Katedra informatiky
Přírodovědecká fakulta
Univerzita Palackého v Olomouci

DIPLOMOVÁ PRÁCE

Řetězové zlomky a jejich použití v informatice

2023

Eliška Foltasová

Vedoucí práce:
doc. RNDr. Miroslav Kolařík, Ph.D.

Studijní program: Informatika,
Specializace: Obecná informatika

Bibliografické údaje

Autor:	Eliška Foltasová
Název práce:	Řetězové zlomky a jejich použití v informatice
Typ práce:	diplomová práce
Pracoviště:	Katedra informatiky, Přírodovědecká fakulta, Univerzita Palackého v Olomouci
Rok obhajoby:	2023
Studijní program:	Informatika, Specializace: Obecná informatika
Vedoucí práce:	doc. RNDr. Miroslav Kolařík, Ph.D.
Počet stran:	62
Přílohy:	elektronická data v úložišti katedry informatiky
Jazyk práce:	český

Bibliographic info

Author:	Eliška Foltasová
Title:	Continued fractions and their application in computer science
Thesis type:	master thesis
Department:	Department of Computer Science, Faculty of Science, Palacký University Olomouc
Year of defense:	2023
Study program:	Computer Science, Specialization: General Computer Science
Supervisor:	doc. RNDr. Miroslav Kolařík, Ph.D.
Page count:	62
Supplements:	electronic data in the storage of department of computer science
Thesis language:	Czech

Anotace

Cílem této diplomové práce je seznámit čtenáře s tématem řetězových zlomků a popsat některá jejich využití v informatice, např. útoky na šifru RSA. V praktické části práce je pak implementována kalkulačka pro počítání s racionálními řetězovými zlomky.

Synopsis

The aim of this Master's thesis is to introduce the subject of continued fraction to the reader and to describe some of their applications in computer science, such as attacks on the RSA cipher. An application for performing calculations with rational continued fractions was implemented.

Klíčová slova: řetězové zlomky, RSA

Keywords: continued fractions, RSA

Tímto děkuji panu docentu RNDr. Miroslavu Kolaříkovi, PhD. za odborné vedení mé diplomové práce, za jeho profesionální a velkorysý přístup. V neposlední řadě děkuji svým blízkým za psychickou podporu.

Odevzdáním tohoto textu jeho autor/ka místopřísežně prohlašuje, že celou práci včetně příloh vypracoval/a samostatně a za použití pouze zdrojů citovaných v textu práce a uvedených v seznamu literatury.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Řetězové zlomky jsou matematickým fenoménem. Představují velice elegantní a efektivní reprezentaci čísel alternativní ke standardní poziční notaci. I přes jejich jednoduchost a praktičnost ovšem nelze říci, že s nimi byla široká veřejnost seznámena – nepatří k běžnému učivu na středních školách a jejich znalost je tedy výsadou zejména matematiků.

Nacházejí své využití nejen v každé přírodní vědě, ale i v hudbě, umění, architektuře a dalších součástech našeho každodenního života.

Na trhu není nedostatek publikací věnujících se řetězovým zlomkům po stránce jak teoretické, tak praktičtější. Hlavním cílem této práce je přiblížit je čtenáři z hlediska informatického. Rozsah tohoto textu neumožňuje shrnutí všech existujících využití řetězových zlomků v informatice, proto je detailní důraz kladen na konkrétní téma útoků na šifru RSA, které jsou chronologicky prezentovány v kapitole 5.

Kapitola 2 slouží jako úvod do teorie řetězových zlomků. Definuje základní pojmy potřebné k porozumění tématu řetězových zlomků, a také přibližuje čtenáři některé jejich vlastnosti.

Součástí kapitoly 3 je popis vzniku a vývoje teorie řetězových zlomků coby matematické disciplíny. Kapitola dále představuje vybraná využití řetězových zlomků a také řetězové zlomky reprezentující některá významná iracionální čísla jako π či Eulerovu konstantu.

Kapitola 4 se soustředí na vlastnosti řetězových zlomků, které je činí vhodnými (či naopak nevhodnými) pro praktickou implementaci, a popisuje Gosperův algoritmus sloužící k aritmetickým výpočtům s řetězovými zlomky.

Poslední kapitola pak slouží jako stručná uživatelská příručka pro aplikaci, která vznikla v rámci praktické části této práce a slouží k počítání s racionálními řetězovými zlomky.

2 Základní pojmy

Kapitola seznamuje čtenáře s pojmy, jejichž znalost je ve zbytku práce nutná k porozumění tématu. Není-li uvedeno jinak, informace obsažené v této kapitole jsou čerpány ze zdrojů [[8]], [[15]].

Definice 1 (Řetězový zlomek)
Výraz

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots}}},$$

kde a_0, a_1, a_2, ... jsou v obecném případě hodnoty nějakého číselného oboru, nazýváme **řetězovým zlomkem** či **řetězcem** (zkráceně ŘZ). Čísla $a_0, a_1, a_2, \ldots$ pak nazýváme **prvky** řetězce.

Není-li řečeno jinak, v této práci považujeme a_0 za celé číslo, a_1, a_2, ... za přirozená čísla.

Pro lepší přehlednost je obvyklé zapisovat řetězový zlomek výčtem jeho prvků ve tvaru $[a_0; a_1, a_2, \ldots, a_k]$.

Definice 2 (Konečný řetězový zlomek)
Je-li počet prvků řetězce konečný, pak on sám je **konečným řetězovým zlomkem** a zapisujeme jej jako

$$[a_0; a_1, a_2, \ldots, a_{n-1}, a_n],$$

kde počet jeho prvků je $n+1$. Říkáme, že takový řetězový zlomek je $n-$**členný** (prvek a_0 nepovažujeme za člen zlomku), případně $(n-1)$**-prvkový**.

Každý konečný řetězový zlomek je výsledkem konečného počtu racionálních operací nad celými čísly, a tedy reprezentuje racionální číslo.

Mezi konečnými řetězovými zlomky a racionálními čísly existuje bijekce, tedy každé racionální číslo lze reprezentovat právě jedním konečným řetězovým zlomkem.

Nebudeme-li se v definici řetězového zlomku omezovat na konečný počet prvků, získáme nekonečný řetězový zlomek:

Definice 3 (Nekonečný řetězový zlomek)
V případě, že počet prvků řetězového zlomku je nekonečný, jedná se o **nekonečný zlomek**, zapisujeme jej

$$[a_0; a_1, a_2, a_3, \ldots].$$

Nekonečnému řetězovému zlomku nelze obecně přiřadit číselnou hodnotu. Je pouze formálním zápisem, podobně jako číselná řada. Při dodržení jednoduchých podmínek, které budou představeny níže v této kapitole, nekonečný zlomek reprezentuje iracionální číslo.

2.1 Sblížené zlomky

Pro konečný řetězový zlomek $\alpha = [a_0; a_1, a_2, \ldots, a_n]$ definujeme

$$s_k = [a_0; a_1, a_2, \ldots, a_k],$$

kde $0 \leq k \leq n$, jako **úsek řetězového zlomku** α a

$$r_k = [a_k; a_{k+1}, a_{k+2}, \ldots, a_n]$$

jako **zbytek řetězového zlomku** α.

Tímto zbytkem můžeme nahradit odpovídající členy v zápisu řetězového zlomku:

Věta 4
Pro $0 \leq k \leq n$ *platí:*

$$[a_0; a_1, a_2, \ldots, a_n] = [a_0; a_1, a_2, \ldots, a_{k-1}, r_k].$$

Každý konečný řetězový zlomek $[a_0; a_1, a_2, \ldots, a_k]$ jsme schopni vyjádřit jako podíl dvou mnohočlenů

$$\frac{P(a_0, a_1, a_2, \ldots a_k)}{Q(a_0, a_1, a_2, \ldots a_k)}$$

s celými koeficienty, tedy jej lze zapsat jako zlomek $\frac{P}{Q}$, kde $P, Q \in \mathbb{Z}$. Tomuto vyjádření říkáme **kanonické**.

Definice 5 (Sblížený zlomek)
O zlomku $\frac{p_k}{q_k}$ pro $0 \leq k \leq n$ hovoříme jako o k**-tém sblíženém zlomku** $n-$členného řetězového zlomku α.

Takových zlomků existuje pro $n-$prvkový konečný řetězový zlomek právě n a jejich podobu lze snadno vypočítat:

$$C_0 = \frac{a_0}{1} = \frac{P_0}{Q_0}$$
$$C_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{P_1}{Q_1}$$
$$C_2 = a_1 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1} = \frac{P_2}{Q_2}:$$

Pro konečný řetězový zlomek α zjevně platí $\frac{P_n}{Q_n} = \alpha$.

Hodnotu čitatele a jmenovatele sblíženého zlomku můžeme vypočítat i rekurentně, a to podle následujících vzorců využívajících předchozí dva členy:

Věta 6 (Zákon znázornění sblížených zlomků)
Pro každé $k \geq 2$ jsou platné následující vztahy:

$$P_k = a_k P_{k-1} + P_{k-2}$$
$$Q_k = a_k Q_{k-1} + Q_{k-2}$$

Dle dohody je také definován sblížený zlomek řádu -1. Platí pro něj $P_{-1} = 1$, $Q_{-1} = 0$. Díky tomuto pravidlu lze rozšířit výše uvedené vzorce i na $k = 1$.

Příklad 7

Rekurentně vypočítáme všechny sblížené zlomky ŘZ $\alpha = [1; 2, 3, 4, 5]$:

$$C_0 = \frac{P_0}{Q_0} = \frac{a_0}{1} = \frac{1}{1}$$
$$C_1 = \frac{P_1}{Q_1} = a_0 + \frac{1}{a_1} = 1 + \frac{1}{2} = \frac{3}{2}$$
$$C_2 = \frac{P_2}{Q_2} = \frac{a_2 P_1 + P_0}{a_2 Q_1 + Q_0} = \frac{3 \cdot 3 + 1}{3 \cdot 2 + 1} = \frac{10}{7}$$
$$C_3 = \frac{P_3}{Q_3} = \frac{a_3 P_2 + P_1}{a_3 Q_2 + Q_1} = \frac{4 \cdot 10 + 3}{4 \cdot 7 + 2} = \frac{43}{30}$$
$$C_4 = \frac{P_4}{Q_4} = \frac{a_4 P_3 + P_2}{a_4 Q_3 + Q_2} = \frac{5 \cdot 43 + 10}{5 \cdot 30 + 7} = \frac{225}{157}$$

Obdobným způsobem jako v předpisu 5 definujeme sblížené zlomky i pro nekonečné řetězové zlomky, ovšem s tím rozdílem, že pro každý nekonečný řetězový zlomek jich nutně existuje nekonečně mnoho. Tvoří tedy posloupnost

$$\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \ldots$$

Každý sblížený zlomek $\frac{P_k}{Q_k}$ nekonečného ŘZ je coby podíl dvou racionálních čísel také racionálním číslem.

Věta 8

Má-li posloupnost sblížených zlomků nekonečného řetězového zlomku limitu α, je tato hodnota rovna hodnotě řetězce, píšeme tedy

$$\alpha = [a_0; a_1, a_2, a_3, \dots].$$

Takový řetězový zlomek se nazývá **konvergentní**. V opačném případě (neexistuje-li limita) říkáme, že zlomek **diverguje**.

Věta 9

Pro konvergenci nekonečného zlomku $[a_0; a_1, a_2, a_3, \dots]$ je nutnou a postačující podmínkou divergence řady

$$\sum_{n=1}^{\infty} a_n.$$

2.2 Vlastnosti sblížených zlomků

Poznatky o vztazích mezi dvěma po sobě jdoucími sblíženými zlomky patří k nejdůležitějším výsledkům teorie řetězových zlomků. Popisuje je několik následujících vět.

Věta 10

Pro všechna $k \geq 0$ platí:

$$Q_k P_{k-1} - P_k Q_{k-1} = (-1)^k$$

Důkaz

Využijeme rekurentní vzorce z Věty 6. Vynásobíme-li první rovnost výrazem Q_{k-1} a druhou výrazem P_{k-1}, máme soustavu

$$\begin{aligned} P_k Q_{k-1} &= a_k P_{k-1} Q_{k-1} + P_{k-2} Q_{k-1} \\ Q_k P_{k-1} &= a_k Q_{k-1} P_{k-1} + Q_{k-2} P_{k-1}. \end{aligned}$$

Odečteme-li první rovnost od druhé, získáváme vztah

$$Q_k P_{k-1} - P_k Q_{k-1} = Q_{k-2} P_{k-1} - P_{k-2} Q_{k-1}.$$

Jelikož víme, že $P_0 = 1$, $Q_0 = 1$, $P_{-1} = 1$ a $Q_{-1} = 0$, pak nutně

$$Q_0 P_{-1} - P_0 Q_{-1} = 1 - 0 = 1.$$

Tímto je věta dokázána. □

Věta 11
Pro všechna $k \geq 1$ platí

$$Q_k P_{k-2} - P_k Q_{k-2} = (-1)^{k-1} a_k.$$

Důkaz
Opět využijeme vzorce z Věty 6. První rovnost vynásobíme výrazem Q_{k-2}, druhou výrazem P_{k-2}:

$$\begin{aligned} P_k Q_{k-2} &= a_k P_{k-1} Q_{k-2} + P_{k-2} Q_{k-2} \\ Q_k P_{k-2} &= a_k Q_{k-1} P_{k-2} + Q_{k-2} P_{k-2}. \end{aligned}$$

Odečtením první rovnosti od druhé získáváme výraz

$$Q_k P_{k-2} - P_k Q_{k-2} = a_k (Q_{k-1} P_{k-2} - P_{k-1} Q_{k-2}).$$

Díky Větě 10 víme, že $Q_{k-1} P_{k-2} - P_{k-1} Q_{k-2} = (-1)^{k-1}$. Věta je tímto dokázána. □

Věta 12
Pro každé $k \geq 1$ platí:

$$\frac{Q_k}{Q_{k-1}} = [a_k; a_{k-1}, a_{k-2}, \ldots, a_1].$$

Důkaz
Tvrzení dokážeme matematickou indukcí:
Pro $k = 1$ je vztah zřejmý:

$$\frac{Q_1}{Q_0} = a_1.$$

Díky Větě 6 víme, že platí:

$$\frac{Q_k}{Q_{k-1}} = a_k + \frac{Q_{k-2}}{Q_{k-1}} = [a_k; \frac{Q_{k-1}}{Q_{k-1}}].$$

Předpokládáme-li, že $k > 1$ a vztah je dokázaný pro $k - 1$, tedy:

$$\frac{Q_{k-1}}{Q_{k-2}} = [a_{k-1}; a_{k-2}, a_{k-3}, \ldots, a_1].$$

Na základě tohoto předpokladu a vztahu 4 je požadovaný vztah dokázán:

$$\frac{Q_k}{Q_{k-1}} = [a_k; a_{k-1}, \ldots, a1].$$

□

Věta 13

Sblížené zlomky sudého řádu tvoří rostoucí posloupnost, kdežto sblížené zlomky lichého řádu tvoří klesající posloupnost. Každý sblížený zlomek lichého řádu je větší než každý libovolný zlomek sudého řádu.

Pro konečný řetězový zlomek α navíc zjevně platí, že každý jeho sblížený zlomek lichého řádu je větší než on sám a každý jeho sblížený zlomek sudého řádu je menší než on sám, s výjimkou posledního zlomku $\frac{P_n}{Q_n}$. Obě posloupnosti se tedy shora, resp. zdola, blíží hodnotě α.

Následující věta je užitečným nástrojem pro ověření, zda jeden zlomek je sblíženým zlomkem druhého. S jejím praktickým využitím se seznámíme v kapitole 5.

Věta 14 (Legendrova věta)

Nechť α je reálné číslo. Jsou-li x, y přirozená vzájemně nesoudělná čísla a platí-li

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{2y^2}, \tag{1}$$

pak $\frac{x}{y}$ je sblíženým zlomkem řetězového zlomku reprezentujícího α.

2.3 Aproximace reálných čísel

Řekneme, že racionální číslo $\frac{n}{d}$ je **nejlepší aproximací** reálného čísla α, neexistuje-li žádné jiné racionální číslo $\frac{n'}{d'}$ tak, že platí

$$\left|\frac{n'}{d'} - \alpha\right| < \left|\frac{n}{d} - \alpha\right|$$

a zároveň $d' \leq d$.

Zkrátíme-li regulární řetězový zlomek reprezentující číslo $\alpha = [a_0; a_1, a_2, \ldots,]$ (tzn. odstraníme-li pro nějaké i člen a_i a všechny členy po něm následující), získáme tím vždy jeho nejlepší racionální aproximaci.

3 Význam řetězových zlomků (nejen) v matematice

Řetězové zlomky matematici využívali při svých výpočtech již ve starověku, trvalo však bezmála dvě tisíciletí, než dostaly svůj ustálený název, poznatky o nich shromážděné byly uceleny a teorie řetězových zlomků se stala samostatným odvětvím matematiky.

Není-li uvedeno jinak, všechny informace představené v této kapitole byly čerpány z publikace [[3]].

3.1 Historický přehled

Za neoficiální počátek existence řetězových zlomků můžeme považovat vznik Eukleidova algoritmu, který je zároveň prvním písemně zaznamenaným netriviálním algoritmem. První zmínky o něm se datují do 3. století před naším letopočtem a matematik Eukleid, po němž je pojmenován, s největší pravděpodobností není jeho autorem.

Za prapůvodce teorie řetězových zlomků jsou považováni Rafael Bombelli a Pietro Cataldi, matematici z italské Bologni. Bombelli se zabýval problémem získání druhé odmocniny nečtvercového čísla. Nalezl řetězový zlomek reprezentující číslo $\sqrt{13}$, a roku 1579 ve svém díle *L'Algebra Opera* své výsledky publikoval.

$$\sqrt{13} = 3 + \cfrac{4}{6 + \cfrac{4}{6 + \cfrac{4}{6 + \ddots}}}.$$

Cataldi se vrátil k Bombelliho práci a jeho algoritmus zobecnil: Hodnotu $\sqrt{n}$ si můžeme rozepsat jako

$$\sqrt{n} = \sqrt{a^2 + r} = a + x,$$

kde za a volíme celé číslo tak, aby zbytek r měl co nejmenší hodnotu. Pak získáváme vztah

$$a^2 + r = a^2 + 2ax + x^2,$$

a zanedbáním členu x^2 dostaneme rovnost

$$r = 2ax,$$

a tedy

$$\sqrt{n} = a + \frac{r}{2a}.$$

Jelikož víme, že $x = \frac{r}{2a}$, a tedy $x^2 = \frac{rx}{2a}$, můžeme si položit

$$r = 2ax + \frac{rx}{2a} = (2a + \frac{r}{2a})x.$$

Využitím této aproximace hodnoty x získáme

$$\sqrt{n} = a + \frac{r}{2a + \frac{r}{2a}} = a + \frac{r}{a + \sqrt{n}}.$$

Tento postup lze opakovat stále dokola, čímž získáme řetězový zlomek

$$n = a + \cfrac{r}{2a + \cfrac{r}{2a + \cfrac{r}{2a + \ddots}}}.$$

John Wallis ve svém díle *Opera Matematica* roku 1695 poprvé použil pojem „řetězový zlomek“ a popsal některé vlastnosti sblížených zlomků a také vzorec pro výpočet $n-$tého sblíženého zlomku.

Za tzv. „zlatou éru“ řetězových zlomků se označuje 18. století, kdy se na rozvoji tohoto odvětví podílelo několik významných matematiků berlínské školy. **Leonhard Euler** jako první dokázal, že každému racionálnímu číslu odpovídá konečný řetězový zlomek, a že každé iracionální číslo lze zapsat nekonečným řetězovým zlomkem. Euler také vyjádřil řetězový zlomek reprezentující Eulerovu konstantu e, jíž je věnována sekce 3.3.3. Popsal též převod řetězového zlomku na mocninnou řadu, a vyjádřil řešení kvadratické rovnice

$$x^2 = ax + b, \text{ kterou lze přepsat jako } x = a + \frac{b}{x},$$

a tedy získal řetězový zlomek

$$x = a + \cfrac{b}{a + \cfrac{b}{a + \cfrac{b}{a + \ddots}}}.$$

Johann Lambert dokázal iracionalitu π pomocí řetězového zlomku funkce tangens:

$$\tan(x) = \cfrac{x}{1 + \cfrac{x^2}{3 + \cfrac{x^2}{5 + \cfrac{x^2}{7 + \cfrac{x^2}{9 + \ddots}}}}}.$$

Joseph-Louis Lagrange dokázal, že každému číslu, které je druhou odmocninou přirozeného nečtvercového čísla, odpovídá periodický řetězový zlomek ve tvaru buď

$$[a_0; a_1, \ldots, a_n, a_n, \ldots, a_1, 2a_0], \qquad \text{nebo} \qquad [a_0; a_1, \ldots, a_n, k, a_n, \ldots, a_1, 2a_0],$$

kde k je přirozené číslo. Lagrange se dále zabýval užitím řetězových zlomků v integrálním počtu.

Ani v 19. století nebylo na řetězové zlomky zapomenuto, naopak v tomto období již byly známé každému matematikovi. Carl Friedrich Gauss navázal na Lambertovo a Eulerovo dílo a z hypergeometrických funkcí vyvodil analytické řetězové zlomky pro reprezentaci mnohých elementárních a některých transcendentních funkcí.

3.2 Vybraná využití řetězových zlomků

3.2.1 Eukleidův algoritmus

Algoritmus hledá pro dvě celá čísla a, b jejich největší společný dělitel, a coby „vedlejší produkt“ vytváří konečný řetězový zlomek. Jeho běh můžeme popsat následovně: Pro přirozená čísla a, b, kde $a \geq b$, existují celočíselné koeficienty q_i, r_i ve tvaru

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, \end{aligned}$$

kde $q_0, q_1, \ldots, q_n$ jsou prvky řetězového zlomku $\frac{a}{b}$, q_n je největší společný dělitel čísel a, b, a $r_n = 0$.

Příklad 15

Hledáme největšího společného dělitele čísel 9261 a 1291. Označíme si $a = 9261$, $b = 1291$.

$$
\begin{aligned}
9261 &= 7 \cdot 1291 + 224 \\
1291 &= 5 \cdot 224 + 171 \\
224 &= 1 \cdot 171 + 53 \\
171 &= 3 \cdot 53 + 12 \\
53 &= 4 \cdot 12 + 5 \\
12 &= 2 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 2 \cdot \mathbf{1} + 0.
\end{aligned}
\qquad
\frac{9261}{1291} = 7 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{2 + \frac{1}{2}}}}}}}.
$$

Zjistili jsme, že $GCD(9261, 1291) = 1$ a $\frac{9261}{1291} = [7; 5, 1, 3, 4, 2, 2, 2]$.

3.2.2 Huygensovo planetárium

Matematik a astronom Christiaan Huygens využil řetězových zlomků při stavbě mechanického modelu sluneční soustavy mezi lety $1680 - 1682$. Huygens dle dostupných údajů věděl, že doba oběhu Saturnu kolem Slunce je přibližně $\frac{77708431}{2640858} \doteq 29,425$ let. Určil si řetězový zlomek odpovídající této hodnotě:

$$\frac{77708431}{2640858} = [29; 2, 2, 1, 5, 1, 4, 1, \dots].$$

Čtvrtý sblížený zlomek je $[29; 2, 2, 1] = \frac{206}{7}$. Huygens tedy opatřil kolo reprezentující oběžnou dráhu Saturnu 206 zuby, a kolo reprezentující oběžnou dráhu Země 7 zuby. Obdobným způsobem pak určil počet ozubených kol i pro oběžné dráhy ostatních planet. Planetárium je často uváděno jako první praktické využití řetězových zlomků.

3.2.3 Gregoriánský kalendář a přestupné roky

Příkladem praktického využití řetězových zlomků, s nímž se setkáváme v každodenním životě, je měření času gregoriánským kalendářem, který byl představen roku 1582 papežem Řehořem XIII. a od té doby si jej osvojila většina světa.

Nový kalendář vznikl s cílem zpřesnění měření času s ohledem na odchylku mezi klasickým kalendářním rokem a časem, který trvá Zemi vykonat jeden oběh kolem Slunce, což je zhruba $365,2422$ dní. Do jeho předchůdce juliánského kalendáře byl sice již zakomponován přestupný (tj. o jeden den delší) rok opakující se každé čtyři roky, to však odpovídalo $365,25$ letům, a docházelo tedy ke zkreslení, které se s probíhajícími lety zvětšovalo a způsobovalo problémy např. při určování data Velikonoc.

Číslo $365,2422$ můžeme zapsat řetězovým zlomkem jako

$$365,2422 = [365; 4, 7, 1, 3, 4, 1, 1, 1, 2].$$

Druhý sblížený zlomek je pak roven

$$365 + \frac{1}{4} = 365,25,$$

což odpovídá průměrné délce jednoho roku zaznamenaného juliánským kalendářem. Určíme si čtvrtý sblížený zlomek:

$$[365; 4, 7, 1] = 365 + \frac{8}{33}.$$

Víme, že gregoriánský kalendář přidává ke „klasickému“ 365 dní trvajícímu roku jeden den každé čtyři roky, s výjimkou let dělitelných 100, které zároveň nejsou dělitelné 400 (proto rok 2000 byl přestupný). Z každých 400 je tedy celkem $4 \cdot (\frac{100}{4} - 1) + 1 = 97$ přestupných. Snadno ověříme, jak přesná je naše aproximace:

$$400 \cdot 365 + 97 = 146097 \text{ dní.}$$

Oproti tomu s vyžitím čtvrtého sblíženého zlomku, který jsme vypočítali, získáváme

$$400 \cdot \left(365 + \frac{8}{33}\right) = 146096,\overline{96} \text{ dní.}$$

Vidíme, že řetězovým zlomkem skutečně dosáhneme velmi přesné aproximace.

3.2.4 Řešení některých rovnic

Diofantická rovnice je polynomiální rovnice, jejíž kořeny mohou nabývat pouze celočíselných hodnot. Existuje několik druhů diofantických rovnic. Řetězové zlomky jsou užitečným nástrojem řešení rovnic.

Indický matematik Árjabhata kolem roku 510 našeho letopočtu využil řetězové zlomky pro řešení lineární rovnice ve tvaru

$$ax - by = c,$$

kde a, b, c jsou přirozená čísla.

Pellova rovnice je rovnice ve tvaru

$$x^2 - ny^2 = 1,$$

kde x, y jsou přirozená čísla a n je přirozené nečtvercové číslo (tzn. není druhou mocninou žádného jiného celého čísla).

První zaznamenaný pokus o řešení Pellovy rovnice se datuje do roku 628, kdy indický matematik Brahmagupta nalezl kořeny rovnice

$$92x^2 + 1 = y^2.$$

Brahmagupta objevil rovnost

$$(x_1^2 - ny_1^2)(x_2^2 - ny_2^2) = (x_1x_2 + ny_1y_2)^2 - n(x_1y_2 + x_2y_1)^2.$$

J. L. Lagrange dokázal, že není-li n čtvercové číslo, pak má taková rovnice nekonečně mnoho vzájemně různých řešení, která mohou být využita pro aproximaci druhé odmocniny n.

Příklad 16

Hledáme kořeny Pellovy rovnice ve tvaru $x^2 - 7y^2 = 1$. Víme, že $\sqrt{7} = [2; \overline{1, 1, 1, 4}]$. Vidíme, že délka periody je 4, a tedy čitatel a jmenovatel třetího sblíženého zlomku budou řešením této rovnice.

n	-2	-1	0	1	2	3	4	5	6	7
a_n			2	1	1	1	4	1	1	1
p_n	0	1	2	3	5	8	37	45	82	127
q_n	1	0	1	1	2	3	14	17	31	48

Vidíme, že $p_3 = 8$, $q_3 = 3$. Dosadíme tyto hodnoty do předpisu rovnice: $8^2 - 7 \cdot 3^2 = 1$. Další řešení nalezneme jako čitatel a jmenovatel každého $k-$tého sblíženého zlomku pro $k = 3 + 4i$, kde $i = \{0, 1, 2, \dots\}$. V tabulce např. máme $p_7 = 127$, $q_7 = 48$. Opět snadno ověříme, že rovnost $127^2 - 7 \cdot 48^2 = 1$ platí.

3.3 Vybrané významné řetězové zlomky

3.3.1 Fibonacciho posloupnost a zlatý řez

Zlatý řez je hodnota

$$\phi = \frac{1 + \sqrt{5}}{2}.$$

Jedná se o číslo s nejobtížnější aproximací pomocí racionálních hodnot. Z tohoto důvodu je mu někdy přezdíváno „nejiracionálnější“ číslo.

Můžeme se s ním setkat nejen v přírodních vědách, ale i v architektuře, umění či hudbě.

Dvě čísla $a, b \in \mathbb{R}, a > b > 0$ splňují podmínku **zlatého řezu**, jestliže platí rovnost:

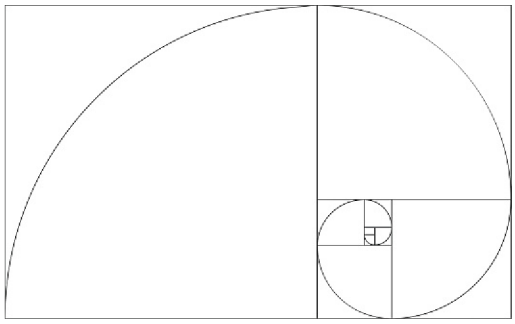
$$\phi = \frac{a + b}{a} = \frac{a}{b}.$$

Hodnotu zlatého řezu lze vyjádřit řetězovým zlomkem:

$$\phi = [1; 1, 1, 1, 1, \dots] = [\overline{1}].$$

Členy Fibonacciho posloupnosti vypočítáme následujícím rekurentním předpisem:

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \text{ pro } n \geq 2. \end{aligned}$$



Obrázek 1: Grafické znázornění zlatého řezu. Zdroj: https://en.wikipedia.org/wiki/Golden_ratio

Jednoduše určíme hodnoty několika dalších členů:

$$\begin{aligned} F_2 &= F_1 + F_0 = 1 + 0 = 1, & F_6 &= F_5 + F_4 = 5 + 3 = 8, \\ F_3 &= F_2 + F_1 = 1 + 1 = 2, & F_7 &= F_6 + F_6 = 8 + 5 = 13, \\ F_4 &= F_3 + F_2 = 2 + 1 = 3, & F_8 &= F_7 + F_6 = 21, \\ F_5 &= F_4 + F_3 = 3 + 2 = 5, & F_9 &= F_8 + F_7 = 34, \dots \end{aligned}$$

Existuje přímá souvislost mezi zlatým řezem a Fibonacciho posloupností, která není na první pohled patrná. Sblížené zlomky ϕ jsou totiž podíly po sobě jdoucích členů Fibonacciho posloupnosti: $\phi_m = \frac{p_m}{q_m} = \frac{F_{m+2}}{F_{m+1}}$, o čemž se snadno přesvědčíme:

$$\begin{aligned} \phi_0 &= [1] = \frac{F_2}{F_1} = \frac{1}{1}, & \phi_2 &= [1;1,1] = \frac{F_4}{F_3} = \frac{3}{2}, \\ \phi_1 &= [1;1] = \frac{F_3}{F_2} = \frac{2}{1}, & \phi_3 &= [1;1,1,1] = \frac{F_5}{F_4} = \frac{5}{3}, \dots \end{aligned}$$

Obecně pak získáváme limitu

$$\phi = \lim_{n\to\infty} \frac{F_{n+1}}{F_n}.$$

3.3.2 Ludolfovo číslo π

Již Archimedes ve 3. století před naším letopočtem omezil hodnotu $\sqrt{3}$ pomocí řetězových zlomků. Jeho motivací byla snaha o aproximaci π. Vyjádřil následující vztah:

$$\frac{265}{153} = \frac{1}{3}[5;5,10] < \sqrt{3} < \frac{1351}{780} = \frac{1}{3}[5;5,10,5].$$

Nyní víme, že řetězový zlomek čísla π má tvar

$$\pi = [3;7,15,1,292,1,1,1,2,1,3,1,14,2,1,1,2,2,2,2,\dots].$$

Z vysoké hodnoty prvku $a_4 = 292$ můžeme vyvodit, že již třetí sblížený zlomek nám poskytne velmi dobrou aproximaci π (čím vyšší je hodnota prvku řetězového zlomku, tím menší je význam jeho a prvků po něm následujících pro aproximaci daného čísla). Konkrétně se tato aproximace se skutečnou hodnotou π shoduje v prvních šesti desetinných číslech:

$$\pi_3 = [3; 7, 15, 1] = \frac{355}{113} \doteq 3,14159292.$$

Řetězový zlomek hodnoty π sice není periodický a neobsahuje žádný očividný vzor, výraz $\frac{4}{\pi}$ má ovšem zajímavější vlastnosti.

John Wallis jej rozepsal jako

$$\frac{4}{\pi} = \frac{3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 7 \cdot \ldots}{2 \times 2 \cdot 4 \cdot 4 \cdot 6 \cdot 6 \cdot \ldots}.$$

William Brouncker poté ukázal, že tento výraz je možné vyjádřit řetězovým zlomkem ve tvaru

$$\frac{4}{\pi} = 1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2 + \ddots}}}}.$$

M.A. Stern roku 1833 poté vyjádřil $\frac{\pi}{2}$ jako

$$\frac{\pi}{2} = 1 - \cfrac{1}{3 - \cfrac{2 \cdot 3}{1 - \cfrac{1 \cdot 2}{3 - \cfrac{4 \cdot 5}{1 - \cfrac{3 \cdot 4}{3 - \cfrac{6 \cdot 7}{1 - \cfrac{5 \cdot 6}{3 - \ddots}}}}}}}.$$

3.3.3 Eulerova konstanta e

Leonhard Euler dokázal, že konstantu $e \doteq 2,71828$, která nese jeho jméno, můžeme řetězovým zlomkem zapsat jako

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots] = [2; \overline{1, 2i, 1}]_{i \geq 1}.$$

Jedná se tedy o řetězový zlomek, v němž ke každému třetímu členu přičítáme hodnotu 2.

Euler využil tento rozvoj k důkazu, že e je iracionálním číslem. Jelikož navíc tento zlomek není periodický a víme, že každý periodický řetězový zlomek odpovídá druhé odmocnině nějakého kladného nečtvercového čísla, Euler usoudil, že i e^2 je iracionální.

Existuje více „hezkých“ reprezentací Eulerovy konstanty řetězovým zlomkem. Neomezujeme-li se na jednoduché řetězové zlomky (tedy povolíme-li ve jmenovateli výskyt i jiné hodnoty než 1), můžeme e vyjádřit jako

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{2}{3 + \cfrac{3}{4 + \cfrac{4}{5 + \ddots}}}}} = 2 + \cfrac{2}{2 + \cfrac{3}{3 + \cfrac{4}{4 + \cfrac{5}{5 + \cfrac{6}{6 + \ddots}}}}}.$$

I pro některé výrazy obsahující hodnotu e existují řetězové zlomky se zajímavými rozvoji. Můžeme si povšimnout opakovaného motivu přičítání stejné hodnoty pro každý třetí prvek:

$$\begin{aligned} \frac{e-1}{e+1} &= [0; 2, 6, 10, 14, 18, 22, \dots] \\ e - 1 &= [1; 1, 2, 1, 1, 4, 1, 1, 6, \dots] \\ \frac{1}{2}(e-1) &= [0; 1, 6, 10, 14, 18, 22 \dots] \end{aligned}$$

Euler také ukázal, že pro každé číslo $a \in \mathbb{N}$ má řetězový zlomek $e^{\frac{1}{a}}$ následující tvar:

$$e^{\frac{1}{a}} = [1; a-1, 1, 3a-1, 1, 1, 5a-1, 1, 1, \dots] = [1; \overline{(2i+1)a-1, 1, 1}]_{i \geq 1}.$$

Níže je uvedeno několik konkrétních příkladů:

$$\begin{aligned} e^{\frac{1}{2}} &= [1; 1, 1, 1, 5, 1, 1, 9, 1, 1, 13, \dots] & e^{\frac{1}{4}} &= [1; 3, 1, 1, 11, 1, 1, 19, 1, 1, 27, \dots] \\ e^{\frac{1}{3}} &= [1; 2, 1, 1, 8, 1, 1, 14, 1, 1, 20, \dots] & e^{\frac{1}{5}} &= [1; 4, 1, 1, 14, 1, 1, 24, 1, 1, 34, \dots] \end{aligned}$$

4 Řetězové zlomky jako nástroj reprezentace čísel

V úvodní kapitole jsme si představili mnohé vlastnosti řetězových zlomků, které naznačují výhodnost jejich použití v oproti dnes převládající poziční notaci.

Výhody reprezentace čísel řetězovými zlomky lze shrnout následujícími body:

- Snadná analýza chyb pomocí sblížených zlomků.
- Všechna racionální čísla můžeme reprezentovat exaktně. Pro srovnání můžeme uvést např. číslo $\frac{1}{10}$, které nemůže být v poziční notaci reprezentováno exaktně, jelikož má v binárním tvaru nekonečný periodický rozvoj: $0,000\overline{1100}$.
- Pro velké množství iracionálních čísel nabízejí jejich nejpřesnější možnou reprezentaci.
- Bez velkého úsilí dokážeme iterativně vygenerovat libovolně větší přesnost.
- Mají příznivé vlastnosti pro použití vlákny – není potřeba znát kompletní vstup pro vypočítání částečného výsledku.
- Nejsou závislé na žádné konkrétní číselné soustavě.

4.1 Úvahy o hardwarové implementaci řetězových zlomků

J.E. Robertson a K. S. Trivedi v článku [[12]] formulují tři fundamentální požadavky na alternativní reprezentaci čísel tak, aby byla možná její hardwarová implementace:

1. Převod do konvenční formy (čímž zde rozumíme poziční notaci) musí být nejen proveditelný, ale také co nejjednodušší. Množina možných výsledků musí odpovídat nějakému intervalu povolených hodnot, který je nepřerušovaný, tedy umožňuje výpočty s nekonečnou přesností. Pro aritmetiku s plovoucí řádovou čárkou je postačující požadavek, aby podíl horní a dolní meze tohoto rozsahu byl alespoň dva.
2. Každý ze sady používaných algoritmů by měl být snadno spustitelný pro zvolenou reprezentaci. Žádoucí je také kompatibilita mezi algoritmy ve smyslu sdílení hardwaru.
3. Jelikož většina algoritmů s výjimkou násobení vyžadují při absenci redundance existenci procedur „pokus-omyl“, musí být nalezena jednoduchá pravidla pro praktický výběr koeficientů.

Nabízí se možnost omezit se na jednoduché řetězové zlomky, tedy čitatel každého částečného podílu bude roven 1. Tímto je problém zredukován na vhodný výběr koeficientů a_i. Určíme podmínky, které budou platit pro množinu číslic, z níž vybíráme a_i:

a) Všechny prvky musí být ve tvaru 2^j, kde j je celé číslo.

b) Nechť rozsah hodnot, které můžeme reprezentovat jako nekonečné řetězové zlomky, je interval $[a, b]$. Požadujeme, aby tento rozsah byl kontinuem mezi a a b.

c) Interval $[\frac{1}{2}, 1]$ by měl být podintervalem intervalu $[a, b]$.

d) Kardinalita množiny číslic by měla být co nejmenší.

e) S touto množinou číslic by mělo být možné vyvinout proceduru

Množina $\{1; 2\}$ zjevně nesplňuje již podmínku b). Množina $\{1, \frac{1}{2}\}$ splňuje všechny podmínky kromě e). Množina $\{1, \frac{1}{2}, \frac{1}{4}\}$ splňuje všech pět podmínek.

Autoři docházejí k závěru, že výsledky teoretických pozorování jsou příznivé.

4.2 Gosperovy algoritmy

Aritmetické výpočty s řetězovými zlomky bez jejich převodu do poziční notace byly považovány za nemožné až do roku 1972, kdy Bill Gosper představil algoritmy, které to umožňují. Publikace [[1]], kde byly algoritmy poprvé popsány, je použita jako hlavní zdroj při psaní této podkapitoly. Detailnější popis fungování algoritmu je převzat ze zdroje [[6]].

Gosper popsal řetězový zlomek v jiné formě než v té, s kterou jsme pracovali dosud. Pohlížel na něj jako na objekt obsahující metodu, která při zavolání vždy vrátí na výstup následující člen zlomku a změní vnitřní stav objektu tak, aby při dalším zavolání mohla vrátit po něm následující člen. Objekt si tedy pamatuje, který člen byl vrácen na výstup při posledním volání. Tyto členy může mít buď uložené v paměti, nebo je může generovat na požádání. Druhá zmíněná varianta je výhodná, požadujeme-li pouze určitou přesnost výsledku. Nejsou zbytečně prováděny žádné výpočty, které nevyužijeme. Výpočty s nekonečnými řetězovými zlomky jsou možné, jelikož máme k nejvýznamnějšímu členu přístup jako první, a následující člen umíme z předchozích vygenerovat.

Na počátku je zlomek v základním tvaru $x = \frac{n}{d}$. Prvním členem, který bude vrácen na výstup, je $p = \lfloor \frac{n}{d} \rfloor$. Označíme si $x = p + \frac{1}{x'}$. Objekt mění svůj vnitřní stav na hodnotu $x' = \frac{n'}{d'} = \frac{1}{x-p}$. Další člen, který dostáváme na výstup, je $p' = \lfloor \frac{n'}{d'} \rfloor$, a tak stále dokola, dokud buď nedosáhneme požadované přesnosti, nebo nenarazíme na ukončovací podmínku: Je-li x celé číslo, pak zjevně $p = x$, a aktualizací stavu objektu bychom získali nedefinovanou hodnotu $x' = \frac{1}{x-p} = \frac{1}{0}$. Nastane-li tedy tento případ, víme, že byl na výstup vrácen poslední člen zlomku, a algoritmus končí.

Příklad 17

Na počátku je dán zlomek $\frac{9}{7} = [1; 3, 2]$. První prvek, který je vrácen na výstup, je

$$p = \left\lfloor \frac{n}{d} \right\rfloor = \left\lfloor \frac{9}{7} \right\rfloor = 1.$$

Víme, že $x = p + \frac{1}{x'}$. Změníme stav z x na

$$x' = \frac{n'}{d'} = \frac{1}{x - p} = \frac{1}{\frac{9}{7} - 1} = \frac{7}{2}.$$

Dalším prvkem, který je vrácen na výstup, je

$$p' = \left\lfloor \frac{7}{2} \right\rfloor = 3.$$

Změníme stav z x' na

$$x'' = \frac{n''}{d''} = \frac{1}{x' - p'} = \frac{1}{\frac{7}{2} - 3} = 2.$$

Na výstup při dalším zavolání vracíme prvek

$$p'' = \lfloor 2 \rfloor = 2.$$

Vidíme, že kdyby se nyní měl objekt x'' pomocí uvedeného vzorce dostat do nového stavu, získali bychom nedefinovanou hodnotu: $x''' = \frac{1}{2-2} = \frac{1}{0}$. Tímto víme, že běh algoritmu musí skončit, na výstup byly skutečně vráceny všechny prvky ŘZ $\frac{9}{7} = [1; 3, 2]$.

Jednodušším typem aritmetické operace je sčítání řetězového zlomku a racionálního čísla (reprezentovaného zlomkem ve tvaru $\frac{p}{q}$, kde $p \in \mathbb{Z}$, $q \in \mathbb{N}$), případně násobení řetězového zlomku racionálním číslem.

Definice 18 (Homografická funkce)

Homografickou funkcí nebo také **Möbiovou transformací** proměnné x rozumíme funkci ve tvaru

$$f(x) = y = \frac{ax + b}{cx + d},$$

kde a, b, c, d jsou celá čísla. Víme přitom, že pokud $a, b, c, d \geq 0$, pak medianta $\frac{a+c}{b+d}$ leží mezi hodnotami $\frac{a}{c}$ a $\frac{b}{d}$. Tuto funkci můžeme reprezentovat maticí ve tvaru $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Proměnnou x budeme rozumět objekt reprezentující řetězový zlomek tak, jak byl popsán výše. Objekt na zavolání vrátí na výstup člen p řetězového zlomku a změní svůj stav z x na x'. Dosazením výrazu $p + \frac{1}{x'}$ za x získáme rovnost

$$y = \frac{a(p + \frac{1}{x'}) + b}{c(p + \frac{1}{x'}) + d} = \frac{apx' + a + bx'}{cpx' + c + dx'} \longmapsto \begin{bmatrix} ap + b & a \\ cp + d & c \end{bmatrix}. \tag{2}$$

I homografickou funkci y zde chápeme jako objekt, který si uchovává svůj vnitřní stav a disponuje metodou, jejímž zavoláním je vrácen výstupní argument a vnitřní stav objektu y se změní na y'. Tento argument si označíme q a obecně se nerovná argumentu p. Obdobně jako u proměnné x platí vzorec

$$y = \frac{1}{y'} + q,$$

pomocí nějž můžeme aktualizovat původní předpis:

$$\begin{aligned} y' = \frac{1}{y - q} &= \left(\frac{ax + b}{cx + d} - q\right)^{-1} = \left(\frac{ax + b - cqx - dq}{cx + d}\right)^{-1} \\ &= \frac{cx + d}{(a - cq)x + b - dq} \longmapsto \begin{bmatrix} c & d \\ a - cq & b - dq \end{bmatrix}. \end{aligned} \tag{3}$$

Objekt y má tedy dvě možnosti. Buď má dostatek informací, aby vydal na výstup q, nebo požádá objekt x o další vstup p. Níže jsou možné situace znázorněny schématicky:

$$\begin{bmatrix} ap + b & a \\ cp + d & c \end{bmatrix} \xleftarrow{\text{vstup } p} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \xRightarrow{\text{výstup } q} \begin{bmatrix} c & d \\ a - cq & b - dq \end{bmatrix}$$

Víme, že hodnota y leží někde na intervalu $\left[\frac{a}{c}, \frac{b}{d}\right]$. Rovnají-li se celé části zlomků $\frac{a}{c}$ a $\frac{b}{d}$ (tzn. platí-li $\left\lfloor \frac{a}{c} \right\rfloor = \left\lfloor \frac{b}{d} \right\rfloor$), pak může y vrátit tuto hodnotu na výstup. V opačném případě potřebuje další informaci od x, čímž je zúžen interval, na němž se hodnota pohybuje.

Příklad 19

Máme ŘZ $x = \frac{17}{13} = [1; 3, 4]$ a chceme jej sečíst s hodnotou $\frac{1}{2}$. Položme si

$$y = x + \frac{1}{2} = \frac{2x + 1}{2} \longmapsto \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}.$$

Vidíme, že $\left\lfloor \frac{a}{c} \right\rfloor = \left\lfloor \frac{2}{0} \right\rfloor \neq \left\lfloor \frac{1}{2} \right\rfloor = \left\lfloor \frac{b}{d} \right\rfloor$, tedy y požádá x o vydání prvku $p = \lfloor x \rfloor = \left\lfloor \frac{17}{13} \right\rfloor = 1$ dle předpisu (2). Zároveň x aktualizuje svůj stav na $x' = \frac{1}{x - p} = \frac{1}{\frac{17}{13} - 1} = \frac{1}{\frac{4}{13}} = \frac{13}{4}$.

$$\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \xrightarrow{1} \begin{bmatrix} 2 \cdot 1 + 1 & 2 \\ 0 \cdot 1 + 2 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 2 & 0 \end{bmatrix}.$$

Stále platí $\left\lfloor \frac{a}{c} \right\rfloor = \left\lfloor \frac{3}{2} \right\rfloor \neq \left\lfloor \frac{2}{0} \right\rfloor = \left\lfloor \frac{b}{d} \right\rfloor$, tedy požádáme x' o další výstup $p' = \lfloor x' \rfloor = \left\lfloor \frac{13}{4} \right\rfloor = 3$, a stav x' změníme na $x'' = \frac{1}{x'-p'} = \frac{1}{\frac{13}{4}-3} = 4$.

$$\begin{bmatrix} 3 & 2 \\ 2 & 0 \end{bmatrix} \xrightarrow{3} \begin{bmatrix} 3 \cdot 3 + 2 & 3 \\ 2 \cdot 3 + 0 & 2 \end{bmatrix} = \begin{bmatrix} 11 & 3 \\ 6 & 2 \end{bmatrix}.$$

Zjistíme, že platí $\left\lfloor \frac{11}{6} \right\rfloor = 1 = \left\lfloor \frac{3}{2} \right\rfloor$. Objekt y tedy vrací tuto hodnotu jako výstup q a mění svůj stav na $y' = \frac{1}{y-q}$ dle vzorce (3):

$$\begin{bmatrix} 11 & 3 \\ 6 & 2 \end{bmatrix} \overset{1}{\Rightarrow} \begin{bmatrix} 6 & 2 \\ 11 - 6 \cdot 1 & 3 - 2 \cdot 1 \end{bmatrix} = \begin{bmatrix} 6 & 2 \\ 5 & 1 \end{bmatrix}.$$

Ověříme, že $\left\lfloor \frac{6}{5} \right\rfloor = 1 \neq 2 = \left\lfloor \frac{2}{1} \right\rfloor$, y' tedy žádá x'' o vydání dalšího členu $p'' = \lfloor 4 \rfloor = 4$. Zároveň vidíme, že stav x'' již nelze změnit, jelikož $\frac{1}{x''-p''} = \frac{1}{4-4} = \frac{1}{0}$, a tedy p'' je posledním členem řetězového zlomku $\frac{17}{13}$.

$$\begin{bmatrix} 6 & 2 \\ 5 & 1 \end{bmatrix} \xrightarrow{4} \begin{bmatrix} 6 \cdot 4 + 2 & 6 \\ 5 \cdot 4 + 1 & 5 \end{bmatrix} = \begin{bmatrix} 26 & 6 \\ 21 & 5 \end{bmatrix}.$$

Zjevně platí $\left\lfloor \frac{26}{21} \right\rfloor = 1 = \left\lfloor \frac{6}{5} \right\rfloor$, na výstup tedy vracíme hodnotu $q' = 1$ a změníme stav y' na y'':

$$\begin{bmatrix} 26 & 6 \\ 21 & 5 \end{bmatrix} \overset{4}{\Rightarrow} \begin{bmatrix} 21 & 5 \\ 26 - 21 \cdot 1 & 6 - 5 \cdot 1 \end{bmatrix} = \begin{bmatrix} 21 & 5 \\ 5 & 1 \end{bmatrix}.$$

Jelikož $\left\lfloor \frac{21}{5} \right\rfloor = 4 \neq 5 = \left\lfloor \frac{5}{1} \right\rfloor$, žádáme x''' o další vstup. Použijeme hodnotu $p = \infty$:

$$\begin{bmatrix} 21 & 5 \\ 5 & 1 \end{bmatrix} \xrightarrow{\infty} \begin{bmatrix} 21 \cdot \infty + 5 & 21 \\ 5 \cdot \infty + 1 & 5 \end{bmatrix} = \begin{bmatrix} 21 & 21 \\ 5 & 5 \end{bmatrix}.$$

Získáváme hodnotu $q'' = \left\lfloor \frac{21}{5} \right\rfloor = 4$, kterou vrátíme na výstup a změníme stav y'' na y''':

$$\begin{bmatrix} 21 & 21 \\ 5 & 5 \end{bmatrix} \overset{4}{\Rightarrow} \begin{bmatrix} 5 & 5 \\ 21 - 5 \cdot 4 & 21 - 5 \cdot 4 \end{bmatrix} = \begin{bmatrix} 5 & 5 \\ 1 & 1 \end{bmatrix}.$$

Nyní získáváme výstupní hodnotu $q''' = \left\lfloor \frac{5}{1} \right\rfloor = 5$, upravíme stav y''' na y'''':

$$\begin{bmatrix} 5 & 5 \\ 1 & 1 \end{bmatrix} \overset{5}{\Rightarrow} \begin{bmatrix} 1 & 1 \\ 5 - 1 \cdot 5 & 5 - 1 \cdot 5 \end{bmatrix} = \begin{bmatrix} 5 & 5 \\ 0 & 0 \end{bmatrix}.$$

Požádáme-li y'''' o další výstup, získáme výraz $\frac{1}{0}$, což je ukončovací podmínka, která nám dává vědět, že objekt vydal na výstup všechny prvky a výsledek je tímto kompletní.

Došli jsme k výsledku $[1; 3, 4] + \frac{1}{2} = [1; 1, 4, 5]$. Snadno ověříme, že výsledek je korektní.

Zatím jsme se seznámili s aritmetikou pro řetězový zlomek a racionální číslo. Chceme ovšem i sčítat a násobit řetězové zlomky mezi sebou. To je možné provést pomocí jejich převodu na **bihomografickou funkci**. Ta má tvar

$$f(x,y) = z = \frac{axy + bx + cy + d}{exy + fx + gy + h},$$

kde a až h jsou celá čísla a x, y pro nás budou dva řetězové zlomky. Funkci můžeme reprezentovat jako matici ve tvaru $\begin{bmatrix} a & b & c & d \\ e & f & g & h \end{bmatrix}$.

Obdobně jako v předchozím případě má objekt z na výběr z několika možností:

- Požádá objekt x o vypočítání výrazu p a jeho vydání na vstup:

$$\begin{bmatrix} a & b & c & d \\ e & f & g & h \end{bmatrix} \xrightarrow{p} \begin{bmatrix} c+ap & d+bp & a & b \\ g+ep & h+fp & e & f \end{bmatrix}$$

- Požádá objekt y o vypočítání výrazu q a jeho vydání na vstup:

$$\begin{bmatrix} a & b & c & d \\ e & f & g & h \end{bmatrix} \xrightarrow{q} \begin{bmatrix} b+aq & a & d+cq & c \\ f+eq & e & h+gq & g \end{bmatrix}$$

- Má dostatek informací pro to, aby vypočítal výraz r a vydal jej na výstup:

$$\begin{bmatrix} a & b & c & d \\ e & f & g & h \end{bmatrix} \xRightarrow{r} \begin{bmatrix} e & f & g & h \\ a-er & b-fr & c-gr & h-dr \end{bmatrix}$$

Nyní hledáme hodnotu $z = f(x,y)$ při ohodnocení dvou proměnných x, y, které se obě pohybují na intervalu $[0;\infty)$. To znamená, že z může nabývat hodnot z této čtvrtroviny.

Zajímá nás ovšem pouze to, jakých hodnot nabývá v krajních bodech čtvrtroviny, tedy $[\infty,\infty]$, $[0;\infty]$, $[\infty;0]$ a $[0;0]$, což jsou právě hodnoty $\frac{a}{e}$, $\frac{b}{f}$, $\frac{c}{g}$ a $\frac{d}{h}$. Shoduje-li se celá část ve všech těchto čtyřech bodech, z ji může dát na výstup. V opačném případě žádá o vstup x nebo y, a to následovně:

- Je-li $\left|\frac{b}{f} - \frac{d}{h}\right| > \left|\frac{c}{g} - \frac{d}{h}\right|$, požádá o vstup x.
- Je-li naopak $\left|\frac{c}{g} - \frac{d}{h}\right| > \left|\frac{b}{f} - \frac{d}{h}\right|$, požádá o vstup y.

Gosper navrhl, jakým způsobem zvolit hodnoty proměnných a až h tak, aby reprezentovaly jednotlivé aritmetické operace:

$$\text{sčítání} : x + y = \frac{x+y}{1} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$
$$\text{odčítání} : x - y = \frac{x+(-y)}{1} = \begin{bmatrix} 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$
$$\text{násobení} : x \cdot y = \frac{xy}{1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$
$$\text{dělení} : x/y = \frac{x}{y} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Problém Gosperových algoritmů leží v operacích s nekonečnými zlomky. Chceme-li např. vynásobit $\sqrt{2} = [1; 2, 2, 2, \dots] \times \sqrt{2} = [1; , 2, 2, 2, \dots]$, tento výpočet poběží donekonečna, aniž by vrátil na výstup jakoukoliv informaci. Otázka, zda prvním členem bude číslo 1 nebo 2, totiž záleží na všech členech rozvoje, kterých je nekonečně mnoho.

5 Útoky na šifru RSA

RSA je jednou z nejstarších v praxi používaných asymetrických šifer. Algoritmus byl představen roku 1977 jeho autory R. Rivestem, A. Shamirem a L. Adlerem. Přestože se v průběhu posledních desetiletí objevily různé pokusy o prolomení této šifry, při dodržení několika zásad je stále považována za bezpečnou a hojně využívána pro šifrování digitální komunikace (e-mail, VPN servery) či v elektronických podpisech.

5.1 Princip fungování RSA

Popis fungování šifry RSA je převzat z článku [[11]].

Spolehlivost RSA je založena na skutečnosti, že problém rozkladu velkého čísla na součin prvočísel je složitý (tzn. není znám algoritmus, který by jej řešil v polynomiálním čase), kdežto násobení dvou čísel je elementární úlohou.

Definice 20 (Eulerova funkce)
Pro číslo $n \in \mathbb{N}$ je hodnota Eulerovy funkce $\varphi(n)$ rovna počtu všech přirozených čísel menších než n, která jsou s ním vzájemně nesoudělná.

Pro prvočíslo p platí $\varphi(p) = p - 1$.

Jsou-li p, q prvočísla, pak pro $n = p \cdot q$ je $\varphi(n) = (p-1)(q-1)$.

Algoritmus RSA lze shrnout do několika kroků:

- Prvním krokem algoritmu je generování klíče. Příjemce náhodně zvolí dvě prvočísla p, q a vypočítá jejich součin $n = p \cdot q$. Čísla p a q by měla být přibližně stejně velká. V praxi se nejčastěji používají hodnoty v rozmezí 1024 až 3072 bitů. Čísla p, q přitom nesmějí být zveřejněna.

- Dále příjemce vypočítá hodnotu Eulerovy funkce $\varphi(n)$ a zvolí z množiny $\{1, 2, \ldots, \varphi(n)\}$ celé číslo e, které je s n nesoudělné. Toto číslo nazýváme *veřejným exponentem.*

- Pomocí rozšířeného Eukleidova algoritmu je nalezen tzv. inverzní prvek d čísla e modulo $\varphi(n)$, tedy musí platit $d \cdot e \equiv 1 \pmod{\varphi(n)}$.

- Dvojice (n, e) je *veřejným klíčem.* Získá-li potenciální útočník přístup k tomuto klíči, nedokáže pomocí něj zprávu jednoduše dešifrovat, a bezpečnost komunikace tedy není ohrožena. Číslo d je pak *soukromým klíčem* neboli *soukromým exponentem.* Ten nesmí příjemce zveřejnit.

- Odesílatel před šifrováním zprávu rozdělí na bloky m_i, přičemž pro jejich velikost platí $m_i < n$. Zprávu dále šifruje pomocí veřejného klíče:

$$c_i \equiv m_i^e \pmod{n}.$$

- Příjemce po obdržení bloky c_i kryptogramu dešifruje soukromým klíčem a získává tak bloky původní zprávy:

$$m_i \equiv c_i^d \pmod{n}.$$

Korektnost algoritmu je zaručena malou Fermatovou větou, která je specifikací Euler-Fermatovy věty.

Věta 21 (Euler-Fermatova věta)
Pro každé číslo $n \in \mathbb{N}$ a s ním nesoudělné číslo $a \in \mathbb{N}$ platí:

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Věta 22 (Malá Fermatova věta)
Pro každé číslo $a \in \mathbb{N}$ a prvočíslo p platí:

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

5.2 Wienerův útok

Roku 1990 popsal M. J. Wiener útok na šifru RSA, která využívá slabin tajného exponentu d. Tato podkapitola čerpá z Wienerova originálního článku [[17]].

Složitost procesu dešifrování je dána velikostí tajného klíče d. Čím menší je jeho velikost (řádově v bitech), tím rychleji proces dešifrování probíhá. Malou velikost exponentu je velmi vhodné zvolit v případě, kdy jsme si předem vědomi významného rozdílu mezi výpočetními silami dvou komunikujících zařízení, jako je např. čipová karta a větší počítač. Zde je vhodné zvolit kratší tajný exponent na straně karty a kratší veřejný exponent na straně počítače, abychom snížili výpočetní nárok na kartu.

Hlavní poznatky z Wienerova článku pak shrnuje následující věta:

Věta 23
Jsou-li v algoritmu RSA splněny následující podmínky:

- $q < p < 2q$
- $0 < e, d < \varphi(n)$
- $e \cdot d - k \cdot \varphi(n) = 1$
- $d < \frac{1}{3} n^{\frac{1}{4}}$,

  pak zlomek $\frac{k}{d}$ je sblíženým zlomkem řetězového zlomku $\frac{e}{n}$ a existuje algoritmus s časovou složitostí $O(\log(n))$, který z veřejného klíče (n, e) dokáže určit hodnoty p, q, d, k.

Důkaz

První část důkazu popisuje algoritmus hledání sblíženého zlomku $\frac{e}{n}$ a ukazuje jeho korektnost.

Logaritmická časová složitost algoritmu plyne ze skutečnosti, že řetězový zlomek rovný $\frac{e}{n}$ má $O(\log(n))$ sblížených zlomků.

Úpravou rovnosti $e \cdot d - k \cdot \varphi(n) = 1$ získáme následující vztah:

$$\frac{e}{\varphi(n)} - \frac{k}{d} = \frac{1}{d \cdot \varphi(n)}, \tag{4}$$

přičemž hodnota $\frac{1}{d \cdot \varphi(n)}$ je dostatečně malá.

Následující lemma je obměnou Věty 13:

Lemma 24

Pro řetězový zlomek $\alpha = [a_0; a_1, \ldots, a_n]$ *a libovolné číslo* $x \in \mathbb{N}$ *platí:*

$$[a_0; a_1, \ldots, a_n] < [a_0; a_1, \ldots, a_{n-1}, a_n + x] \text{ pro sudá } n,$$
$$[a_0; a_1, \ldots, a_n] < [a_0; a_1, \ldots, a_{n-1}, a_n + x] \text{ pro lichá } n.$$

Autor využívá algoritmu, který převádí reprezentaci racionálního čísla řetězovým zlomkem na jeho reprezentaci zlomkem $\frac{P}{Q}$, kde $P \in \mathbb{Z}$. $Q \in \mathbb{N}$.

Nechť α' je dolní odhad zlomku α, tedy pro nějaké $\delta \geq 0$ platí

$$\alpha' = \alpha(1 - \delta). \tag{5}$$

Pro $i \in \{0, 1, 2, \ldots\}$ si označme $i-$té členy zlomků α, α' jako a_i, resp. a'_i, jejich $i-$té zbytky pak r_i, resp. r'_i. Je-li hodnota δ dostatečně malá, lze čitatel a jmenovatel klasické reprezentace zlomku α získat následujícím postupem:

1. Nastav hodnotu i na 0.
2. Urči člen a'_i řetězového zlomku α'.
3. Vypočítej zlomek rovný

$$[a'_0; a'_1, \ldots, a'_{i-1}, a'_i + 1], \text{ je-li } i \text{ sudé},$$
$$[a'_0; a'_1, \ldots, a'_{i-1}, a'_i], \text{ je-li } i \text{ liché}.$$

4. Ověř, zda platí $\alpha' = \alpha$.
5. V kladném případě vrať čitatel a jmenovatel zlomku $\alpha' = \frac{p'_i}{q'_i}$, v záporném případě zvyš i o 1 a pokračuj instrukcí 2.

Algoritmus tedy vrací správný výsledek, jestliže je splněn následující vztah:

$$[a_0; a_1, \dots a_{n-1}, a_n - 1] < \alpha' \leq [a_0; a_1, \dots, a_n] \text{ pro sudá } n,$$
$$[a_0; a_1, \dots a_{n-1}, a_n + 1] < \alpha' \leq [a_0; a_1, \dots, a_n] \text{ pro lichá } n,$$

kde n je počet členů zlomku α. Správnost tohoto vztahu vychází z Lemmatu 24.

Stěžejní částí algoritmu je omezení přijatelné velikosti odchylky δ. Tu lze vyjádřit jako

$$\delta = 1 - \frac{\alpha}{\alpha'}. \tag{6}$$

Wiener zkoumal podobu této odchylky v závislosti na počtu n členů řetězového zlomku α. Problém si rozdělil na několik možných případů (jednotlivé postupy odvození zde z důvodu snahy o stručnost textu nejsou uvedeny, jsou ovšem dostupné v článku [17]):

1. $n = 0$:
$$\delta < \frac{1}{a_0}$$
2. $n = 1$:
$$\delta < \frac{1}{\frac{3}{2}P_1Q_1}$$
3. $n \geq 2$ a zároveň n je sudé:
$$\delta < \frac{1}{P_nQ_n}$$
4. $n \geq 3$ a zároveň n je liché:
$$\delta < \frac{1}{\frac{3}{2}P_nQ_n}.$$

Z porovnání všech možných případů vyplývá, že pro odchylku δ musí platit $\delta < \frac{1}{\frac{3}{2}P_nQ_n}$, kde P_n, Q_n jsou čitatelem a jmenovatelem n-tého sblíženého zlomku ŘZ α.

Význam výše odvozené odchylky δ pro možný útok na šifru RSA vysvětluje Wiener následovně:

V rovnosti
$$e \cdot d \equiv 1 \pmod{\varphi(n)}$$
můžeme dle [11] nahradit $\varphi(n)$ hodnotou $LCM(p-1, q-1)$, což je nejmenší společný násobek čísel $p-1$, $q-1$. Rovnost si tedy můžeme přepsat do tvaru

$$e \cdot d = K \cdot LCM(p-1, q-1) + 1,$$

kde $K \in \mathbb{Z}$.

Zároveň víme, že musí platit

$$LCM(p-1, q-1) \cdot GCD(p-1, q-1) = (p-1)(q-1),$$

kde $GCD(p-1, q-1)$ je největším společným dělitelem $p-1$, $q-1$. Tuto hodnotu si pro lepší přehlednost označíme proměnnou G.

Je nutné počítat s možností, že K a G mají netriviální společné dělitele. Vyjádříme si proměnné $k = \frac{K}{GCD(K,G)}$ a $g = \frac{G}{GCD(K,G)}$. Pak nutně $GCD(k, g) = 1$. Získáváme rovnost

$$e \cdot d = \frac{k}{g}(p-1)(q-1) + 1. \tag{7}$$

Obě strany získané rovnice lze vydělit výrazem $p \cdot q \cdot d$, čímž získáme na levé straně hodnotu $\frac{e}{pq}$, která je veřejně dostupnou informací ($p \cdot q = n$ a dvojice (n, e) je, jak víme, veřejným klíčem).

Tuto rovnost si pak můžeme přepsat na

$$\frac{e}{pq} = \frac{k}{gd}(1-\delta), \qquad \text{kde } \delta = \frac{p+q-1-\frac{g}{k}}{pq}. \tag{8}$$

Výraz $\frac{e}{pq}$ je dolním odhadem výrazu $\frac{k}{gd}$. Jelikož dle definice víme, že čísla k, g jsou vzájemně nesoudělná, a zároveň lze dokázat, že k, d jsou také vzájemně nesoudělná, pak i dvojice k, dg je nesoudělná, a tedy pro nalezení těchto hodnot lze využít výše představený algoritmus za předpokladu, že hodnota δ vyhovuje podmínce:

$$\delta < \frac{1}{\frac{3}{2}kdg}. \tag{9}$$

Předpokládáme-li, že výraz $-1 - \frac{g}{k}$ v čitateli δ má zanedbatelnou hodnotu, získáváme po jednoduchých úpravách nerovnost

$$kdg < \frac{pq}{\frac{3}{2}(p+q)}. \tag{10}$$

□

5.2.1 Korektnost výsledku

Správnost výsledného odhadu hodnot k, dg je snadné ověřit. Za předpokladu, že $ed > pq$ vyplývá z rovnice (7) vztah $k > g$. S jeho pomocí si tuto rovnici můžeme přepsat jako

$$edg = k(p-1)(q-1) + g. \tag{11}$$

Vydělíme-li obě strany rovnice proměnnou k, získáváme na pravé straně odhad $(p-1)(q-1)$ a zbytek $\frac{g}{k}$. Vyjde-li pak aproximace $(p-1)(q-1)$ rovna 0, víme, že odhady k a dg jsou nesprávné (algoritmus by vrátil výslednou faktorizaci n jako pq a 1 namísto p a q). Z odhadu $(p-1)(q-1)$ můžeme vyjádřit odhad $p+q$ pomocí následujícího předpisu:

$$\frac{pq - (p-1)(q-1) + 1}{2} = \frac{p+q}{2}. \tag{12}$$

Jelikož p, q jsou obě lichá, musí být výraz $\frac{p+q}{2}$ celé číslo. V záporném případě víme, že vrácený výsledek není správný. Dále z tohoto výrazu můžeme vyjádřit $(\frac{p-q}{2})^2$:

$$\left(\frac{p+q}{2}\right)^2 - pq = \left(\frac{p-q}{2}\right)^2$$

Je-li odhad $(\frac{p-q}{2})^2$ čtvercovým číslem, pak jsou odhady k a dg správné, a d vyjádříme jako podíl dg/g.

Wienerův útok je možné uskutečnit v časové složitosti polynomiální vůči velikosti modulu n. Lze jej ovšem uplatnit pouze v případě, kdy je velikost tajného exponentu d v bitech nanejvýše čtvrtinová oproti modulu n. V praktické implementaci RSA se ovšem nejčastěji setkáváme s případem, kdy jsou bitové velikosti d a n srovnatelné.

5.2.2 Wienerovy návrhy na vylepšení útoku

Wiener již ve svém původním článku navrhl několik možných strategií, jak zvýšit efektivitu útoku rozšířením povolené velikosti tajného exponentu d:

- Povolení algoritmu hledat d mírně větší, než je hodnota vyhovující nerovnosti (10). Algoritmus po přesáhnutí této hranice může fungovat korektně, není to ovšem zaručené. K tomuto nápadu se vrátili roku 2005 Stenfield et al.

- Zvolení těsnějšího horního odhadu hodnoty $\varphi(n) = (p-1)(q-1)$ než $n = pq$. Nabízí se využít výraz

  $$\lfloor(\sqrt{pq} - 1)^2\rfloor.$$

  V tomto případě bychom mohli nerovnost (10) přepsat jako

  $$kdg < \frac{2}{3}\left(\frac{\sqrt{pq}-1}{\sqrt{p}-\sqrt{q}}\right)^2. \tag{13}$$

  Díky této změně jsme schopni nalézt větší exponent d oproti původní verzi: jeho maximální velikost se zvyšuje s klesajícím rozdílem $|p-q|$. V dalších sekcích této kapitoly se seznámíme s několika dalšími pokusy o vylepšení aproximace $\varphi(n)$.

- Spuštění algoritmu pro větší množství odhadů $\frac{k}{dg}$, přičemž hodnoty těchto odhadů rostou. Při zachování nerovnosti (10) pracuje algoritmus v polynomiálním čase, po jejím porušení již počet provedených kroků roste exponenciálně.

- Snaha o nalezení hodnoty g nebo jejího prvočíselného rozkladu. Je-li t dělitelem g, pak

$$t\left(\frac{e}{pq}\right) \text{ je dolním odhadem } \frac{k}{d\left(\frac{g}{t}\right)}$$

a nerovnost (10) můžeme upravit na

$$kd\left(\frac{g}{t}\right) < \frac{pq}{\frac{3}{2}(p+q)}.$$

Tímto zvýšíme velikost exponentu d, který můžeme najít pomocí t. Prvočíselný rozklad g (a tedy i t) lze najít např. faktorizací $pq-1$, jelikož víme, že $g = GCD(p-1, q-1)$ a $pq-1 = (p-1)(q-1)+(p-1)+(q-1)$. V případě, že vychází g jako velká hodnota a jeho faktory jsou také velké, může být jeho faktorizace obtížná.

Autor sám došel k závěru, že každý z těchto postupů prakticky umožňuje provést útok na šifru RSA s exponentem d pouze o několik málo bitů větším oproti jeho původnímu omezení. Jeho nápady ovšem sloužily jako velmi užitečná inspirace pro směr, kterým se v budoucnosti ubíral výzkum.

5.3 De Wegerův útok

Informace prezentované v této podkapitole jsou čerpány z de Wegerova původního článku [[16]].

Přestože je pro optimální fungování šifry RSA žádoucí, aby prvočísla p, q byla přibližně stejně velká, příliš malý rozdíl mezi nimi může ohrozit bezpečnost šifry.

Je-li tento rozdíl $|p-q|$ menší než $cn^{\frac{1}{4}}$, kde c je hodnota konstantní vůči n, lze čísla p, q velice rychle nalézt **Fermatovou faktorizační metodou**. Ta hledá pro n přirozená čísla x, y tak, aby platilo $4n = x^2 - y^2$ (a zároveň $x \neq n+1, y \neq n-1$). Jestliže $n = pq$, pak získáme p, q jako $p = \frac{1}{2}(x+y)$, $q = \frac{1}{2}(x-y)$.

Hodnoty x, y pak nalezneme dosazováním $x = \lceil 2n^{\frac{1}{2}} \rceil + i$, kde $i \in \{0, 1, 2, \dots\}$, dokud není výraz $\sqrt{x^2 - 4n}$ celé číslo.

Programátoři jsou varováni před generováním prvočísel s příliš malým rozdílem. Např. standard ANSI X9.31 vyžaduje, aby se p a q lišila v prvních 100 bitech.

Za předpokladu, že p a q jsou bitově stejně velká, počet bitů obou je roven polovině velikosti n, a rozdíl mezi nimi má tedy velikost maximálně $n^{\frac{1}{2}}$. Jsou-li p a q generována náhodně, je velice vysoká pravděpodobnost, že tato velikost bude skutečně $n^{\frac{1}{2}}$.

Úspěch Wienerova útoku spočívá v nahrazení hledaného zlomku $\frac{e}{\varphi(n)}$ jeho aproximací $\frac{e}{n}$, tedy v relativně malém rozdílu mezi hodnotami n a $\varphi(n)$. De Weger zdokonalil tento odhad – došel k poznatku, že $n + 1 - 2n^{\frac{1}{2}}$ je pro hodnotu $\varphi(n)$ lepší aproximací než n, a tento výraz dále využíval ve svých výpočtech. Zároveň

se podivil nad zjištěním, že toto takřka banální vylepšení nebylo v dostupné literatuře v době publikace jeho článku dosud zmíněno.

De Wegerovo pozorování se opírá o následující jednoduché lemma:

Lemma 25
Jestliže $n = pq$ a $\Delta = p - q$, pak:

$$0 < (p+q) - 2n^{\frac{1}{2}} < \frac{\Delta^2}{4n^{\frac{1}{2}}}.$$

Důkaz

Víme, že platí vztah $\Delta^2 = (p+q)^2 - 4n = ((p+q) - 2n^{\frac{1}{2}})((p+q) + 2n^{\frac{1}{2}})$, tedy $p + q - 2n^{\frac{1}{2}} > 0$ a

$$p + q - 2n^{\frac{1}{2}} = \frac{\Delta^2}{p + q + 2n^{\frac{1}{2}}} < \frac{\Delta^2}{4n^{\frac{1}{2}}}.$$

□

Věta 26 (de Wegerův výsledek)
Nechť $\Delta = n^\beta$ pro $\beta \in \langle \frac{1}{4}, \frac{1}{2} \rangle$ a nechť $d = n^\delta$. Pak je možné aplikovat Wienerův útok na šifru RSA, pohybuje-li se δ na intervalu $\frac{3}{4} - \beta$.

Připomeňme, že toto je vylepšení oproti Wienerovu pozorování, kde musela být splněna podmínka $\delta < \frac{1}{4}$.

Důkaz

Na základě rovnosti

$$n + 1 - \varphi(n) = pq + 1 - (p-1)(q-1) = p + q$$

a Lemmatu 25 získáme nerovnici

$$0 < (n + 1 - 2n^{\frac{1}{2}}) - \varphi(n) < \frac{\Delta^2}{4n^{\frac{1}{2}}}. \tag{14}$$

Z rovnosti (4) si můžeme vyjádřit nerovnici:

$$\left| \frac{e}{n + 1 - 2n^{\frac{1}{2}}} - \frac{k}{d} \right| < e \left| \frac{1}{n + 1 - 2n^{\frac{1}{2}}} - \frac{1}{\varphi(n)} \right| + \left| \frac{e}{\varphi(n)} - \frac{k}{d} \right|.$$

Z této nerovnosti skutečnosti $e < \varphi(n)$ pak jsme schopni odvodit

$$\left| \frac{e}{n + 1 - 2n^{\frac{1}{2}}} - \frac{k}{d} \right| < \varphi(n) \frac{|(n + 1 - 2n^{\frac{1}{2}}) - \varphi(n)|}{(n + 1 - 2n^{\frac{1}{2}})\varphi(n)} + \frac{1}{\varphi(n)d}.$$

Nakonec s využitím vztahu (14) můžeme upravit pravou stranu nerovnosti:

$$\left| \frac{e}{n + 1 - 2n^{\frac{1}{2}}} - \frac{k}{d} \right| < \frac{1}{\varphi(n)} \left(\frac{\Delta^2}{4n^{\frac{1}{2}}} + \frac{1}{d} \right). \tag{15}$$

U každé prakticky použitelné varianty RSA lze předpokládat, že platí $\varphi(n) > \frac{3}{4}n$ a také $n > 8d$. Do nerovnosti (15) si tedy můžeme dosadit výrazy $\Delta = n^{\beta}$, $d = n^{\delta}$ a získáváme

$$\left|\frac{e}{n+1-2n^{\frac{1}{2}}} - \frac{k}{d}\right| < \frac{1}{3}n^{2\beta-\frac{3}{2}} + \frac{4}{3nd} < \frac{1}{3}n^{2\beta-\frac{3}{2}} + \frac{1}{6n^{2\delta}}. \tag{16}$$

Předpokládáme-li, že $2\beta - \frac{3}{2} < -2\delta$, tzn. $\delta < \frac{3}{4} - \beta$, potom dostaneme

$$\left|\frac{e}{n+1-2n^{\frac{1}{2}}} - \frac{k}{d}\right| < \frac{1}{2d^2}. \tag{17}$$

Jestliže je tedy splněna podmínka $\delta \in \frac{3}{4} - \beta$, pak je $\frac{k}{d}$ sblíženým zlomkem řetězového zlomku $\frac{e}{n+1-2n^{\frac{1}{2}}}$ a lze jej snadno nalézt. Znalost tajného exponentu d pak umožňuje kýženou faktorizaci n. □

5.4 Další vývoj a rozšíření Wienerova útoku

V nadcházejících letech se vědcům navazujícím na Wienerovu práci podařilo docílit zajímavých výsledků a rozšířit jeho útok či objevit některé jeho dosud nepopsané vlastnosti.

Níže představené výsledky není možné porovnat v rámci jejich významu pro bezpečnost šifry RSA. Každý z nich pohlíží na Wienerův útok z jiného úhlu a bylo jej dosaženo se specifickým teoretickým či praktickým cílem a s využitím jiných pomocných metod. Všechny jsou však v souladu s Wienerovým odkazem založeny na řetězových zlomcích.

5.4.1 Zobecnění Wienerova a de Wegerova výsledku

Jak již bylo v sekci 5.2 zdůrazněno, ne každá implementace šifry RSA je Wienerovým útokem napadnutelná. V praxi se velice často setkáváme s případem, kdy je tajný exponent d pro potřeby tohoto útoku příliš velký.

Roku 2004 přišli J. Blömer a A. May s nápadem, jak rozšířit interval, na kterém se hodnota d pohybuje. Jejich postup využívá metody D. Coppersmithe ([5]), s níž se v této práci nebudeme detailně seznamovat, jelikož nesouvisí přímo s řetězovými zlomky a využívá pokročilých algebraických metod. Zajímá nás pouze skutečnost, že tato metoda dokáže nalézt kořeny modulárních polynomických rovnic, a konkrétně pro šifru RSA to znamená, že jsme schopni nalézt prvočíselný rozklad n, známe-li alespoň polovinu bitů p (bráno zleva).

Zdrojem informací zpracovaných v této sekci je článek [[2]].

Autoři pracují s konceptem *slabých klíčů*. Obecně se jedná o dvojice veřejných klíčů (n, e), kde zvolená podoba klíče e usnadňuje rozklad klíče n na prvočísla.

Formálně jsou pak definovány následovně:

Definice 27 (Slabé klíče)
Nechť C je třída dvojic (n, e). *Velikostí* C rozumíme počet všech prvků e, které pro pevně dané n vyhovují potřebám RSA (tedy jsou nesoudělné s $\varphi(n)$).

Třída C se nazývá *slabou*, jestliže jsou splněny následující podmínky:

1. Velikost C je polynomiální vůči n.
2. Existuje pravděpodobnostní algoritmus, který pro každý vstup $(n, e) \in C$ vrací faktorizaci n v čase polynomiálním vůči $\log(n)$.

Prvky takové třídy označujeme jako *slabé klíče*.

V případě původního Wienerova útoku je pro tvůrce šifry snadné na první pohled určit, které z dvojic klíčů (n, e) jsou slabé: stačí prozkoumat několik prvních bitů tajného exponentu d. V zobecněné verzi, kterou Blömer s Mayem popisují, již není tato vlastnost zjevná.

Autoři využívají Coppersmithova výsledku prezentovaného v článku [[5]]:

Věta 28 (Coppersmith)
Nechť $n = pq$ je modulem šifry RSA a p, q jsou prvočísla stejné bitové délky. Předpokládejme, že máme aproximaci p s aditivní chybou o velikosti nejvýše $n^{\frac{1}{4}}$. Pak jsme schopni získat rozklad n na prvočísla v čase polynomiálním vůči $\log n$.

Následující věta shrnuje stěžejní poznatky Blömera a Maye:

Věta 29 (Zobecnění Wienerova výsledku)
Nechť $c \leq 1$ je reálné číslo a (n, e) je dvojice veřejných klíčů šifry RSA, kde $n = pq$ a $p - q \geq cn^{\frac{1}{2}}$. Předpokládáme, že $e \in \mathbb{Z}^*_{\varphi(n)}$ splňuje rovnici $ex + y = k\varphi(n)$, kde $x, y \in \mathbb{R}$ a zároveň

$$0 < x \leq \frac{1}{3} n^{\frac{1}{4}} \qquad a \qquad |y| \leq cn^{-\frac{3}{4}} ex.$$

Pak jsme schopni prvočíselný rozklad n nalézt v čase polynomiálním vůči $\log n$.

Důkaz
Důkaz věty je rozdělen na několik dílčích kroků. Prvním z nich je důkaz, že neznámé parametry k, x lze nalézt jako čitatel a jmenovatel nějakého sblíženého zlomku ŘZ $\frac{e}{n}$. Rovnici

$$ex + y = k(n - p - q + 1) \tag{18}$$

můžeme podělit proměnnou n a po provedení jednoduchých úprav získáváme

$$\frac{e}{n} - \frac{k}{x} = -\frac{k(p + q - 1) + y}{nx}. \tag{19}$$

Z rovnice (18) plyne, že každé číslo, které dělí zároveň x a k, musí být i dělitelem y. Vydělíme-li tuto rovnici hodnotou $GCD(x,k)$, získáme vztah $ex' + y' = 0 \pmod{\varphi(n)}$, kde $x' \leq x$, $y' \leq y$. Bez ztráty na obecnosti tedy můžeme předpokládat, že $\frac{k}{x}$ je zlomkem v základním tvaru.

Dosazením do Legendrovy věty 14 máme

$$\left|\frac{e}{n} - \frac{k}{x}\right| < \frac{1}{2x^2},$$

tedy s využitím rovnosti (19) musí platit

$$|k(p+q-1)+y| < \frac{n}{2x}.$$

Pokusíme se omezit hodnotu, kterou může nabývat parametr $k = \frac{ex+y}{\varphi(n)}$. Dle předpokladu $|y| \leq cn^{-\frac{3}{4}}$.

Beze ztráty na obecnosti můžeme předpokládat $n \geq (\frac{8}{c})^4$. Kdyby nerovnost neplatila, mohli bychom namísto Wienerova útoku využít Fermatovu faktorizaci.

Podmínka $n \geq (\frac{8}{c})^4$ implikuje $n \geq 2^{12}$, z čehož jsme schopni odvodit $|y| \leq \frac{1}{4}ex$. Získáváme tedy omezení

$$\frac{3}{4}\frac{ex}{\varphi(n)} \leq k \leq \frac{5}{4}\frac{ex}{\varphi(n)}. \tag{20}$$

Z této nerovnosti pak odvodíme

$$k(p+q-1)+y \leq \frac{15}{4}\frac{ex}{\varphi(n)} \cdot n^{\frac{1}{2}} + cn^{-\frac{3}{4}}ex \leq \frac{15}{4}xn^{\frac{1}{2}} + xn^{\frac{1}{4}} \leq 4xn^{\frac{1}{2}}, \tag{21}$$

předpokládáme-li stále $n \geq 2^{12}$.

Musí být tedy splněna podmínka $4xn^{\frac{1}{2}} < \frac{n}{2x}$, kterou můžeme přepsat jako $x < \frac{1}{\sqrt{8}}n^{\frac{1}{4}}$. Tento vztah je v souladu s omezením $x \leq \frac{1}{3}n^{\frac{1}{4}}$.

Víme tedy, že zlomek $\frac{k}{x}$ musí být sblíženým zlomkem řetězového zlomku $\frac{e}{n}$. Těchto zlomků je $\mathcal{O}(\log n)$.

Dalším krokem je dokázat, že správně nalezené hodnoty k, x umožňují faktorizaci n.

Rovnost (18) si můžeme přepsat jako

$$n + 1 - \frac{ex}{k} = p + q + \frac{y}{k}. \tag{22}$$

Jelikož parametry n, e, x, y jsou v tuto chvíli známé, jsme schopni vypočítat odhad součtu $p+q$, kde $\frac{y}{k}$ je aditivní chyba tohoto odhadu shora omezená hodnotou $\frac{4}{3}cn^{\frac{1}{4}}$, jak víme z nerovnosti (20).

Nyní je naším cílem nalézt aproximaci p, která umožní použití Coppersmithova algoritmu.

Víme, že ze součtu $p+q$ a hodnoty n umíme získat výraz $p-q$ využitím vzorce

$$p - q = \sqrt{(p-q)^2} = \sqrt{p^2 - 2pq + q^2} = \sqrt{(p+q)^2 - 4n}.$$

Odhad $p+q$ s maximální chybou $\frac{4}{3}cn^{\frac{1}{4}}$ si označíme jako s. V tom případě je $t = \sqrt{s^2 - 4n}$ odhadem $p - q$ s aditivní chybou shora omezenou $9n^{\frac{1}{4}}$.

Ověříme, že tento předpoklad je korektní. Musí platit $s^2 - 4n \geq 0$. Jelikož

$$s^2 - 4n = (p-q)^2 + 2\frac{y}{k}(p+q) + \left(\frac{y}{k}\right)^2,$$

stačí ukázat, že $|2\frac{y}{k}(p+q)| \leq (p-q)^2$. Víme, že platí $|\frac{y}{k}| \leq \frac{4}{3}cn^{\frac{1}{4}}$, a tedy $|2\frac{y}{k}(p+q)| \leq 8cn^{\frac{3}{4}}$. Podmínku $n \geq (\frac{8}{c})^2$ si můžeme přepsat jako $8 \leq c^{\frac{1}{4}}$, a tím získáváme $8cn^{\frac{3}{4}} \leq c^2 n \leq (p-q)^2$, což jsme chtěli dokázat.

Z předpokladu $n \geq 2^{12}$ plyne, že aditivní chyba $\frac{y}{k}$ je shora omezena $\frac{4}{3}cn^{\frac{1}{4}} \leq \frac{1}{2}n^{\frac{1}{2}} \leq \frac{1}{4}(p+q)$. Jelikož $s = (p+q) + \frac{y}{k}$, musí platit nerovnost

$$s \leq \frac{5}{4}(p+q). \tag{23}$$

Výraz $t - (p-q)$ si můžeme rozepsat jako

$$t - (p-q) = \sqrt{s^2 - 4n} - (p-q) = \frac{(s-(p+q))(s+(p+q))}{\sqrt{s^2-4n} + (p-q)}.$$

S využitím nerovností (23), $s - (p+q) \leq \frac{4}{3}cn^{\frac{1}{4}}$ a $p - q \geq cn^{\frac{1}{2}}$ konečně získáme požadovaný vztah:

$$t - (p-q) \leq \frac{\frac{4}{3}cn^{\frac{1}{4}} \cdot \frac{27}{4}n^{\frac{1}{2}}}{(p-q)} \leq 9n^{\frac{1}{4}}.$$

Z parametrů t a s získáme odhad p, jímž je $\frac{1}{2}(s+t)$, a maximální chybu vypočítáme jako

$$\left|\frac{1}{2}(s+t) - p\right| = \frac{1}{2}|s - p - q + t - p + q|$$

$$\leq \frac{1}{2}|s - (p+q)| + \frac{1}{2}|t - (p-q)| \leq \frac{2}{3}cn^{\frac{1}{4}} + \frac{9}{2}n^{\frac{1}{4}} \leq 6n^{\frac{1}{4}}.$$

Označíme si $\tilde{p} = \frac{1}{2}(s+t)$. Pak máme na výběr z právě šesti hodnot $k \in \{-3, -2, -1, 0, 1, 2\}$, které můžeme dosadit do předpisu $\tilde{p} + (2k+1)n^{\frac{1}{4}}$ a získat tak aproximaci p s maximální chybou $n^{\frac{1}{4}}$. Na všechny z nich je možné aplikovat Coppersmithův algoritmus, kterým získáme faktorizaci n v polynomiálním čase. □

Jsou-li splněny podmínky z Věty 29, algoritmus zobecněného Wienerova útoku lze shrnout následujícími kroky:

1. Urči řetězový zlomek odpovídající $\frac{e}{n}$.

2. Pro každý sblížený zlomek $\frac{k}{x}$ tohoto zlomku:

   a) Vypočítej $s = n + \frac{ex}{k}$, $t = \sqrt{s^2 - 4n}$, $\tilde{p} = \frac{1}{2}(s + t)$.

   b) Aplikuj Coppersmithův algoritmus na hodnoty $\tilde{p} + (2k+1)n^{\frac{1}{4}}$ pro $k \in \{-3, -2, -1, 0, 1, 2, 3\}$. Jestli algoritmus vrátil faktorizaci n (tedy čísla p, q), zastav.

Věta 30 (Zobecnění de Wegerova výsledku)
Nechť je dána dvojice veřejných klíčů (n, e) šifry RSA a $n = pq$. Předpokládejme, že e splňuje rovnost $ex + y = 0 \pmod{\varphi(n)}$, kde $x, y \in \mathbb{R}$, a zároveň

$$0 < x \leq \frac{1}{3}\sqrt{\frac{\varphi(n)}{e}}\frac{n^{\frac{3}{4}}}{p-q} \qquad a \qquad |y| \leq \frac{p-q}{\varphi(n)n^{\frac{1}{4}}} \cdot ex.$$

Pak jsme schopni prvočíselný rozklad n nalézt v čase polynomiálním vůči $\log n$.

Důkaz tvrzení je proveden obdobně jako u Věty 29 s rozdílem, že hodnota n je nahrazena $n' = n - \lfloor 2\sqrt{n} \rfloor$.

Analogicky lze pak sestavit i alternativní verzi zobecněného Wienerova algoritmu, kde v prvním kroku opět nahradíme hodnotu n hodnotou n' a hledáme sblížené zlomky ŘZ $\frac{e}{n'}$. Zbylé kroky algoritmu jsou již totožné s jeho původní verzí.

5.4.2 Verheul-van Tilborgovo vylepšení

Roku 1997 se E.R. Verheul a H.C.A. van Tilborg v článku [14] vrátili k Wienerově myšlence, která uvažuje možnost, že jeho útok je možné aplikovat i v případě, kdy bitová délka d těsně přesáhne mez $n^{\frac{1}{4}}$.

Informace představené v této sekci jsou čerpány z Verheulova a Tilborgova původního článku [[14]].

Nový útok je odpovědí na Wienerův nápad na vylepšení jeho vlastního algoritmu, kde autor navrhuje lineární prohledávání možných odhadů hodnoty $\frac{k}{dg}$. Algoritmus prohledává hrubou silou binární strom a provádí zhruba $\log_2 n \cdot 2^{2r}$ odhadů, kde $r = \log_2 (d/n)^{\frac{1}{2}}$.

Autoři využívají poznatků o řetězových zlomcích, z nichž většina byla představena v kapitole 2. Velká část jejich úvah se zabývá vzájemnou pozicí sblížených zlomků dvou racionálních čísel, která si spolu s jejich reprezentací řetězovými zlomky budeme ve zbytku této sekce značit jako $\alpha = \langle a_0; a_1, \ldots, a_m \rangle$, $\beta = \langle b_0; b_1, \ldots, b_n \rangle$, jejich i-té sblížené zlomky jako $\alpha_i = \frac{p_i}{q_i}$, resp. $\beta_i = \frac{u_i}{v_i}$.

Lemma 31
Nechť $\alpha_i = \frac{p_i}{q_i}$. Označme si $r_{i+1} = [a_{i+1}, a_{i+2}, \ldots, a_m]$. Pak pro $2 \leq i < m$ máme

$$\alpha = \frac{(a_i + \frac{1}{r_{i+1}})p_{i-1} + p_{i-2}}{(a_i + \frac{1}{r_{i+1}})q_{i-1} + q_{i-2}}.$$

Lemma 32

Nechť α, β jsou racionální čísla a $\alpha < \beta$. Pak platí $\alpha_i \leq \beta_i$ pro $0 \leq i \leq min(m, n)$. Navíc, je-li $m < i \leq n$, pak $\beta_i \geq \alpha$, a je-li $n < i \leq m$, pak $\alpha_i \geq \beta$.

Vracejí se k Wienerově rovnici (4).

Věta 33

Nechť $\frac{p_i}{q_i}$ je $i-$tým sblíženým zlomkem čísla α, a $\frac{x}{y}$ je zlomek, pro nějž platí

$$\left|\alpha - \frac{x}{y}\right| < \left|\alpha - \frac{p_i}{q_i}\right|.$$

Pak nutně platí $y > q_i$.

Věta 34

Nechť $\alpha = \langle a_0; a_1, \ldots, a_m\rangle$, $\beta = \langle b_0; b_1, \ldots, b_n\rangle$ jsou dvě reálná čísla a platí $\alpha < \beta$. Pak pro $0 \leq i \leq min(m, n)$ jsou následující podmínky ekvivalentní:

- $\alpha_i \neq \beta_i$
- $\beta_i \in (\alpha, \beta]$ *pro sudá* i, $\beta_i \in [\alpha, \beta)$ *pro lichá* i
- $|\beta - \beta_i| < |\beta - \alpha|$ *pro sudá* i, $|\alpha_i - \beta| < |\beta - \alpha|$ *pro lichá* i.

Právě ekvivalence první a třetí podmínky přináší možnost získat u šifry RSA informaci o tajném klíči d z dvojice veřejných klíčů (n, e).

Následující věta je základem Verheulových a van Tilbergových úvah:

Věta 35

Nechť α, β jsou dvě reálná čísla a číslo u je horní mezí $|\alpha - \beta|$. Nechť j je největším lichým indexem, pro nějž platí

$$|\beta - \alpha| \leq u \leq |\alpha_i - \alpha|. \tag{24}$$

Pak buď platí $\alpha_i = \beta$ nebo jsou si všechny prvky (a tedy i sblížené zlomky) řetězových zlomků α, β rovny až po j.

Navíc, je-li q_j jmenovatelem j-tého sblíženého zlomku α, pak nejvyšší index j', pro který platí

$$q_{j'} \leq \frac{1}{\sqrt{u}},$$

je dolní mezí j.

Níže představené lemma je pak užitečné pro aplikaci poznatků z Věty 35 v kontextu šifry RSA:

Lemma 36

Nechť $0 < \alpha < \beta$ a je dáno číslo δ tak, že platí $\alpha = (1-\delta)\beta$. Hodnoty δ_{max}, δ_{min} jsou horní, resp. nezáporná dolní mez δ. Pak

$$|\beta - \alpha| \leq \frac{\delta_{max}}{1 - \delta_{min}}, \tag{25}$$

$$\textit{jestli } \beta \leq 1, \ \textit{pak } |\beta - \alpha| \leq \delta_{max}. \tag{26}$$

Verheul a van Tilborg se vracejí k Wienerově rovnici (7) a dodávají, že v typickém systému RSA je hodnota proměnné g velice malá. Jsou-li navíc p, q silná prvočísla (tzn. každé z nich je dvojnásobkem nějakého prvočísla zvýšeným o jedničku), musí být g rovné buď 1, nebo 2.

Jelikož $\sqrt{2pq} \leq p + q$, podíl $\frac{\sqrt{2}}{\sqrt{n}}$ je vždy dolní mezí δ. Navíc za předpokladu $p < q$ je podíl $\frac{2}{p}$ horní mezí δ.

S využitím Věty 35 víme, že sblížené zlomky čísla $\frac{k}{dg}$ mohou být nalezeny až po řád j, kde počet bitů jmenovatele je roven zhruba čtvrtině počtu bitů modulu n.

Označíme si $\alpha = \frac{e}{pq}$, $\beta = \frac{k}{dg}$, kde $\alpha = [a_0; a_1, a_2, \dots]$, $\beta = [b_0; b_1, b_2, \dots]$, $\frac{p_i}{q_i}$ je i-tý sblížený zlomek α, $\frac{u_i}{v_i}$ je i-tý sblížený zlomek β. Předpokládejme, že u je horní mezí $|\beta - \alpha|$, pak přirozené číslo j je maximálním číslem, pro nějž platí

$$|\beta - \alpha| \leq u \leq |\alpha_j - \alpha|. \tag{27}$$

Jelikož $\alpha < \beta$, musí platit $a_{j+1} \leq b_{j+1}$. Označme si $b_{j+1} = a_{j+1} + \Delta$.

Dále si položme $s_{j+2} = [b_{j+2}, \dots, b_n]$. Nechť $s_{j+2} = \frac{U}{V}$, kde $U \geq V$ a U, V jsou vzájemně nesoudělná. Získáváme rovnost

$$b_{j+1} + \frac{1}{s_{j+2}} = a_{j+1} + \Delta + \frac{V}{U}.$$

Z nerovnosti (31) pak vyplývá

$$\begin{aligned} \frac{k}{dg} &= \frac{(a_{j+1} + \Delta + \frac{V}{U})p_j + p_{j-1}}{(a_{j+1} + \Delta + \frac{V}{U})q_j + q_{j-1}} = \frac{(a_{j+1}p_j + p_{j-1}) + (\Delta + \frac{V}{U})p_j}{(a_{j+1}q_j + q_{j-1}) + (\Delta + \frac{V}{U})q_j} \\ &= \frac{p_{j+1} + (\Delta + \frac{V}{U})p_j}{q_{j+1} + (\Delta + \frac{V}{U})q_j} = \frac{p_{j+1}U + (U\Delta + V)p_j}{q_{j+1}U + (U\Delta + V)q_j}. \end{aligned} \tag{28}$$

Předpokládáme, že čitatel a jmenovatel zlomku $\frac{k}{dg}$ na levé straně rovnosti (28) jsou vzájemně nesoudělné, tzn. jedná se o zlomek v základním tvaru. Náš předpoklad lze snadno ověřit s využitím Věty 10:

$$\begin{aligned} q_{j+1}k - p_{j+1}dg &= q_{j+1}(p_{j+1}U + (U\Delta + V)p_j) - p_{j+1}(q_{j+1}U + (U\Delta + V)q_j) \\ &= q_{j+1}(U\Delta + V)p_j - p_{j+1}(U\Delta + V)q_j \\ &= (U\Delta + V)(q_{j+1}p_j - p_{j+1}q_j) \\ &= \pm(U\Delta + V). \end{aligned} \tag{29}$$

Z výše vyjádřené rovnosti můžeme vyvodit, že každý společný dělitel k a dg (označíme si jej C) musí zároveň dělit $(\Delta U + V)$. Zároveň musí C dělit $p_{j+1}U$ a $q_{j+1}U$, a protože víme, že p_{j+1}, q_{j+1} jsou vzájemně nesoudělná čísla, znamená to, že C dělí U, a tedy dělí zároveň $(V + \Delta U) - \Delta U = V$. Jedinou možností tedy je, že $C = GCD(U, V) = 1$.

Na základě rovnosti (28) nám každý odhad Δ, V a U, kde $U \geq V$, dá i odhad $\frac{k}{gd}$, a Wienerovým testem dokážeme v polynomiálním čase ověřit, je-li tento výsledek správný, a v kladném případě obdržíme i hodnoty d, p a q.

Pro odhad $u = \frac{4}{\sqrt{n}}$ index j definovaný ve vztahu (27) splňuje

$$|x_{j+2} - x| < \frac{4}{\sqrt{n}}. \tag{30}$$

Z Věty 10, Lemmatu 31 a vztahu $a_{j+3} \leq r_{j+3} \leq a_{j+3} + 1$ můžeme vyvodit

$$\begin{aligned} |\alpha - \alpha_{j+2}| &= \left| \frac{r_{j+3}p_{j+2} + p_{j+1}}{r_{j+3}q_{j+2} + q_{j+1}} - \frac{p_{j+2}}{q_{j+2}} \right| = \left| \frac{p_{j+1}q_{j+2} - p_{j+2}q_{j+1}}{q_{j+2}(r_{j+3}q_{j+2} + q_{j+1})} \right| \\ &= \left| \frac{1}{q_{j+2}(r_{j+3}q_{j+2} + q_{j+1})} \right| \geq \left| \frac{1}{q_{j+2}((a_{j+3} + 1)q_{j+2} + q_{j+1})} \right|. \end{aligned} \tag{31}$$

Autoři dále využívají výsledků teorie pravděpodobnosti. Knuth v publikaci [[9]] zmiňuje, že v náhodném reálném čísle $\alpha = [a_0; a_1, a_2, a_3, \dots]$ můžeme pravděpodobnost, že se na a-té pozici vyskytuje číslice rovna a, vypočítat jako

$$\log_2\left(1 + \frac{1}{a}\right) - \log_2\left(1 + \frac{1}{(a+1)}\right) = \log_2 \frac{(a+1)^2}{(a+1)^2 - 1}.$$

Odsud získáváme výsledky:

1 se vyskytuje na 1. pozici s pravděpodobností $\log_2\left(\frac{4}{3}\right) \approx 41,504\%$;
2 se vyskytuje na 2. pozici s pravděpodobností $\log_2\left(\frac{9}{8}\right) \approx 16,993\%$;
3 se vyskytuje na 3. pozici s pravděpodobností $\log_2\left(\frac{16}{15}\right) \approx 9,311\%$;
4 se vyskytuje na 4. pozici s pravděpodobností $\log_2\left(\frac{25}{24}\right) \approx 5,889\%$;

$$\vdots$$

Jelikož $q_{j+2} = a_{j+2}q_{j+1} + q_j$, můžeme odhadnout q_{j+2} jako $2q_{j+1}$. Tedy pravá strana nerovnice (31) je zhruba $\frac{1}{10q_{j+2}^2}$. Ze vztahů (30) a (31) plyne, že s pravděpodobností zhruba 20 % je

$$\frac{4}{n^{\frac{1}{2}}} > |\alpha_{j+2} - \alpha| \geq \frac{1}{10} q_{j+1}^2.$$

Můžeme vyvodit, že $q_{j+1} > \frac{n^{\frac{1}{4}}}{7}$, neboli počet bitů hodnoty q_{j+1} je minimálně čtvrtina počtu bitů $n^{\frac{1}{4}}$ snížená o 3.

Ukázali jsme, že g je velmi malé, proto počet bitů dg je roven počtu bitů d zvýšenému o jedničku. Pro $d > n^{\frac{1}{4}}$ odhadli Verheul s van Tilborgem časovou složitost běhu jejich algoritmu následovně: Nechť

$$\log_2 d = \log n^{\frac{1}{4}} + r.$$

Z rovnosti (28) a předpokladu, že k a dg jsou vzájemně nesoudělná, můžeme vyvodit, že $q_{j+1}U$ je menší nebo rovno dg. Tedy $\lg U + \lg n^{\frac{1}{4}} - 3 \leq \lg n^{\frac{1}{4}} + x + 1$, a proto

$$\log_2 U \leq r + 4.$$

Vzhledem k tomu, že dle dohody $V \leq U$, tatáž nerovnost platí i pro V. Hodnota Δ je přitom malá. Víme, že $\Delta = b_{j+1} - a_{j+1}$, a tyto členy jsou s vysokou pravděpodobností opět malé. Navíc s pravděpodobností 50 % je poslední pozice, na které se částečné podíly α a β shodují, sudá, a v tom případě je Δ rovna 0. Celkově je množství informace potřebné k nalezení $\frac{k}{dg}$ (a tedy i d, p, q) zhruba $2r + 8$ bitů. Algoritmus Verheula a van Tilborga tedy přináší oproti Wienerovu návrhu $\log_2 n$-násobné zlepšení.

Dujella ([7]) prezentoval detailnější pohled na analýzu časové složitosti algoritmu Verheula a van Tilborga. Zanedbal parametry g, Δ vzhledem k jejich předpokládané malé velikosti, a vzorec (28) přeformuloval následovně:

$$\begin{aligned} k &= rp_{j+1} + sp_j \\ d &= rq_{j+1} + sq_j, \end{aligned}$$

kde r, s jsou přirozená čísla a zároveň platí $|p_{j+1}q_j - q_{j+1}p_j| = 1$. Jsou-li r, s dostatečně malá, jsme schopni je nalézt hrubou silou. Pokusíme se odhadnout počet kroků tohoto vyhledávání nalezením horních mezí r, s.

Položme si $D = \frac{d}{n^{\frac{1}{4}}}$.

Věta 37

$$\frac{1}{q_j(q_{j+1} + q_j)} < \left|\alpha - \frac{p_j}{q_j}\right| < \frac{1}{q_j q_{j+1}}. \tag{32}$$

Ze vztahu (32) vyplývá

$$r = dq_j \left(\frac{p_j}{q_j} - \frac{k}{d}\right).$$

Odhad s závisí na hodnotě výrazu $(\frac{e}{n} - \frac{p_{j+1}}{q_{j+1}}) - \frac{3\sqrt{2}}{2}\frac{e}{n\sqrt{n}}$.

Předpokládejme nejdříve $\frac{e}{n} - \frac{p_{j+1}}{q_{j+1}} > \frac{3}{\sqrt{22}}\frac{e}{n\sqrt{n}}$ (počítáme s tím, že tato možnost nastane v 50 % případů).

Jelikož

$$\frac{1}{q_{m+2}^2(a_{j+3}+2)} < \frac{p_{j+2}}{q_{j+2}} - \frac{e}{n} < \frac{3\sqrt{2}}{2}\frac{e}{n\sqrt{n}} < \frac{3\sqrt{2}}{2\sqrt{n}},$$

získáváme

$$q_{j+2} > \frac{n^{\frac{1}{4}}}{(\frac{3\sqrt{2}}{2}(a_{j+3})+2))^{\frac{1}{2}}}.$$

Navíc víme, že $q_{j+1} > \frac{q_{j+2}}{q_{j+2}+1}$. Propojením všech těchto znalostí dostaneme

$$r < \left(\frac{3\sqrt{2}}{2}(a_{j+3}+2)\right)^{\frac{1}{2}}(a_{j+2}+1)D,$$

$$s < \left(\frac{3\sqrt{2}}{2}(a_{j+3}+2)\right)^{\frac{1}{2}}D.$$

Tedy počet kroků algoritmu je pro tento případ shora omezen hodnotou

$$\frac{3\sqrt{2}}{2}(a_{j+3}+2)(a_{j+2}+1)D^2.$$

Nyní zanalyzujme druhý případ, tedy $\frac{e}{n} - \frac{p_{j+1}}{q_{j+1}} \leq \frac{3\sqrt{2}}{2}\frac{e}{n\sqrt{n}}$. V tom případě platí

$$s = dq_{j+1}\left(\frac{k}{d} - \frac{p_{j+1}}{q_{j+1}}\right) < dq_{j+1}\left(\frac{p_j}{q_j} - \frac{p_{j+1}}{q_{j+1}}\right) = \frac{d}{q_j}.$$

Jelikož je v tomto případě $\frac{p_{j+1}}{q_{j+1}}$ hodnota velmi blízká $\frac{e}{n}$, získáváme odhad q_{j+1} obdobně jako odhad q_{j+2} v případě předchozím:

$$q_{j+1} > \frac{n^{\frac{1}{4}}}{(\frac{3\sqrt{2}}{2}(a_{j+2}+2))^{\frac{1}{2}}}.$$

Máme

$$r < \left(\frac{3\sqrt{2}}{2}(a_{j+2}+2)\right)^{\frac{1}{2}}D,$$

$$s < \left(\frac{3\sqrt{2}}{2}(a_{j+2}+2)\right)^{\frac{1}{2}}(a_{j+1}+1)D$$

a počet kroků algoritmu je shora omezen hodnotou

$$\frac{3\sqrt{2}}{2}(a_{j+2}+2)(a_{j+1}+1)D^2.$$

Příklad 38

Ukážeme si, že Verheulův a van Tilborgův algoritmus může vrátit příznivé výsledky i při zvolení většího u, než je $\frac{4}{\sqrt{n}}$. Opět pro ilustraci vybíráme mnohem menší čísla než ta, která se používají v praktické implementaci šifry RSA.

Položme si $n = 3187766754862423734823 3$, $e = 711516780480876521 04$. Pak $u \doteq \frac{1}{\sqrt{n}} = \frac{1}{178543181187}$.

Pak největším lichým indexem i, pro nějž platí $u \leq |\alpha - \alpha_i|$, je 7. Vypočítáme si

$$\alpha_7 = \frac{1493}{6689},$$
$$\alpha_8 = \frac{34668}{155321}.$$
$$\alpha_9 = \frac{174833}{783294}.$$

Dosazením do vzorce (28) získáváme vztah

$$\frac{k}{dg} = \frac{34668U + (U\Delta + V)14399}{155321U + (U\Delta + V)6689}.$$

Nyní hrubou silou hledáme odpovídající hodnoty U, V a Δ, a Wienerovým testem ověřujeme správnost výsledku. Získáváme hodnoty $U = 21$ (5 bitů), $V = 5$ (3 bity), $\Delta = 0$, $g = 2$, $d = 1647593$ (21 bitů), $p = 119922166271$ (37 bitů), $q = 265819644023$ (38 bitů). Vidíme, že počet bitů d přesáhl $n^{\frac{1}{4}}$ o 2. Hrubou silou jsme hledali informaci o velikosti 8 bitů, což se shoduje s naším předpokladem. Navíc si můžeme povšimnout, že 9. sblížený zlomek $\frac{e}{n} = \alpha_9 = \frac{174833}{783294}$ se liší od odhadu $\frac{k}{dg} = \frac{140165}{627973}$, což znamená, že Wienerův algoritmus by zde selhal.

Za zmínku stojí nestandardní varianta šifry RSA, kde je veřejný exponent e zvolen úmyslně větší než n, což lze zařídit např. přidáním násobku hodnoty $LCM(p-1, q-1)$. Označíme jej $e = n^\theta$, kde $\theta > 1$. Pak z Lemmatu 36 vyplývá, že $n^{\theta-1,5}$ je horní mezí hodnoty $|\beta - \alpha|$. V případě, že $\theta > 1,5$, tento útok nefunguje (nevrací žádnou informaci o hodnotě d).

5.4.3 Dujellovo vylepšení

Roku 2004 navázal A. Dujella svou publikací [[7]] na práci Wienera a Verheula s van Tilborgem. Autor se vrátil k původnímu Wienerovu útoku a prezentoval myšlenku, že není nutné testovat všechny možné sblížené zlomky řetězového zlomku $\frac{e}{n}$ k nalezení d.

Informace uvedené v této sekci jsou čerpány z Dujellova článku [[7]].

Stejně jako Wiener předpokládejme $p < q < 2p$. Pak $\frac{(p+q)^2}{n} = \frac{p^2+q^2}{pq} + 2$, a tedy $2n^{\frac{1}{2}} < p + q < \frac{3\sqrt{n}}{2} n^{\frac{1}{2}}$. Z toho vyplývá

$$\frac{k}{d} - \frac{e}{n} = \frac{k(p+q) - k - 1}{dn} > \frac{2k(\sqrt{n}-1)}{dn}.$$

Jelikož $\frac{k}{d} > \frac{e}{n} \cdot \frac{n}{n-2\sqrt{n}+1}$, získáváme nerovnost

$$\frac{k}{d} - \frac{e}{n} > \frac{2e}{n\sqrt{n}} \tag{33}$$

a zároveň

$$\frac{k}{d} - \frac{e}{n} < \frac{3\sqrt{2}}{2}\frac{k}{d\sqrt{n}}.$$

Můžeme předpokládat, že $n > 10^8$. Tento předpoklad nás nijak neomezuje. Víme totiž, že jako modul n bývá v praxi voleno řádově mnohem větší číslo.

Na základě předchozích úvah a podmínky $p < q < 2p$ získáváme nerovnici

$$\frac{k}{d} - \frac{e}{n} < \frac{3\sqrt{2}}{2}\frac{e}{n\sqrt{n}} \tag{34}$$

a z nerovností (33) a (34) můžeme vyvodit, že $\frac{k}{d}$ je jediným sblíženým zlomkem ŘZ $\frac{e}{n}$ lichého řádu, který splňuje

$$\frac{2e}{n\sqrt{n}} < \frac{k}{d} - \frac{e}{n} < \frac{3\sqrt{2}}{2}\frac{e}{n\sqrt{n}}. \tag{35}$$

To je důsledkem skutečnosti, že jsou-li $\frac{p_m}{q_m}$, $\frac{p_{m+2}}{q_{m+2}}$ dva po sobě jdoucí sblížené zlomky reálného čísla α lichého řádu, pak je $\frac{p_{m+2}}{q_{m+2}}$ minimálně dvojnásobně lepší aproximací α než $\frac{p_m}{q_m}$.

Věta 39

Pro řetězový zlomek $\alpha = [a_0; a_1, \ldots, a_m, a_{m+1}, \ldots]$ a jeho sblížené zlomky $\frac{p_m}{q_m}$, $\frac{p_{m+1}}{q_{m+1}}$ platí

$$\frac{1}{q_m(q_{m+1}+q_m)} < \left|\alpha - \frac{p_m}{q_m}\right| < \frac{1}{q_m q_{m+1}}.$$

Dujella přichází s rozšířením Legendrovy věty:

Věta 40

Nechť α je iracionální číslo. Jsou-li x, y přirozená vzájemně nesoudělná čísla a platí-li

$$\left|\alpha - \frac{x}{y}\right| < \frac{c}{y^2}, \tag{36}$$

kde c je kladné reálné číslo, pak $(x, y) = (rp_{m+1} \pm sp_m, rq_{m+1} \pm sq_m)$ pro nezáporná celá čísla m, r, s a navíc platí $rs < 2c$.

Důkaz

Předpokládejme, že platí $\alpha < \frac{x}{y}$ (opačný případ je analogický). Nechť m je největší liché číslo splňující

$$\alpha < \frac{x}{y} \leq \frac{p_m}{q_m}$$

Definujeme si čísla r, s jako:

$$\begin{aligned} x &= rp_{m+1} + sp_m \\ y &= rq_{m+1} + sq_m \end{aligned}$$

Jelikož $|p_{m+1}q_m - p_m q_{m+1}| = 1$, můžeme předpokládat, že r a s jsou celá čísla, a jestliže $\frac{p_{m+1}}{q_{m+1}} < \frac{x}{y} \leq \frac{p_m}{q_m}$, pak $r \geq 0$ a $s > 0$.

Víme, že platí

$$\left|\frac{p_{m+2}}{q_{m+2}} - \frac{x}{y}\right| < \left|\alpha - \frac{x}{y}\right| < \frac{c}{y^2}$$

a zároveň

$$\begin{aligned} \left|\frac{p_{m+2}}{q_{m+2}} - \frac{x}{y}\right| &= \frac{(x_{m+2}q_{m+1} + q_m)(rp_{m+1} + sp_m) - (x_{m+2}p_{m+1} + p_m)(rq_{m+1} + sq_m))}{yq_{m+1}} \\ &= \frac{sx_{m+2} - r}{yq_{m+2}}. \end{aligned}$$

Z těchto dvou rovností vyplývá vztah

$$b(sx_{m+2} - r) < cq_{m+2} = \frac{c}{s}((sx_{m+2} - r)q_{m+1} + y),$$

z čehož můžeme úpravou získat nerovnost

$$(sx_{m+2} - r)(y - \frac{c}{s}q_{m+1}) < \frac{c}{s}y.$$

Navíc platí

$$\frac{1}{sx_{m+2} - r} > \frac{y - \frac{c}{s}q_{m+1}}{\frac{c}{s}y} = \frac{s}{c} - \frac{1}{r + \frac{sq_m}{q_{m+1}}} \geq \frac{s}{c} - \frac{1}{r}.$$

Získáváme kvadratickou nerovnost:

$$r^2 - srx_{m+2} + cx_{m+2} > 0. \tag{37}$$

Předpokládejme nyní, že $s^2x_{m+2} \geq 4c$. Pak $s^4x_{m+2}^2 - 4cs^2x_{m+2} \geq (s^2x_{m+2} - 4c)^2$, a proto z nerovnosti (37) vyplývá buď

$$r < \frac{1}{2s}(s^2x_{m+2} - \sqrt{s^4x_{m+2}^2 - 4cs^2x_{m+2}}) \leq \frac{2c}{s},$$

nebo

$$r > \frac{1}{2s}(s^2 x_{m+2} - \sqrt{s^4 x_{m+2}^2 - 4cs^2 x_{m+2}}) \geq \frac{1}{s}\left(s^2 x_{m+2} - 2c\right).$$

Z první možnosti získáváme předpoklad $rs < 2c$ zadaný dokazovanou větou. Vezměme v potaz druhou možnost, t.j. nerovnost

$$rs > s^2 x_{m+2} - 2c. \tag{38}$$

Definujme si proměnnou $t = sx_{m+2} - r$. Jelikož $\frac{p_{m+2}}{q_{m+2}} < \frac{a}{b}$, víme, že t je přirozené číslo. Nyní máme hodnoty x, y definované jako

$$x = rp_{m+1} + sp_m = (sx_{m+2} - t)p_{m+1} + sp_m = sp_{m+2} - tp_{m+1},$$
$$y = rq_{m+1} + sq_m = (sx_{m+2} - t)q_{m+1} + sq_m = sq_{m+1} - tq_{m+1}.$$

Tímto můžeme nerovnost (38) přepsat na $st < 2c$, a zadané tvrzení jsme dokázali pro $s^2 x_{m+2} \geq 4c$. Naopak platí-li $s^2 x_{m+2} < 4c$, máme díky vztahu $r < sx_{m+2}$ dvě možnosti:

1. Je-li $r < \frac{1}{2}sx_{m+2}$, pak platí $rs < \frac{1}{2}s^2 x_{m+2} < 2c$.
2. Je-li $r \geq \frac{1}{2}sx_{m+2}$, pak $t = sx_{m+2} - r \leq \frac{1}{2}sx_{m+2}$ a $st \leq \frac{1}{2}s^2 x_{m+2} < 2c$.

Tvrzení je dokázáno pro všechny případy, které mohou nastat. □

Dujellovo rozšíření Wienerova útoku se velmi podobá algoritmu Verheula a van Tilborga s tím rozdílem, že po získání startovního sblíženého zlomku využívá namísto vyhledávání hrubou silou odhady získané diofantickou aproximací.

Nechť j je největší liché přirozené číslo, které splňuje

$$\frac{p_j}{q_j} > \frac{e}{n} + \frac{3\sqrt{2}}{2}\frac{e}{n\sqrt{n}}.$$

Mohou nastat dvě možné situace: Nerovnost $\frac{p_{m+2}}{q_{m+2}} \geq \frac{k}{d}$ může a nemusí platit. Nejdřív budeme předpokládat, že podmínka je splněna.

Hledáme zlomek $\frac{k}{d}$ mezi zlomky ve tvaru $\frac{r'p_{j+3}+s'p_{j+2}}{r'q_{j+3}+s'q_{j+2}}$. Stejně jako v sekci 5.4.2 získáváme vztah

$$q_{j+2} > \frac{n^{\frac{1}{4}}}{(\frac{3\sqrt{2}}{2}(a_{j+3}+2))^{\frac{1}{2}}}.$$

Nyní dostáváme:

$$r' = dq_{j+2}\left(\frac{p_{j+2}}{q_{j+2}} - \frac{k}{d}\right) < dq_{j+2} \cdot \left(\frac{3\sqrt{2}}{2} - 1\right)\frac{e}{n\sqrt{n}} < \left(\frac{3\sqrt{2}}{4} - 1\right) dq_{j+2}\left(\frac{p_{j+2}}{q_{j+2}} - \frac{e}{n}\right)$$
$$< \left(\frac{3\sqrt{2}}{4} - 1\right)\frac{d}{q_{j+3}} < \left(\frac{3\sqrt{2}}{4} - 1\right)\frac{(\frac{3\sqrt{2}}{2}(a_{j+3}+2))^{\frac{1}{2}}}{a_{j+3}}D$$

a

$$s' = dq_{j+3}\left(\frac{k}{d} - \frac{p_{j+3}}{q_{j+3}}\right) \leq \left(\frac{p_{j+2}}{q_{j+2}} - \frac{p_{j+3}}{q_{j+3}}\right) = \frac{d}{q_{j+2}}$$
$$< (\frac{3\sqrt{2}}{2}(a_{j+3}+2))^{\frac{1}{2}}D.$$

Tedy jsme schopni nalézt hodnotu $\frac{k}{d}$ v maximálně $r's' < \frac{0{,}1295(a_{j+3}+2)}{a_{j+3}} \leq 0{,}3885D^2$ krocích, přičemž $D = \frac{d}{n^{\frac{1}{4}}}$.

Nyní předpokládejme $\frac{p_{j+2}}{q_{j+2}} < \frac{k}{d}$. Máme

$$\frac{k}{d} - \frac{e}{n} < \frac{3\sqrt{2}}{2}\frac{e}{n\sqrt{n}} < \frac{3\sqrt{2}}{2\sqrt{n}} = \frac{3\sqrt{2}D^2}{2d^2}.$$

Z Věty 40 vyplývá, že buď $\frac{k}{d} = \frac{rp_{j+1}+sp_j}{rq_{j+1}+sq_j}$, nebo $\frac{k}{d} = \frac{sp_{j+2}-tp_{j+1}}{sq_{j+2}-tq_{j+1}}$, kde r, s, t jsou přirozená čísla splňující $rs < 3\sqrt{2}D^2$, $st < 3\sqrt{2}D^2$.

Počet možných párů (r, s) a (s, t) je $\mathcal{O}(D^2 \log D)$. Tyto páry ovšem nejsou vybírány libovolně, splňují nerovnosti $r < a_{j+2}s$ a $t < a_{j+2}s$.

Označme si $A = max\{a_{j+i}\}$, kde $j \in \{1, 2, 3\}$. Pak je počet kroků Dujellova útoku $\mathcal{O}(D^2 \log A)$. Jedná se o zlepšení oproti Verheulovu a van Tilborgovu algoritmu představenému v předchozí sekci, který (použijeme-li stejné značení) dosahuje časové složitosti $\mathcal{O}(D^2A^2)$.

Dujella prakticky demonstroval úskalí snižující efektivitu Verheulova a van Tilborgova algoritmu. Ten vrací výsledky v přijatelném čase pouze v případě, že členy řetězového zlomku $\frac{e}{n}$ jsou dostatečně malé. Tento případ je obvyklý, ovšem nikoliv zaručený, jak se můžeme přesvědčit v následujícím příkladě:

Příklad 41

Nechť $n = 7978886869909$, $e = 4603830998027$ a $d < 10000000$. Řetězový zlomek $\frac{e}{n}$ je

$$[0, 1, 1, 2, 1, 2, 1, 18, 10, 1, 3, 3, 1, 6, 57, 2, 1, 2, 14, 7, 1, 2, 1, 4, 6, 2]$$

a sblížené zlomky jsou

$$\begin{array}{lll} \alpha_0 = 0, & \alpha_3 = \frac{3}{5}, & \alpha_6 = \frac{15}{26}, \\ \alpha_1 = 1, & \alpha_4 = \frac{4}{7}, & \alpha_7 = \frac{281}{487}, \\ \alpha_2 = \frac{1}{2} & \alpha_5 = \frac{11}{19}, & \alpha_8 = \frac{2825}{4896}, \end{array}$$

$$\vdots$$

Vidíme, že

$$\frac{281}{487} < \frac{e}{n} + \frac{3\sqrt{2}}{2}\frac{e}{n\sqrt{n}} < \frac{11}{19}.$$

Tedy $j = 5$, a tajný exponent d hledáme mezi hodnotami ve tvaru $26r + 19s$, $487s - 26t$, nebo $4896r' + 487s'$. Wienerovým testem pak zjistíme, že $s = 12195$ a $t = 77$ nám vrátí správný výsledek $d = 5936963$.

Porovnáme-li hodnoty s a t s čísly r a s vrácenými Verheulovým a van Tilborgovým algoritmem pro tentýž vstup, získáváme opět $s = 12195$, ovšem $r = 219433$ je větší než $t = 77$, což je v souladu s Dujellovým předpokladem. Vidíme tedy, že efektivita Dujellovy metody není závislá na dostatečně malé velikosti částečných podílů ŘZ $\frac{e}{n}$.

5.4.4 Útok Nassra et al.

Roku 2008 publikují D.I. Nassr, H.M. Bahig, A. Bhery a S.S. Daoud nově objevenou slabinu šifry RSA. Jejich článek [[10]] byl použit jako zdroj při psaní této sekce.

Autoři pro potřeby své práce formalizují Wienerův útok následovně:

Definice 42 (Wienerův útok)
Nechť m je reálné číslo a (n, e) je veřejným klíčem šifry RSA s tajným klíčem d, přičemž platí $ed - 1 = t\varphi(n)$. Pak definujeme **Wienerův útok** na trojici n, e, m, značeno $\mathrm{WA}(n, e, m)$, následovně:

$$WA(n, e, m) = \begin{cases} \frac{t}{d} & \text{je-li } \frac{t}{d} \text{ sblíženým zlomkem ŘZ } \frac{e}{m}; \\ \text{selhání} & \text{jinak.} \end{cases} \tag{39}$$

Jinými slovy, $WA(n, e, m)$ je úspěšný, vrací-li $\frac{t}{d}$. Je také možné útok zapisovat jako $\mathrm{WA}(n, e, m, C)$, kde C je souhrn doplňujících podmínek, které musejí být splněny (např. požadavky na vzájemný vztah čísel p, q).

Autoři dále definovali pojem **Wienerův interval**. Jedná se o interval, na němž se může pohybovat velikost tajného exponentu d tak, aby bylo možné úspěšně provést Wienerův útok (nejčastěji navíc v polynomiálním čase).

Definice 43 (Wienerův interval)
Nechť (n, e) je veřejný klíč šifry RSA. Pak interval $I \subset \mathbb{R}$ se nazývá **Wienerův interval**, jestliže je Wienerův útok úspěšný pro každé $m \in I$.

Autoři dále shrnuli několik podstatných vlastností Wienerova intervalu:

- Není-li řečeno jinak, na prvočíselný rozklad n se nevztahují žádná omezení, tedy Wienerův útok je možné aplikovat i na nestandardní verze šifry RSA (např. na verzi, kde $n = p^k r$).

- S rostoucím d se zmenšuje velikost I.
- Nechť $m = \varphi(n) + \epsilon, |\epsilon| < 1$. Jelikož je snadné ověřit, zda platí $\lfloor m \rfloor = \varphi(n)$ nebo ne, máme možnost omezit interval I následovně:

$$I = [\varphi(n) - \frac{\varphi(n)}{2d^2+1}, \varphi(n) - 1] \cup [\varphi(n) + 1, \varphi(n) + \frac{\varphi(n)}{2d^2-1}]. \tag{40}$$

Objev Nassra et al. je prezentován v následující větě:

Věta 44

Nechť $(n = pq, e)$ je dvojice veřejných klíčů šifry RSA s tajným exponentem $d = n^\delta$, kde $p > q$ a $2p < n - \frac{9}{4}\sqrt{n}$. Předpokládejme, že $p_0 \geq \sqrt{n}$ je aproximací p a platí $|p - p_0| \leq \frac{1}{8}n^\alpha$, $\alpha \leq \frac{1}{2}$ a $\delta < \frac{1-\alpha}{2}$. Pak je $[(n+1) - \lambda_1; (n+1) - \lambda_2]$ Wienerův interval pro (n, e), přičemž λ_1, λ_2 jsou definovány následovně:

$$\lambda_1 = \begin{cases} p_0 + \frac{n}{p_0} + \frac{1}{8}n^\alpha & \text{je-li } p_0 \leq p; \\ p_0 + \frac{n}{p_0 - \frac{1}{8}n^\alpha} & \text{je-li } p \leq p_0 \text{ a } \sqrt{n} \leq p_0 - \frac{1}{8}n^\alpha; \\ 2\sqrt{2} + \frac{1}{8}n^\alpha & \text{je-li } p \leq p_0 \text{ a } \sqrt{n} > p_0 - \frac{1}{8}n^\alpha. \end{cases} \tag{41}$$

$$\lambda_2 = \begin{cases} p_0 + \frac{n}{p_0 + \frac{1}{8}n^\alpha} & \text{je-li } p_0 \leq p; \\ \frac{n}{p_0} + p_0 - \frac{1}{8}n^\alpha & \text{je-li } p \leq p_0 \text{ a } \sqrt{n} \leq p_0 - \frac{1}{8}n^\alpha; \\ \sqrt{n} + \frac{n}{\sqrt{n} + \frac{1}{8}n^\alpha} & \text{je-li } p \leq p_0 \text{ a } \sqrt{n} > p_0 - \frac{1}{8}n^\alpha. \end{cases} \tag{42}$$

Pro $\frac{1}{4} < \alpha \leq \frac{1}{2}$ je věta rozšířením Coppersmithova výsledku 28.

Důkaz

Ukážeme, že $[n+1-\lambda_1, n+1-\lambda_2]$ je Wienerův interval tak, jak byl definován v (43). Podmínky je nutné ověřit pro všechny tři možné případy, které mohou nastat pro proměnné p, p_0:

1. Jestliže $p_0 \leq p$, pak

$$p_0 \leq p \leq p_0 + \frac{1}{8}n^\alpha$$

a zároveň

$$\frac{n}{p_0 q \frac{1}{8}n^\alpha} \leq q \leq \frac{n}{p_0}.$$

Tedy musí platit

$$\lambda_2 = p_0 + \frac{n}{p_0 + \frac{1}{8}n^\alpha} \leq p + q \leq \lambda_1 = p_0 + \frac{n}{p_0} + \frac{1}{8}n^\alpha.$$

Definujeme si interval $I_1 = [n + 1 - \lambda_1, n + 1 - \lambda_2]$. Jelikož $\varphi(n) = (p - 1)(q - 1) = n + 1 - (p + q)$, určitě můžeme předpokládat, že $\varphi(n) \in\in I_1$.

Nyní ukážeme, že $I_1 \subset I$ dle (40). Proměnnými l_1, resp. u_1 si označíme nejlevější a nejpravější bod intervalu I_1. Chceme tedy dokázat korektnost následujících nerovností:

$$l_1 = n + 1 - \lambda_1 > \varphi(n) - \frac{\varphi(n)}{2d^2 + 1},$$
$$u_1 = n + 1 - \lambda_2 < \varphi(n) + \frac{\varphi(n)}{2d^2 - 1}.$$

Víme, že platí

$$u_1 - l_1 = \frac{\frac{1}{8}n^{1+\alpha}}{p_0(p_0 + \frac{1}{8}n^\alpha)} + \frac{1}{8}n^\alpha \leq \frac{1}{4}n^\alpha$$

a

$$\frac{n}{2} < \frac{n}{2} + 1 \leq l_1, \text{ jelikož } 2p \leq n - \frac{9}{4}n^{\frac{1}{2}}.$$

Tím získáváme

$$u_1 \leq l_1 + \frac{1}{4}n^\alpha < l_1 + \frac{1}{4}n^{1-2\delta} = l_1 + \frac{\frac{n}{2}}{2d^2} < l_1 + \frac{l_1}{2d^2 - 1} \leq \varphi(n) + \frac{\varphi(n)}{2d^2 - 1}$$

a

$$l_1 \geq u_1 - \frac{1}{4}n^\alpha > u_1 - \frac{1}{4}n^{1-2\delta} = u_1 - \frac{\frac{n}{2}}{2d^2} > u_1 - \frac{\frac{n}{2} + 1}{2d^2 + 1} \geq u_1 - \frac{u_1}{2d^2 + 1}$$
$$\geq \varphi(n) - \frac{\varphi(n)}{2d^2 + 1}.$$

.

Tím jsme dokázali, že $I_1 = [l_1, u_1]$ je Wienerův interval pro (n, e).

2. Je-li $p \leq p_0$ a $\sqrt{n} \leq p_0 - \frac{1}{8}n^\alpha$, pak platí

$$\sqrt{n} \leq p_0 - \frac{1}{8}n^\alpha \leq p \leq p_0$$

a

$$\frac{n}{p_0} \leq q \leq \frac{n}{p_0 - \frac{1}{8}n^\alpha}.$$

Obdobně jako v prvním případě si označíme krajní body intervalu I_2 jako l_2, u_2. Pak získáváme

$$l_2 = n+1-(p_0+\frac{n}{p_0}-\frac{1}{8}n^\alpha) \leq \varphi(n) = n+1-p-q \leq u_2 = n+1-(\frac{n}{p_0}+p_0-\frac{1}{8}n^\alpha).$$

Nyní chceme ukázat, že $I_2 = [l_2, u_2]$ je Wienerův interval. Zjevně platí

$$u_2 - l_2 = \frac{\frac{1}{8}n^{1+\alpha}}{p_0(p_0 - \frac{1}{8}n^\alpha)} + \frac{1}{8}n^\alpha \leq \frac{1}{4}n^\alpha$$

a zároveň

$$\frac{n}{2} < l_2, \text{ jelikož } 2p \leq n - \frac{9}{4}\sqrt{n}.$$

Tedy získáváme

$$u_2 \leq l_2 + \frac{1}{4}n^\alpha < l_2 + \frac{1}{4}n^{1-2\delta} = l_2 + \frac{\frac{n}{2}}{2n^{2\delta}} < l_2 + \frac{l_2}{2d^2-1} \leq \varphi(n) + \frac{\varphi(n)}{2d^2-1}$$

a

$$\begin{aligned} l_2 &\geq u_2 - \frac{1}{4}n^\alpha > u_2 - \frac{1}{4}n^{1-2\delta} > u_2 - \frac{\frac{n}{2}+1}{2n^{2\delta}+1} \geq u_2 - \frac{l_2}{2d^2+1} \\ &\geq u_2 - \frac{u_2}{2d^2+1} \geq \varphi(n) - \frac{\varphi(n)}{2d^2+1}. \end{aligned}$$

Tímto jsme dokázali, že $I_2 = [l_2, u_2]$ je Wienerovým intervalem pro (n, e).

3. $p \leq p_0$ a $p_0 - \frac{1}{8}n^\alpha < \sqrt{n}$:
   Musí platit $p - \sqrt{n} < \frac{1}{8}n^\alpha$. Jelikož $\sqrt{n}$ je aproximace p, která odpovídá prvnímu případu, interval

$$[n+1-(2\sqrt{n}+\frac{1}{8}n^\alpha), n+1-(\sqrt{n}+\frac{n}{\sqrt{n}+\frac{1}{8}n^\alpha})]$$

   je Wienerovým intervalem pro (n, e). Tímto je tvrzení dokázáno pro všechny případy.

□

5.4.5 Tonien-Bunderův útok

S dosud nejnovějším průlomem přicházejí roku 2017 J. Tonien a M. Bunder. Článek [[4]], kde tento objev publikovali, byl využit jako zdroj při psaní této sekce.

Autoři ve své větě využívají následující pomocné lemma:

Lemma 45

Pro $n > 2000000$ *platí:*

$$\frac{(\frac{3}{\sqrt{2}} - 2)n^{\frac{1}{2}} + 4}{2(n - \frac{3}{\sqrt{2}}n^{\frac{1}{2}})^2} < \frac{1}{16n^{\frac{3}{2}}}. \tag{43}$$

Důkaz

Nerovnici (43) si můžeme upravit na

$$8n^{\frac{1}{2}}\left(\left(\frac{3}{\sqrt{2}} - 2\right)n^{\frac{1}{2}} + 4\right) < \left(n^{\frac{1}{2}} - \frac{3}{\sqrt{2}}\right)^2,$$

což odpovídá

$$(32 + 3\sqrt{2})n^{\frac{1}{2}} < (17 - 12\sqrt{2})n + \frac{9}{2}.$$

Po dosazení $n = 2000000$ snadno ověříme, že nerovnost je splněna. □

Hlavní výsledek Toniena a Bundera shrnuje následující věta:

Věta 46

Jestliže jsou v šifře RSA splněny následující podmínky:

- $q < p < 2q$
- $0 < e < \varphi(n)$
- $n > 2000000$
- $d < 2\sqrt{2}(\frac{n}{e})^{\frac{1}{2}}n^{\frac{1}{4}}$

a

$$n' = [n - \left(1 + \frac{3}{2\sqrt{2}}\right)n^{\frac{1}{2}} + 1],$$

pak $\frac{k}{d}$ *je sblíženým zlomkem ŘZ* $\frac{e}{n'}$ *a tedy můžeme z dvojice veřejných klíčů* (n, e) *získat informaci* p, q, d, k.

Důkaz

Položme si $\varphi_1 = (n + 1) - \frac{3}{\sqrt{2}}n^{\frac{1}{2}}$, $\varphi_2 = (n + 1) - 2n^{\frac{1}{2}}$. Jelikož $q < p < 2q$, a tedy $1 < \sqrt{\frac{p}{q}} < \sqrt{2}$, víme, že

$$2 < \frac{p+q}{n^{\frac{1}{2}}} = \sqrt{\frac{p}{q}} + \sqrt{\frac{q}{p}} < \sqrt{2} + \frac{1}{\sqrt{2}}.$$

Po vynásobení nerovnice výrazem $n^{\frac{1}{2}}$ získáváme

$$2n^{\frac{1}{2}} < p + q < \frac{3}{\sqrt{2}} n^{\frac{1}{2}}.$$

Zároveň víme, že pro $\varphi(n) = (p-1)(q-1)$ musí platit následující vztah:

$$\varphi_1 = (n+1) - \frac{3}{\sqrt{2}} n^{\frac{1}{2}} < \varphi(n) < (n+1) - 2n^{\frac{1}{2}}.$$

Nechť $\varphi_{mid} = n - (1 + \frac{3}{2\sqrt{2}})n^{\frac{1}{2}} + 1$ je středním bodem intervalu $[\varphi_1, \varphi_2]$, $n' = \varphi_{mid}$. Jelikož $\varphi(n) \in (\varphi_1, \varphi_2)$, máme

$$|\varphi(n) - n'| < |\varphi(n) - \varphi_{mid}| + |\varphi_{mid} - n'| < \frac{1}{2}(\varphi_2 - \varphi_1) + 1 = \frac{1}{2}(\varphi_2 - \varphi_1 + 2).$$

$$\left|\frac{e}{n'} - \frac{k}{d}\right| = \left|\left(\frac{e}{n'} - \frac{e}{\varphi(n)}\right) + \left(\frac{e}{\varphi(n)} - \frac{k}{d}\right)\right| = \left|\frac{e(\varphi(n) - n')}{n'\varphi(n)} + \frac{1}{d\varphi(n)}\right|$$

$$= \left|\frac{e(\varphi(n) - n')}{n'\varphi(n)} + \frac{e}{\varphi(n)(k\varphi(n)+1)}\right| < \frac{e|\varphi(n) - n'|}{n'\varphi(n)} + \frac{e}{\varphi(n)(k\varphi(n)+1)}$$

$$< \frac{e(\varphi_2 - \varphi_1 + 2)}{2\varphi_1^2} + \frac{e}{\varphi_1^2} < \frac{e(\varphi_2 - \varphi_1 + 4)}{2(\varphi_1 - 1)^2} = e\frac{(\frac{3}{\sqrt{2}-2})n^{\frac{1}{2}} + 4}{2(n - \frac{3}{\sqrt{2}}n^{\frac{1}{2}})^2}.$$

Díky Lemmatu 45 pak dostáváme

$$\left|\frac{e}{n'} - \frac{k}{d}\right| < \frac{e}{16n^{\frac{3}{2}}} < \frac{1}{2d^2},$$

čímž je důkaz dokončen. □

Na této podmínce je oproti ostatním rozšířením Wienerova útoku zajímavé, že závisí jak na tajném exponentu d, tak na veřejném exponentu e. Zjednodušeně lze tedy říci, že šifra RSA může být prolomena, je-li tajný exponent d nebo veřejný exponent e dostatečně malý. Původní Wienerův útok přitom nemůže být aplikován na implementaci RSA s (relativně) malým veřejným exponentem.

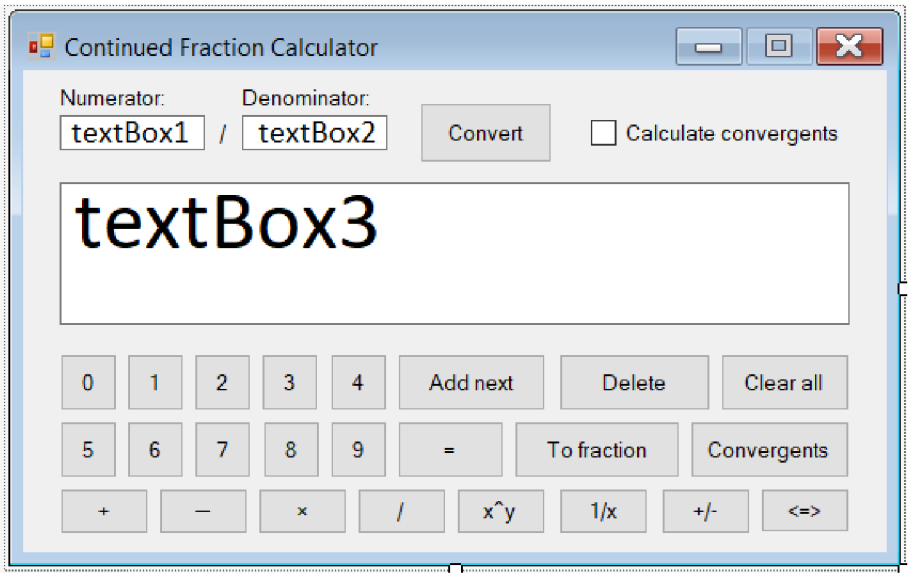
Poznamenejme, že ve Větě 46 můžeme poslední podmínku nahradit $d < 2\sqrt{2}n^{\frac{1}{4}}$, čímž se zbavíme členu e a zachováváme výrazné zlepšení oproti Wienerovu omezení $d < \frac{1}{3}n^{\frac{1}{4}}$.

Autoři experimentálně zjistili, že modul n o velikosti 1024 bitů je jejich algoritmus schopen faktorizovat v polynomiálním čase, pohybuje-li se d do velikosti 270 bitů. To je zlepšení oproti Wienerovu výsledku, u nějž je pro stejně velké n povolená velikost d shora omezena 255 bity.

6 Kalkulačka pro počítání s řetězovými zlomky

V praktické části práce byla implementována desktopová aplikace sloužící jako kalkulačka pro počítání s racionálními řetězovými zlomky. Technologiemi použitými pro implementaci programu byl jazyk C# s jeho rozšířením Windows Forms.

Aplikace umožňuje převod zlomku v základním tvaru na řetězový zlomek, výpočet sblížených zlomků a dále základní aritmetické operace s řetězovými zlomky.



Obrázek 2: Vzhled uživatelského rozhraní aplikace s označením textBoxů.

TextBox1 a textBox2 přijímají vstup z klávesnice. Povolené jsou kladné hodnoty v rozsahu 32-bitového integeru, tedy celá čísla na intervalu $\langle 0; 2147483647 \rangle$. Při zaškrtnutí kolonky **Calculate convergents** jsou navíc vypsány všechny sblížené zlomky výsledného řetězového zlomku.

Vstup do textBoxu3 uživatel vkládá pomocí tlačítek dostupných v uživatelském rozhraní (vstup z klávesnice tedy není umožněn). Automatické formátování vstupu zabraňuje vzniku chyb při jeho zadávání ze strany uživatele.

Tlačítko **Add next** slouží k zadání dalšího členu zlomku (nový člen bude od předchozího automaticky oddělen čárkou, případně středníkem).

Jsou implementovány následující operace pro řetězové zlomky:

- **sčítání** ve tvaru *zlomek1* + *zlomek2*
- **odečítání** v absolutní hodnotě: Je-li *zlomek1* větší než *zlomek2*
- **násobení** ve tvaru *zlomek1* * *zlomek2*
- **dělení** ve tvaru *zlomek1* / *zlomek2*
- **umocňování** ve tvaru *zlomek1* **1** *celé číslo*

- **obrácená hodnota** ve tvaru *zlomek1*$\hat{}$**(-1)**
- **porovnávání dvou zlomků** ve tvaru *zlomek1* <=> *zlomek2*

Nadbytečné nuly na počátku čísel jsou ignorovány.

Je-li výsledek poslední operace řetězový zlomek, program si jej uchovává v paměti a je tedy možné s ním dále pracovat.

Operand binární operace je možné měnit před započetím zadávání druhého argumentu.

Příklad **Delete** maže poslední člen posledního zadávaného zlomku či právě zadaný operand. Příkaz **Clear all** oproti tomu vymaže obsah všech textboxů a všechny uložené mezivýsledky.

Příkaz **To fraction** převede řetězový zlomek na reprezentaci zlomkem v základním tvaru.

Příkaz **Convergents** pro zadaný řetězový zlomek vypočítá všechny jeho sblížené zlomky.

Tlačítko +/- slouží k přepínání znaménka exponentu. Znaménko může být změněno kdykoliv do vyhodnocení operace.

Tlačítko = slouží k vyhodnocení momentálně zadávaného výrazu (tedy výsledku aplikace operace na zadané argumenty).

7 Závěr

Práce seznámila čtenáře s tématem řetězových zlomků, představila jejich nejdůležitější vlastnosti a význam v historii matematiky.

Bohužel se nejeví jako příliš pravděpodobné, že by v nejbližší době řetězové zlomky začaly být masově používány pro reprezentaci čísel jak v software, tak v hardware, a to navzdory jejich příznivým vlastnostem, kterými v mnoha ohledech převyšují dnes standardní poziční notaci. Dobrou zprávou ovšem je, že zlomky nacházejí využití v rozličných odvětvích informatiky. Útoky na šifru RSA s pomocí řetězových zlomků byly za posledních více než 30 let od představení Wienerova útoku zdokonalovány a dá se předpokládat, že jejich vývoj není u konce.

Literatura

[1] M. Beeler, R.W Gosper and R. Schroeppel. *HAKMEM (AI Memo 239)*. Tech. zpr. Cambridge, Massachussetts, USA: Massachusetts Institute of Technology, AI Laboratory, ún. 1972. 102 pp.

[2] Johannes Blömer and Alexander May. „A Generalized Wiener Attack on RSA“. In: *International Conference on Theory and Practice of Public Key Cryptography*. 2004, s. 1–13.

[3] Claude Brezinski. *History of Continued Fractions and Padé Approximants*. První vyd. Berlin: Springer-Verlag and Heidelberg, 1941. 551 pp.

[4] Martin Bunder and Joseph Tonien. „New attack on the RSA cryptosystem based on continued fractions“. In: *Malaysian Journal of Mathematical Sciences* 11 (srp. 2017), s. 45–57.

[5] Don Coppersmith. „Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities“. In: *Journal of Cryptology* 10 (1997), s. 233–260. DOI: 10.1007/s001459900030.

[6] Mark Jason Dominus. *Arithmetic with Continued Fractions*. 2006. URL: https://perl.plover.com/yak/cftalk/ (cit. 07/30/2023).

[7] Andrej Dujella. „Continued fractions and RSA with small secret exponent“. In: *Tatra Mt. Math. Publ.* 29 (břez. 2004), s. 101–112.

[8] A. J. Chinčin. *Řetězové zlomky*. První vyd. Praha: Přírodovědecké vydavatelství, 1952. 104 pp.

[9] Donald Knuth. *The Art of Computer Programming: Seminumerical Algorithms*. Druhé vyd. Roč. 2. New York: Addison-Wesley, 1981.

[10] Dieaa I. Nassr aj. „A new RSA vulnerability using continued fractions“. In: *2008 IEEE/ACS International Conference on Computer Systems and Applications*. 2008, s. 694–701. DOI: 10.1109/AICCSA.2008.4493604.

[11] R.L. Rivest, A. Shamir and L. Adleman. „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems“. In: *Communication of ACM* 21.2 (1978), s. 120–126.

[12] James E. Robertson and Kishor Trivedi. „The status of investigations into the use of continued fractions for computer hardware“. In: *1972 IEEE 2nd Symposium on Computer Arithmetic (ARITH)*. 1972, s. 1–30. DOI: 10.1109/ARITH.1972.6153902.

[13] Ron Steinfeld aj. „Converse Results to the Wiener Attack on RSA“. In: *Public Key Cryptography - PKC 2005* (2005), s. 184–198.

[14] Eric R. Verheul and Henk C.A. van Tilborg. „Cryptanalysis of ‘Less Short’ RSA Secret Exponents“. In: *Applicable Algebra in Engineering, Communication and Computing* 8 (čvc 1997), s. 425–435. DOI: 10.1007/s002000050082.

[15] Pavel Vít. *Řetězové zlomky*. První vyd. Roč. 49. Škola Mladých Matematiků. Praha: Mladá Fronta, 1982. 159 pp.

[16] Benne de Weger. „Cryptanalysis of RSA with Small Prime Difference“. In: *Applicable Algebra in Engineering, Communication and Computing* 13 (led. 2002), s. 17–28. DOI: 10.1007/s002000100088.

[17] Michael J. Wiener. „Cryptanalysis of Short RSA Secret Exponents“. In: *IEEE Transactions on Information Theory* 36 (1990), s. 553–558.