jako $p = 427$ a $q = 32\,623$.

# ZÁVĚR

V této bakalářské práci s názvem „Klasické i moderní faktorizační algoritmy“ jsou popsány různě náročné faktorizační algoritmy. Práce seznamuje s vybranými klasickými i moderními metodami faktorizace.

Jedním z hlavních přínosů této bakalářské práce je usnadnění se zorientovat v problematice faktorizace celých čísel. Každá metoda je podrobně popsána, vysvětlena a doplněna o názornou ukázku, ke každému algoritmu je uveden alespoň jeden příklad k názornějšímu pochopení.

V první části práce je vysvětlena teorie faktorizace, jsou zde popsány důležité matematické pojmy pro proces faktorizace. Stejně tak je zde uveden přínos faktorizace v oblasti matematiky. Jsou zde uvedeny podrobné postupy, jak faktorizaci využít pro získaní největšího společného dělitele a nejmenšího společného násobku. V závěru úvodu tématu je uveden význam prvočísel a samotné faktorizace pro bezpečnost moderní šifrovacích nástrojů. Princip využití je demonstrován na šifrovací metodě RSA, která je opět podrobně vysvětlena a doplněna o příklad.

Druhá kapitola se zabývá velmi užitečnými nástroji, a to metodami testování prvočíselnosti. Pro faktorizaci je testování prvočíselnosti velmi důležité, protože prvočísla nelze rozdělit na faktory. Bylo by tedy zbytečné se pokoušet tyto čísla faktorizovat. Test prvočíselnosti je dále využitelný po provedení samotné faktorizace, kdy se zjišťuje, zda získané faktory jsou prvočísly nebo jsou čísly složenými, a tedy proces faktorizace může pokračovat.

Stěžejní část práce je rozebírána ve třetí a čtvrté kapitole. Ve třetí kapitole jsou popsány čtyři klasické metody: metoda pokusného dělení, polynomická faktorizace, Fermatova faktorizační metoda a Eulerova faktorizační metoda. Pro moderní faktorizační metody byly vybrány a zpracovány: Pollardova p-1 metoda, metoda kvadratického síta a Shanksova čtvercová metoda.

Každá metoda má své výhody i nevýhody, které se projevují nejen časovou náročností, ale také vhodností použitelnosti dané metody pro jednotlivá čísla. Podrobnější srovnání jednotlivých metod je uvedeno v následující souhrnu.

| | |
|---|---|
| 1 | **Metoda pokusného dělení:**<br>faktorizované číslo $N$ se postupně zkouší dělit prvočísly, která jsou menší než číslo $\lfloor\sqrt{N}\rfloor$. |
| | Vstupní data nejsou omezená, metoda je vhodná pro čísla s menším řádem cifer, jelikož pro velká čísla by byla metoda velice zdlouhavá. |
| | Výsledkem této metody je úplná faktorizace zadaného čísla $N$ na prvočísla, protože během faktorizace dojde k vyhledání všech prvočíselných faktorů. |

| | |
|---|---|
| 2 | **Polynomická metoda:**<br>pomocí metody se vyhledávají čtverce $x^2$ a $y^2$, tak aby platila následující rovnice: $N = x^2 - y^2 = (x - y) \cdot (x + y)$. Určí se hodnota $y = 1$, která se postupně zvyšuje vždy o jednu a hledá se čtvercové číslo $x^2$. |
| | Vychází se z předpokladu, že vstupní hodnota $N$ je liché číslo. Metoda je nejvhodnější pro čísla, u kterých se $y = 1$ nebo blízké k jedné. |
| | Výsledkem této metody je nalezení dvou faktorů čísla $N$, které nemusejí být prvočíslem. |

| | |
|---|---|
| 3 | **Fermatova faktorizační metoda:**<br>je založena na předpokladu, že číslo $N$ se dá zapsat jako rozdíl dvou čtverců: $N = s^2 - t^2$. Určí se hodnota $s = \lfloor\sqrt{N}\rfloor + 1$ a $t = \sqrt{-N + s^2}$. Postupy se provádí zvýšení hodnoty $s$ o 1 a hledá se celé číslo $t$. |
| | Vychází se z předpokladu, že vstupní hodnota $N$ je liché číslo. Metoda je nejvhodnější pro čísla, u kterých se $s = 1$ nebo blízké k jedné. |
| | Výsledkem této metody je nalezení dvou faktorů čísla $N$, které nemusejí být prvočíslem. |

| | |
|---|---|
| 4 | **Eulerova faktorizační metoda:**<br>je založena na předpokladu, že zadané číslo $N$ se dá zapsat jako součet čtverců, a to dvěma různými způsoby: $N = a^2 + b^2 = c^2 + d^2$. |
| | Aby tato metoda mohla být použita, musí se pro číslo $N$ nejprve nalézt zápis dvou různých součtů čtverců, pokud tato čísla nejsou nalezena nebo neexistují nelze tuto metodu použít. |
| | Výsledkem této metody je nalezení dvou faktorů čísla $N$. |

| | |
|---|---|
| 5 | **Pollardova metoda p-1:**<br>vychází z Malé Fermatovy věty: $a^{k(p-1)} \equiv 1 \; mod \; p$, a hledá se číslo $M$, které je součinem prvočísel a jejich mocnin menších než hranice $B$. Jeden z faktorů se určí jako $q = NSD(a^M - 1; N)$. |
| | Metoda je výhodná pro čísla $N$ o určité hladkosti $B$. Pokud je zvolena hranice $B$ nízká může dojít k selhání algoritmu. S každým zvýšením hranice $B$ roste složitost a časová náročnost metody. |
| | Výsledkem této metody je nalezení dvou faktorů čísla $N$. |

| | |
|---|---|
| 6 | **Metoda kvadratického síta:**<br>vychází ze vzorce: $N = x^2 - y^2$, tedy hledají se dvě taková čísla, pro něž platí, že rozdíl jejich druhých mocnin se rovná zadanému číslu N. $y^2 = \left(\lfloor\sqrt{N}\rfloor + k\right)^2 - N$ . Hledá se takové $k$, aby platil výchozí vzorec. |
| | Vstupní data nejsou omezená. Obtížnost této metody závisí na velikosti faktorizovaného čísla více než na struktuře čísla a jeho vlastnostech. |
| | Výsledkem této metody je nalezení dvou faktorů čísla $N$. |

| | |
|---|---|
| 7 | **Shanksova čtvercová faktorizační metoda:**<br>vychází z Fermatovy faktorizační metody a využívá binární kvadratické formy, základní myšlenka vychází ze vztahu: $x^2 \equiv y^2 (mod\ N)$. |
| | Vstupní hodnota nesmí být druhou mocninou nebo prvočíslem. |
| | Výsledkem této metody je nalezení dvou faktorů čísla $N$, které nemusejí být prvočíslem. |

# RESUMÉ

V bakalářské práci jsou popsány různě náročné faktorizační algoritmy, které jsou rozděleny do dvou kapitol, jak již název napovídá do klasických a moderních. Ke každému algoritmu je uveden alespoň jeden příklad k názornějšímu pochopení. Celková práce je rozdělena do čtyř hlavních kapitol.

První kapitola je rozčleněna do pěti podkapitol. Na začátku je popsán nejdůležitější pojem této práce tedy faktorizace a co si člověk má představit pod tímto matematickým pojmem. V druhé podkapitole jsou popsány další základní matematické pojmy, které s touto problematikou souvisejí. Najde se zde vysvětlení pojmů jako je například prvočíslo, čtvercové číslo, složené číslo nebo prvočíselný rozklad. Ve třetí a čtvrté podkapitole se může čtenář seznámit s využitím faktorizace v matematice a šifrování. V poslední podkapitole jsou uvedeny pomocné algoritmy, které se využívají při samotné faktorizaci.

Druhá kapitola se zabývá testováním prvočíselnosti. Tímto testováním je dobré se zabývat, aby se zbytečně faktorizace neprováděla pro čísla, pro která je to nemožné. Proto jsou v této kapitole uvedeny jednoduché a obecné algoritmy pro testování prvočíselnosti ze kterých se dozvíme, zda je zadané číslo prvočíslem nebo číslem složeným. Tedy pokud zadané číslo vyjde pomocí těchto testů jako prvočíslo, nemusí se již faktorizovat neboli nelze nalézt jeho jiné faktory nežli samotné zadané číslo.

Třetí kapitola pojednává o klasických faktorizačních metodách. Jedná se o poměrně jednoduché metody, které mají snadný výpočet. Nevýhodou těchto metod je, že jsou určeny pro čísla specifického charakteru.

Poslední čtvrtá kapitola uvádí moderní faktorizační metody, které jsou na rozdíl od klasickým faktorizačních metod v principu složitější, avšak ve většině případů odpadají podmínky na podobu čísla, které se má faktorizovat.

# RESUME

The bachelor's thesis describes various demanding factorization algorithms. The description of these algorithms is divided into two chapters, as the title suggests it is divided into classic and modern. At least one example is given for each algorithm for easier and clear understanding of it. The work is divided into four main chapters.

The first chapter is divided into five subchapters. In the beginning, the most important concept of this work is described, that is the factorization. It describes what is represented by this mathematical term. The second subchapter describes other basic mathematical concepts related to this issue. There is an explanation of terms such as prime number, square number, composite number or prime decomposition. In the third and fourth subchapters, readers can learn about the use of factorization in mathematics and encryption. The last subchapter presents the auxiliary algorithms that are used in the factorization.

The second chapter deals with the testing of prime. It is good to deal whit this testing so that factorization is not done unnecessarily for numbers that cannot be factorized. Therefore, this chapter provides simple and general algorithms for testing prime numbers. These tests determine whether the number entered is a prime number or a composite number. If the result of the number test is prime number, this need not be further factorized. It is not possible to find factors other than the number entered.

The third chapter deals with classic factoring methods. These methods are relatively simple that have an easy calculation. The disadvantage of these methods is that they are designed for numbers of a specific nature.

The last fourth chapter sets out modern factoring methods. These methods are more complex in principle unlike classic factoring methods. In most cases, the conditions for the form of the number to be factorized are eliminated.

# SEZNAM LITERATURY


[1] Algoritmy.net. *Faktorizace* [online]. 2015 [cit. 2020-06-21]. Dostupné z: https://www.algoritmy.net/article/111/Faktorizace

[2] Dostudujte.cz. *Prvočíselné rozklady: Prvočíselný rozklad – rozklad čísel na součin prvočísel* [online]. Praha, 2012 [cit. 2020-06-21]. Dostupné z: https://www.dostudujte.cz/matematika/cisla/rozklad-cisel-na-prvocisla

[3] *Matematika: Prvočísla a čísla složená* [online]. 2011 [cit. 2020-06-21]. Dostupné z: http://www.matematikasestka.wz.cz/cisla.html

[4] *IT slovník: Čtvercové číslo* [online]. 2008 [cit. 2020-06-21]. Dostupné z: https://it-slovnik.cz/pojem/ctvercove-cislo

[5] *Matematika: Čísla soudělná a nesoudělná* [online]. 2011 [cit. 2020-06-21]. Dostupné z: http://www.matematikasestka.wz.cz/soudelna.html

[6] *ITnetwork.cz: Největší společný dělitel (Euklidův algoritmus)* [online]. 2019 [cit. 2020-06-21]. Dostupné z: https://www.itnetwork.cz/algoritmy/matematicke/algoritmus-vypocet-nejvetsiho-spolecneho-delitele-eukliduv-algoritmus

[7] *Wikipedie: Eukleidův algoritmus* [online]. [cit. 2020-06-21]. Dostupné z: https://cs.wikipedia.org/wiki/Eukleidův_algoritmus

[8] *Algoritmy.net: Euklidův algoritmus* [online]. 2015 [cit. 2020-06-21]. Dostupné z: https://www.algoritmy.net/article/44/Eukliduv-algoritmus

[9] HORA, Jaroslav. *O některých otázkách souvisejících s využíváním programů počítačové algebry ve škole: III. díl*. Plzeň: Pedagogické centrum Plzeň, 2005. ISBN 80-7020-092-8.

[10] CRANDALL, Richard a Carl POMERANCE. *Prime numbers: A Computational Perspective*. Druhá edice. United States of America: Springer, 2000. ISBN 978-0387-25282-7.

[11] *Fi.muni.cz: Eulerova funkce φ* [online]. [cit. 2020-06-21]. Dostupné z: https://www.fi.muni.cz/~zlamal/fonctionPhiDEuler.html

[12] *Wikisofia: Asymetrická kryptografie* [online]. 2013 [cit. 2020-06-21]. Dostupné z: https://wikisofia.cz/wiki/Asymetrická_kryptografie

[13] *Voho.eu: Eratosthenovo síto* [online]. 2008 [cit. 2020-06-21]. Dostupné z: http://voho.eu/wiki/algoritmus-eratosthenes/

[14] *Algoritmy.net: Fermatův test prvočíselnosti* [online]. [cit. 2020-06-21]. Dostupné z: https://www.algoritmy.net/article/61/Fermatuv-test

[15] *Algoritmy.net: Rabin-Millerův test prvočíselnosti* [online]. [cit. 2020-06-21]. Dostupné z: https://www.algoritmy.net/article/73/Rabin-Milleruv-test

[16] *Algoritmy.net: Elementární test prvočíselnosti* [online]. [cit. 2020-06-21]. Dostupné z: https://www.algoritmy.net/article/38/Elementarni-test

[17] *WolframMathWorld: Polynomial Factorization* [online]. 2020 [cit. 2020-06-21]. Dostupné z: https://mathworld.wolfram.com/PolynomialFactorization.html

[18] *Math.feld.cvut.cz: Fermatův faktorizační algoritmus* [online]. [cit. 2020-06-21]. Dostupné z: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj36J7bqpPqAhUWTxUIHWK2AWkQFjAAegQIAxAB&url=ftp%3A%2F%2Fmath.feld.cvut.cz%2Fpub%2Fnentvich%2Fx01dml%2Fx01dml_pomocny_text.pdf&usg=AOvVaw0vka5bQlHjPWB_UgraLAqt

[19] *MT MacTutor: Pierre de Fermat* [online]. 1996 [cit. 2020-06-21]. Dostupné z: https://mathshistory.st-andrews.ac.uk/Biographies/Fermat/

[20] *MT MacTutor: Leonhard Euler* [online]. 1998 [cit. 2020-06-21]. Dostupné z: https://mathshistory.st-andrews.ac.uk/Biographies/Euler/

[21] GATHEN, Joachim von zur a Jürgen GERHARD. *Modern computer algebra*. 3rd ed. Cambridge: Cambridge University Press, 2013. ISBN 978-1107039032.

[22] *WolframMathWorld: Quadratic Sieve* [online]. 2020 [cit. 2020-06-21]. Dostupné z: https://mathworld.wolfram.com/QuadraticSieve.html

[23] *Wikipedia: Shanks's square forms factorization* [online]. 2020 [cit. 2020-06-21]. Dostupné z: https://en.wikipedia.org/wiki/Shanks%27s_square_forms_factorization

[24] WAGSTAFF, Samuel S. *The Joy of Factoring*. AmericanMathematical Society, 2013. ISBN 1-4704-1048-6.

[25] CHILDS, Lindsay. *A concrete introduction to higher algebra*. Third edition. New York: Springer, [2009]. Undergraduate texts in mathematics. ISBN 978-0-387-74527-5.

# SEZNAM OBRÁZKŮ A TABULEK



**Zdroje obrázků:**

1. Wikimedia [online]. 2020 [cit. 2020-06-21]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/thumb/f/f3/Pierre_de_Fermat.jpg/225px-Pierre_de_Fermat.jpg
2. Mendeleu, [online]. 2020 [cit. 2020-06-21]. Dostupné z: http://user.mendelu.cz/marik/wiki/am/slidy/vyroci_2015/Euler.jpg