ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PEDAGOGICKÁ

KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

NĚKTERÉ METODY PRO PRVOČÍSELNÉ ROZKLADY

DIPLOMOVÁ PRÁCE

Bc. Zdeněk Šuster

Učitelství pro 2. stupeň ZŠ, obor Ma-Fy

Vedoucí práce: PhDr. Lukáš Honzík PhD.

Plzeň 2018

Prohlašuji, že jsem diplomovou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

Plzeň, 30. června 2018

.....

vlastnoruční podpis

Chtěl bych poděkovat svému vedoucímu diplomové práce PhDr. Lukáši Honzíkovi, PhD., za odborné vedení, pomoc a rady při zpracování této práce.

Zadání práce - bude vloženo

Obsah

Úvod **6**

Prvočíselný rozklad a jeho využití **7**

Prvočíslo 7

Prvočíselný rozklad 7

Způsoby zápisu prvočíselného rozkladu na základní škole 7

Tabulková způsob zápisu 7

Řádkový způsob zápisu 8

Grafický způsob zápisu 8

Eratosthénovo síto 9

Využití prvočíselného rozkladu 11

Kombinatorika 11

Největší společný dělitel 13

Nejmenší společný násobek 14

Představení vybraných algoritmů pro prvočíselný rozklad **15**

Faktorizace dělením („Hrubá síla“) 15

Pollardův rho algoritmus 16

Pollardův p - 1 algoritmus 19

Eulerova metoda 21

Ilustrační příklady práce vybraných algoritmů **24**

Faktorizace dělením („Hrubá síla“) 24

Pollardův rho algoritmus 26

Pollardův p - 1 algoritmus 36

Eulerova metoda 38

Krátké porovnání algoritmů po stránce jejich výpočetní náročnosti **41**

Faktorizace dělením („Hrubá síla“) 41

Pollardův rho algoritmus 41

Pollardův p - 1 algoritmus 42

Eulerova metoda 42

Porovnání algoritmů z hlediska časové náročnosti 42

Závěr **45**

Resumé **46**

Seznam obrázků **47**

Seznam použité literatury a webových zdrojů **48**

Úvod

U algoritmů a metod pro prvočíselný rozklad je důležitý pojem prvočíslo, který je rozebrán v první kapitole této práce. S prvočísly se žáci setkávají už na základní škole, kdy dojde k vysvětlení termínu prvočíslo a k jeho využití, a to nejčastěji pro znázornění prvočíselného rozkladu, který lze znázornit tabulkou, graficky či řádkově. O dalším využití prvočíselného rozkladu žáci získávají informace na střední a vysoké škole, jako například v kombinatorice, při výpočtu variací či kombinací, dále při výpočtech největšího společného dělitele a nejmenšího společného násobku. S prvočísly se pracuje také při sestavování Eratosthénova síta.

Tato práce se skládá ze čtyř kapitol, ve které jsou vysvětleny vybrané algoritmy či metody pracujících právě s prvočíselným rozkladem.

Právě ve druhé kapitole jsou představeny čtyři vybrané algoritmy pro prvočíselný rozklad. První metodou je tzv. hrubá síla, která se nejlépe využívá pro menší čísla jako i Eulerova metoda. Při použití větších čísel dochází k velmi časově náročnému výpočtu.

Dalšími důležitými algoritmy jsou Pollardovy algoritmy, konkrétně Pollardův rho algoritmus a Pollardův p - 1 algoritmus. Výstup těchto algoritmů je právě prvočíselný rozklad nějakého čísla N. Tyto algoritmy se dají využít pro velká čísla N.

Třetí kapitola se věnuje ukázce několika ilustračních příkladů ke každému algoritmu, a v poslední kapitole jsou zmíněna různá úskalí a nevýhody všech představovaných metod.

Poslední kapitola je zaměřená na krátké porovnání algoritmů z hlediska jejich výpočetní náročnosti.

1. Prvočíselný rozklad a jeho využití

Prvočíslo

Před vysvětlením prvočíselného rozkladu je důležité nejprve definovat pojem, který je pro prvočíselný rozklad zásadní. Tím je prvočíslo.

Prvočíslo je přirozené číslo, které je beze zbytku dělitelné pouze číslem jedna a sebou samým. Číslo 1 prvočíslem není, jelikož je dělitelné jen sebou samým, tj. jediným přirozeným číslem. Tudíž nejmenším prvočíslem je číslo 2, je dělitelné beze zbytku číslem 1 a 2. Je to zároveň jediné prvočíslo, které je sudé.

Všechna ostatní prvočísla jsou lichá, protože jakékoliv jiné sudé číslo je dělitelné kromě jedničky a sebou samým ještě právě dvojkou.

Prvočíselný rozklad

Prvočíselný rozklad se řídí dle základní věty aritmetiky, tj. každé přirozené číslo větší než jedna lze jednoznačně rozložit na součin prvočísel.

Potom tedy takovéto přirozené číslo můžeme nazvat složeným číslem.

Věta: Pro každé přirozené číslo m, kde $m > 1$, platí:

$$m = n_1 \cdot n_2 \cdot n_3 \cdot n_4 \cdot \ldots \cdot n_n$$

Př.) Rozložte číslo 24 na součin prvočísel.

$$24 = 2 \cdot 2 \cdot 2 \cdot 3$$

Na základní škole se tento rozklad vysvětluje žákům na základních třech metodách, a to tabulkové, řádkové a grafické.

Způsoby zápisu prvočíselného rozkladu na základní škole

Tabulkový způsob zápisu

U tabulkové metody se využívají dva sloupce, kde do levého sloupce jeho první řádky se napíše zadané číslo, které chceme rozložit na součin prvočísel. V pravém sloupci jsou zapsána prvočísla, kterými dělíme právě zadané prvočíslo. Po vydělení napíšeme výsledek

do druhého řádku levého sloupce a pokračujeme stejným způsobem do té doby, dokud se v levém sloupci neobjeví číslo 1.

Výše uvedený postup aplikujeme na rozkladu složeného čísla 24.

24	2
12	2
6	2
3	3
1	

Řádkový způsob zápisu

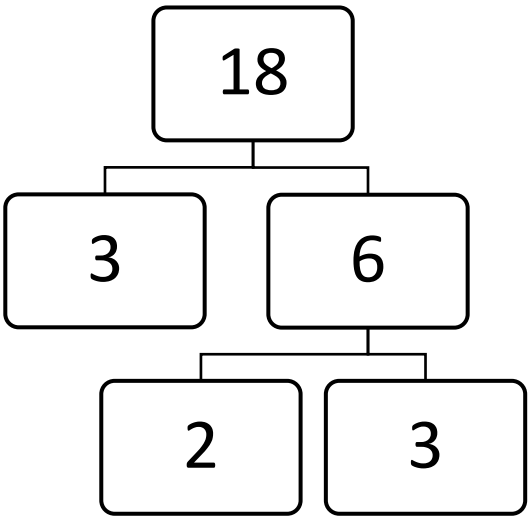
Jak už název vypovídá, budeme zapisovat postupný rozklad zadaného složeného čísla na součin prvočísel. Tudíž za zadané složené číslo, které chceme rozložit, napíšeme matematický symbol rovná se (=). Poté hledáme první prvočíslo, kterým lze vydělit zadané číslo. Po nalezení tohoto prvočísla provedeme zápis za symbol rovná se, kam zapíšeme součin nalezeného prvočísla a čísla, které vzešlo z podílu hledaného čísla a nalezeného prvočísla. Toto číslo se budeme snažit dále rozložit, tudíž budeme opět hledat takové prvočíslo, kterým lze vydělit právě zmiňované číslo. Tento proces opakujeme do té doby, než za symbolem rovná se budou jen samí prvočíselní dělitele. Ukážeme si tuto metodu na rozkladu složeného čísla 100.

$$100 = 2 \cdot 50 = 2 \cdot 2 \cdot 25 = 2 \cdot 2 \cdot 5 \cdot 5$$

Grafický způsob zápisu

Tato metoda se může také nazývat metodou stromu, kdy si pod zadané číslo, které chceme rozložit, ilustrujeme rozvětvení. Na levou stranu *„rozvětvení“* se zapisují vždy čísla s menší hodnotou, a na pravou stranu čísla s větší hodnotou. Tato čísla vzejdou z prvotního rozkladu. Pokud po prvním kroku rozkladu se nebudou nalézat pod rozvětvením prvočísla, opět následuje stejný postup, a to znázornění dalšího rozvětvení,

pod které se zapíší čísla, která vzešla z rozkladu daného čísla. Grafická metoda končí v tu chvíli, kdy pod všemi šipkami se nacházejí prvočísla.



Obrázek 1: Grafické schéma prvočíselného rozkladu

Eratosthenovo síto

Zmiňme také Eratosthenovo síto, které se přímo nezabývá prvočíselným rozkladem, ale jedná se o metodu výběru prvočísel.

Eratosthenés z Kyrény byl jedním z matematiků a fyziků antického Řecka. Jeho hlavním oborem, pro který vytvořil základy, byla geografie. Začal používat pojmy jako geografie, zeměpisná šířka a délka. Jak se zabýval matematikou a geografií, tak položil základy podoboru geografie, a to matematické geografii. Působil také jako správce proslulé Alexandrijské knihovny.

Tomuto starořeckému učenci je připisován algoritmus tzv. Eratosthenovo síto, které je datováno do roku 200 př. n. l. Jedná se jednu z metod, kterou lze použít na základní škole pro názornou ukázku nalezení prvočísel. Pro prvočísla vyšších hodnot můžeme použít jiných testů, jako Rabin-Millerův a Lehmannův test.

Eratosthenovo síto je metoda pro nalezení všech prvočísel menších než zadaná horní mez.

Kroky algoritmu:

a) Nejprve vypíšeme všechna čísla od čísla 2 do čísla *n*, a předpokládáme, že všechna jsou prvočísla.

b) Z tohoto seznamu čísel si vezmeme první prvočíslo, tj. číslo 2. Víme, že všechny další násobky prvočísla 2 nemohou být z definice prvočíslem, tudíž je vyškrtneme.

c) Nyní si vezmeme další prvočíslo, které následuje po číslu 2, tj. číslo 3, a vyškrtáme opět jeho násobky.

d) V posledním kroku opakujeme krok c), dokud nedojdou v seznamu čísel všechny násobky prvočísel.

Čísla ověřujeme jen do odmocniny horní meze $\sqrt{n}$.

Př.) Najděte všechna prvočísla do 20.

a) Vypíšeme si do tabulky všechny čísla od 2 do čísla *n* = 20.

	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20

b) Odstraníme z tabulky násobky prvočísla 2.

	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20

c) Určíme další prvočíslo, tj. číslo 3, a odstraníme jeho násobky.

	2	**3**	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20

d) V tomto kroku předchozí krok opakovat nemusíme, jelikož následující prvočíslo $5 > \sqrt{n}$. Tím pádem se v seznamu čísel nenachází žádné složené číslo, které můžeme rozložit na součin.

	2	**3**	
5		**7**	
		11	
13			
17		**19**	

Pomocí těchto osmi prvočísel a metody faktorizace dělením si můžeme ověřit, zda se jedná o prvočíslo nebo číslo složené až do hodnoty 400.

Využití prvočíselného rozkladu

Prvočíselný rozklad můžeme využít v řadě odvětví matematiky jako například v kombinatorice, při výpočtech největšího společného dělitele a nejmenšího společného násobku.

1) Kombinatorika

I v oblasti matematiky, jako je kombinatorika, můžeme nalézt využití prvočíselného rozkladu.

S prvočíselným rozkladem se můžeme setkat při zjišťování n prvků, které tvoří daný počet skupin k-té třídy. V následujících příkladech si ukážeme využití u kombinací a variací bez opakování.

Př.) Četa vojáků má vyslat na stráž 4 muže. Kolik mužů má četa, je-li možno úkol splnit 210 způsoby?

U tohoto příkladu se bude jednat o kombinace bez opakování, a budeme zde hledat určitý počet *n* prvků 4-té třídy, což čítá počet vojáků vyslaných na stráž. Nyní provedeme zápis pro kombinace bez opakování.

$$C_4(n) = 210$$

Z výše uvedeného vztahu vyplývá následující vztah, kdy se kombinační číslo rovná číslu 210.

$$\binom{n}{4} = 210$$

Poté si dané kombinační číslo rozepíšeme do tvaru zlomku, který je roven číslu 210.

$$\frac{n!}{4! \cdot (n-4)!} = 210$$

S využitím faktoriálu budeme provádět následné úpravy, pomocí kterých dospějeme k výsledku.

$$\frac{n \cdot (n-1) \cdot (n-2) \cdot (n-3) \cdot (n-4)!}{4! \cdot (n-4)!} = 210$$

$$n \cdot (n-1) \cdot (n-2) \cdot (n-3) = 5040$$

$$5040 = 2^4 \cdot 3^2 \cdot 5 \cdot \mathbf{7}$$

Následně si upravíme čísla z rozkladu v součin čtyř po sobě jdoucích přirozených čísel.

$$5040 = 10 \cdot 9 \cdot 8 \cdot 7$$

$$\boldsymbol{n = 10}$$

Četa má celkem 10 mužů při splnění jejího vyslání 210 způsoby.

Př.) Do školského výboru se vybírají předseda, místopředseda, tajemník a pokladník celkem 840 způsoby. Ze skupiny kolika žáků lze zvolit do tohoto výboru výše zmiňované pozice?

Jedná se o variace bez opakování, tudíž si pro ně zapíšeme ze zadání zápis.

$$V_4(n) = 840$$

$$\frac{n!}{(n-4)!} = 840$$

Pomocí faktoriálu budeme provádět následné úpravy, pomocí kterých dospějeme k výsledku.

$$\frac{n \cdot (n-1) \cdot (n-2) \cdot (n-3) \cdot (n-4)!}{(n-4)!} = 840$$

$$n \cdot (n-1) \cdot (n-2) \cdot (n-3) = 840$$

$$840 = 2^3 \cdot 3 \cdot 5 \cdot \mathbf{7}$$

Následně si upravíme čísla v součin čtyř po sobě jdoucích přirozených čísel.

$$840 = 7 \cdot 6 \cdot 5 \cdot 4$$

$$\boldsymbol{n = 7}$$

Skupina, ze které se vybírají kandidáti do školské výboru, má 7 členů.

2) Největší společný dělitel

Největším společným dělitelem vybraných dvou a více celých čísel, která jsou nenulová, je největší kladné číslo, které dělí každé vybrané celé číslo.

Př.) Dřevěný kvádr s rozměry 72 cm, 48 cm a 30 cm se má rozřezat na co nejmenší počet shodných krychlí. Vypočítejte délku hran krychlí a jejich počet

Nejprve si všechny tři rozměry rozložíme na součin prvočísel pomocí řádkové metody:

72 = 2 · 36 = 2 · 2 · 18 = 2 · 2 · 2 · 9 = 2 · 2 · 2 · 3 · 3

48 = 2 · 24 = 2 · 2 · 12 = 2 · 2 · 2 · 6 =2 · 2 · 2 · 2 · 3

30 = 2 · 15 = 2 · 3 · 5

Poté si ze všech řádků zapíšeme ta prvočísla, která se vyskytují ve všech rozkladech, a tím zjistíme největší společný dělitel tří čísel.

$D(72, 48, 30) = 2 \cdot 3 = 6$

Tudíž největším společným dělitelem čísel 72, 48 a 30 je číslo 6. To znamená, že délka hrany krychle bude 6 cm.

Poté si dopočteme na kolik shodných krychlí se zadaný kvádr rozřeže. Zde už ale nebude používat prvočíselný rozklad.

Mějme tedy počet shodných krychlí x.

$x = (72 : 6) \cdot (48 : 6) \cdot (30 : 6) = 12 \cdot 8 \cdot 5 = 480.$

Kvádr tedy můžeme rozřezat na 480 shodných krychlí.

3) Nejmenší společný násobek

Nejmenším společným násobkem několika zadaných čísel je nejmenší kladné celé číslo, které je celočíselným násobkem všech daných čísel.

Př.) Na přehradě jezdí tři okružní parníky s trasami o délce trvání 75 minut, 30 minut a 60 minut. Pokud všechny tři parníky vyjedou současně z přístaviště v 8 hodin, v kolik hodin se nejdříve opět v přístavišti setkají?

Nyní si všechny tři časové údaje rozložíme na součin prvočísel pomocí tabulkové metody:

75	3
25	5
5	5
1	

30	2
15	3
5	5
1	

60	2
30	2
15	3
5	5
1	

Z výše uvedených tabulek si vypíšeme nejvyšší mocniny nacházejících se v prvočíselných rozkladech čísel. Následným součinem těchto násobků pak zjistíme nejmenší společný násobek.

$n(75, 30, 60) = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 300$

Parníky se znovu setkají za 300 minut, což je v 13:00 hodin.

2. Představení vybraných algoritmů pro prvočíselný rozklad

a) Faktorizace dělením („Hrubá síla“)

Tato metoda pro prvočíselný rozklad je jedna s časově nejnáročnějších, pokud se jedná o vyšší čísla. U nižších čísel se znalostí malé a velké násobilky prvočíselný rozklad nebude tak časově náročný.

Př.) Rozložte číslo 12 na součin prvočísel.

$$n = 12$$

12 : 2 = 6, zbytek 0 => přidáme do rozkladu číslo 2

6 : 2 = 3, zbytek 0 => přidáme do rozkladu číslo 2

3 : 3 = 1, zbytek 0 => přidáme do rozkladu číslo 3

Rozklad je dokončen, nemusíme další čísla testovat, a prvočíselný rozklad čísla 12 bude vypadat následovně:

$$\boldsymbol{n = 12 = 2 \cdot 2 \cdot 3}$$

Př.) Rozložte číslo 100 na součin prvočísel.

$$n = 100$$

100 : 2 = 50, zbytek 0 => přidáme do rozkladu číslo 2

50 : 2 = 25, zbytek 0 => přidáme do rozkladu číslo 2

25 : 2 = 12, zbytek 1 => musíme otestovat další prvočíslo 3

25 : 3 = 8, zbytek 1 => musíme otestovat další prvočíslo 5

25 : 5 = 5, zbytek 0 => přidáme do rozkladu číslo 5

5 : 5 = 1, zbytek 0 => přidáme do rozkladu číslo 5

Rozklad je dokončen, opět nemusíme další čísla testovat, a prvočíselný rozklad čísla 100 bude vypadat následovně:

$$n = 100 = 2 \cdot 2 \cdot 5 \cdot 5$$

b) Pollardův rho algoritmus

John Michael Pollard je britský matematik, který se narodil v roce 1941. Mezi jeho nejvýznamnější objevy patří algoritmy pro faktorizace velkých čísel Pollardův rho algoritmus a Pollardův p - 1 algoritmus. Dále také algoritmy pro výpočet diskrétních logaritmů.
Vystudoval Univerzitu v Cambridge, kde obdržel všechny tři tituly, a to titul B.A. v roce 1963, titul M.A. v roce 1965 a doktorský titul Ph.D. v roce 1978. V dalších letech pracoval pro významné britské společnosti jako British Telecom.
V roce 1971 představil diskrétní Fourierovou analýzu pomocí Cooley-Tukeyho algoritmu.
V roce 1999 získal ocenění RSA od společnosti Compaq Computer

John Michael Pollard vymyslel svůj rho algoritmus v roce 1975, který je obzvláště rychlý pro rozkládání velkých složených čísel s nízkým prvočíselným faktorem, tj. s nízkými čísly v prvočíselném rozkladu. Nejpozoruhodnějším úspěchem tohoto algoritmu je úspěšná faktorizace osmého Fermatova čísla.

Formulace Pollardova rho algoritmu:

Mějme přirozené číslo N, které chceme faktorizovat. Poté si zvolíme přirozené číslo x_0 a vypočítáme určitý počet členů posloupnosti nezáporných celých čísel $\{x_i\}$, která jsou definována takto:

$$x_{i+1} \equiv x_i^2 + 1 (mod\ N)$$

Předpokládejme, že prvočíslo p je nejmenším prvočíselným dělitelem čísla N. Poté ještě předpokládejme, že $\{x_i\}$ je posloupnost pseudonáhodných čísel modulo p. Dále nechť pro jisté dva členy x_n, x_m, kde $n > m$, této posloupnosti platí, že $x_n \equiv x_m \pmod p$.

Platí tedy $p \mid (x_n - x_m)$, $p \mid N$, to znamená, že největší společný dělitel $D(x_n - x_m, N) > 1$. Jestliže zároveň x_n neodpovídá $x_m \pmod p$, potom je $D(x_n - x_m, N) < N$ a nalezli jsme netriviální (vlastní) dělitel čísla N. Pro ověření správnosti tohoto dělitele lze využít jeden

z efektivnějších algoritmů, Euklidův algoritmus, pomocí kterého nalezeme výše zmiňovaného dělitele.

Časově a početně náročné by bylo, pokud bychom museli počítat $D(x_n - x_m, N)$ pro všechny dvojice $n, m \in N$, $n > m$. Tím by se zcela znehodnotilo praktické využití této metody. Můžeme si ale část těchto výpočtů ušetřit, a testovat jen dvojice x_{2i}, x_i, $i \in N$ (Floydův trik).

Postup algoritmu:

Je dáno přirozené číslo *N*, které chceme rozložit.

1. Zvolme si číslo x_0
2. Vypočteme $x_{i+1} \equiv x_i^2 + 1 (mod\ N)$, pro přirozená čísla až do určité hodnoty *i.*
3. Pro přirozená čísla *i* provedeme výpočty $D(x_{2i} - x_i, N)$.
    a) pokud nalezneme netriviálního dělitele čísla *N*, dospěli jsme k řešení
    b) pokud nenalezneme netriviálního dělitele čísla *N*, neuspěli jsme. [1]

Př.) Rozložme číslo *N* = 527 pomocí Pollardovy rho metody. [1]

Zvolíme si vhodné $x_0 = 3$. Následně vypočteme dalších deset členů posloupnosti $\{x_i\}$:

$x_1 \equiv x_0^2 + 1 \pmod{527}$ -> $x_1 \equiv 3^2 + 1 \pmod{527}$ -> $x_1 \equiv \mathbf{10} \pmod{527}$

$x_2 \equiv x_1^2 + 1 \pmod{527}$ -> $x_2 \equiv 10^2 + 1 \pmod{527}$ -> $x_2 \equiv \mathbf{101} \pmod{527}$

$x_3 \equiv x_2^2 + 1 \pmod{527}$ -> $x_3 \equiv 101^2 + 1 \pmod{527}$ -> $x_3 \equiv \mathbf{189} \pmod{527}$

$x_4 \equiv x_3^2 + 1 \pmod{527}$ -> $x_4 \equiv 189^2 + 1 \pmod{527}$ -> $x_4 \equiv \mathbf{413} \pmod{527}$

$x_5 \equiv x_4^2 + 1 \pmod{527}$ -> $x_5 \equiv 413^2 + 1 \pmod{527}$ -> $x_5 \equiv \mathbf{349} \pmod{527}$

$x_6 \equiv x_5^2 + 1 \pmod{527}$ -> $x_6 \equiv 349^2 + 1 \pmod{527}$ -> $x_6 \equiv \mathbf{65} \pmod{527}$

$x_7 \equiv x_6^2 + 1 \pmod{527}$ -> $x_7 \equiv 65^2 + 1 \pmod{527}$ -> $x_7 \equiv \mathbf{10} \pmod{527}$

$x_8 \equiv x_7^2 + 1 \pmod{527}$ -> $x_8 \equiv 10^2 + 1 \pmod{527}$ -> $x_8 \equiv \mathbf{101} \pmod{527}$

$x_9 \equiv x_8^2 + 1 \pmod{527}$ -> $x_9 \equiv 101^2 + 1 \pmod{527}$ -> $x_9 \equiv \mathbf{189} \pmod{527}$

$x_{10} \equiv x_9^2 + 1 \pmod{527}$ -> $x_{10} \equiv 189^2 + 1 \pmod{527}$ -> $x_{10} \equiv \mathbf{413} \pmod{527}$

Dále si určíme největší společné dělitele:

$D(x_2 - x_1, N) = D(101 - 10, 527) = 1,$

$D(x_4 - x_2, N) = D(413 - 101, 527) = 1,$

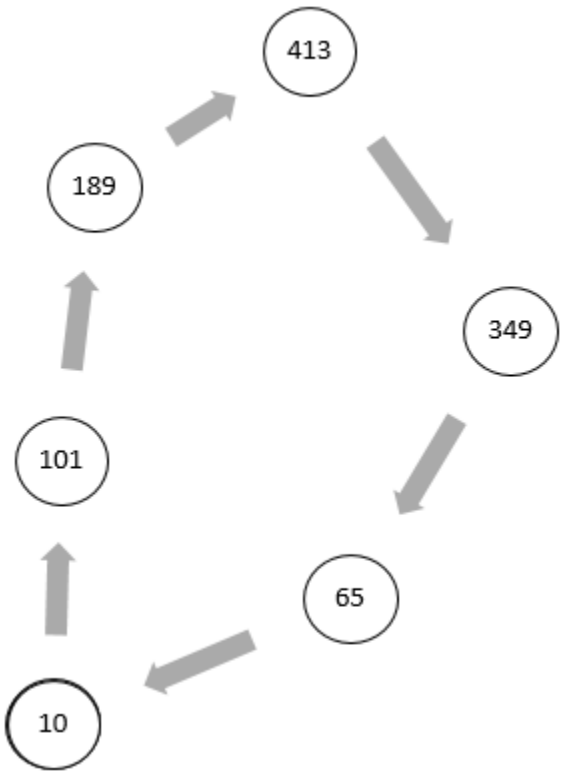
$D(x_6 - x_3, N) = D(65 - 189, 527) = 31.$

Další největší společný dělitele hledat nemusíme, jelikož jsme nalezli netriviální dělitel čísla $N = 527$, tj. číslo 31.

Tudíž platí:

$$\boldsymbol{N = 527 = 31 \cdot 17.}$$

Ze získané posloupnosti $\{x_i\}$ můžeme odůvodnit, proč právě název rho algoritmus, který nese označení po písmenu řecké abecedy ρ. První člen x_0 je předperiodou, a poté od sedmého členu posloupnosti $\{x_i\}$ dochází k zacyklení, jelikož $x_1 = x_7 = 10$. Zacyklení si ukážeme na uzlovém grafu:



Obrázek 2: Zacyklení Pollardova rho algoritmu

c) Pollardův p - 1 algoritmus

Opět se jedná o algoritmus Johna Pollarda ze 70. let 20. století, který umí rychle najít velmi velkého prvočíselného dělitele čísla *N*. Tento algoritmus můžeme využít například v kryptografii a pracuje na principu Malé Fermatovy věty, kde rozklad čísla *a* na faktory závisí na následující větě.

Malá Fermatova věta:

Pro každé prvočíslo *p* a každé číslo *a* platí:

$$a^p \equiv a(mod\ p)$$

Formulace Pollardova p -1 algoritmu:

Mějme tedy prvočíslo *N*, které chceme faktorizovat. Také platí, že prvočíslo *p* dělí *N*. Prvočíslo *p* není dopředu známé. Nechť $a \geq 1$ je přirozené číslo, které je nesoudělné s *N*, pokud největší společný dělitel *D(a, N)* = 1. Poté z Malé Fermatovy věty vyplývá následující vztah:

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

Dále předpokládejme, že mocnina *p - 1* je nepříliš velkou mocninou *B*, kterou musí zaujímat hladké číslo. Potom *p - 1* dělí *B!*, jelikož všechny mocniny prvočísel dělící *p - 1* jsou menší než *B*. Pak platí:

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

Mějme tedy $p \mid (a^{B!} - 1)$ a $p \mid N$, pak platí:

$$D(a^{B!} - 1, N) > 1$$

Zvyšováním hodnoty *B* nalezneme s velkou pravděpodobností netriviálního dělitele čísla *N*. [2]

Popis algoritmu:

1. Zvolíme si složené číslo *N* a vhodnou hodnotu *B*.
2. Vybereme hodnotu *a*, která je nesoudělná s *N*.
3. Vypočítáme: $d = D(a^{k!} - 1, N)$, pokud se $d \neq 1$, vrátíme se opět k výpočtu *d*.

4. Vypočítáme si mocninu, kde $b = a$. Potom $j = 2$ až do B. Dále $b = b^j \pmod N$.
5. Jestliže je $d = 1$, potom neexistuje hladké číslo B, které je dělitelem N.
6. Jestliže je $d = N$, potom všechny dělitele čísla N jsou hladké.

Algoritmus může selhat jen ve dvou případech. V prvním případě, pokud $d = 1$, a to nastane tehdy, kdy $p \leq B$, tj. $p - 1$ je hladké číslo B. Pokud chceme v tomto případě dojít ke zdárnému řešení, musíme zvýšit hodnotu B a projít postup algortimu znovu.
Druhým případ nastane, pokud $d = N$ a nalezneme současně všechny prvočíselné dělitele N. Potom jsou všechny prvočíselné dělitele N hladké. Pokud bychom zvolili jiné a, tak se nemusí jednat o vhodný krok, jelikož pro a je nesoudělné s N by byla hodnota $a^{B!} \bmod N$ stále rovna 1. Vhodným způsobem by bylo za a volit prvočísla a dělit nimi číslo N nebo zmenšení hodnoty B a projít algoritmus znovu.

Př.) Mějme zadané číslo $N = 1\,403$. Poté zvolme hodnotu $B = 5$ a vypočtěme součin všech prvočísel menších než mezní hodnota $B(2, 3)$, která jsme nalezli pomocí Eratosthenova síta. Následně vybereme hodnotu $a = 2$ a provedeme výpočet.

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

$$2^{2!} \equiv 4 \ (mod\ 1\,403)$$

Poté si vypočteme největší společný dělitel $d = D(4 - 1, 1403) = 1$, tudíž můžeme pokračovat ve výpočtu dále.

$$2^{3!} \equiv 64 \ (mod\ 1\,403)$$

Opět si vypočteme $d = D(64 - 1, 1403) = 1.$

$$2^{4!} \equiv 142 \ (mod\ 1\,403)$$

Zjišťujeme dále největšího společného dělitele $d = D(142 - 1, 1403) = 1.$

$$2^{5!} \equiv 794 \ (mod\ 1\,403)$$

Zde se $d = D(794 - 1, 1403) = 61.$

Dospěli jsme k rozkladu čísla $1\,403 = 61 \cdot 23$, tj. na součin prvočísel. Pro zajímavost stojí za zmínku, že výraz $61 - 1 = 2^2 \cdot 3 \cdot 5$, kde $B = 5$ je hladké číslo. To znamená, že žádný z jeho prvočíselných dělitelů není větší než 5.

d) Eulerova metoda

Leonard Euler (1707 - 1783) byl významný švýcarský matematik a fyzik, který se narodil v roce 1707 v Basileji Paulu Eulerovi a Markétě Bruckerové. Eulerův otec se v jeho mládí pravidelně navštěvoval s Johannem Bernoullim, s dalším významným švýcarským matematikem, tudíž se tak Leonhard Euler dostal přímo k pramenům matematického poznání a už v dětství si osvojil základní formy matematické myšlenkové činnosti.

Díky vazbám na Johanna Bernoulliho začal Leonhard Euler studovat už ve 13 letech na Univerzitě v Basileji, kde navštěvoval právě Bernoulliho přednášky. Ten odhalil jeho velký talent při řešení matematických problémů, a nabídl mu dokonce i individuální konzultace. Učení mu šlo velmi lehce, měl velmi vyspělé logické uvažování a vynikající paměť. Proto už v roce 1726, kdy mu bylo 19 let, složil doktorské zkoušky na Univerzitě v Basileji z fyziky. Poté se také ucházel o profesuru z fyziky, ale díky nízkému věku nebyl přijat.

Postupem času navštěvoval významné univerzity v Evropě. Z Univerzity v Basileji se vydal nejprve do Ruska, do Ruské akademie věd, kam ho pozvali oba synové Johanna Bernoulliho, se kterými se seznámil právě při společných schůzkách s jejich otcem v dětství. Zde mu bylo nabídnuto i místo fyziologa v oddělení pro medicínu. Roku 1733 byl jmenován profesorem a vedoucím matematického oddělení petrohradské Akademie místo Nikolase Bernoulliho, který zemřel.

V Petrohradě se také poprvé oženil. Z jedenácti předvedených nevěst si vybral tu, která se mu zdála nejvhodnější. Čas ukázal, že jeho volba byla šťastná. V roce 1735 oslepl na jedno oko. Historici udávají, že se tak stalo po třídenní a třínoční usilovné práci na výpočtu astronomických tabulek, na který by ostatní matematici potřebovali měsíce.

Roku 1741 Euler z Ruska odešel a přijal pozvání pruského krále Fridricha II. Velikého do Berlína. Strávil pak v Pruské akademii věd celých 25 let. Z tohoto období pochází jeho nejvýznamnější objev, a to vlnová rovnice. Původně šlo o zajímavou, ale poněkud okrajovou otázku kmitání houslové struny. Už staří Řekové věděli, že struna může kmitat mnoha různými způsoby, podle toho, jak se na ni brnkne. Vědci se od 17. století pokoušeli vypočítat, jak se v průběhu kmitu mění její tvar. Počátkem 18. století se objevilo několik významných prací na toto téma, až konečně roku 1748 Euler s použitím Newtonovy

mechaniky sestavil a vyřešil vlnovou rovnici pro strunu. Je to parciální diferenciální rovnice, která popisuje změny tvaru struny v čase i v prostoru.

O 11 let později odvodil vlnovou rovnici pro kmitající plochu s pevným okrajem jako například buben. Mohlo by se zdát, že se taková matematika houslí a bubnů týká jen hudby, ale není to pravda. Záhy se vlnová rovnice začala objevovat ve všech možných oblastech fyziky. V hydrodynamice popisuje formování a pohyb vodních vln, v akustice popisuje šíření zvukových vln ve vzduchu. Následně se objevila v 19. století v teorii elektromagnetických vln.

Po dlouhém působení v Berlíně, které trvalo čtvrt století, se opět vrátil do Ruska, kde už strávil zbytek svého života. Vrátil se v roce 1766 díky pozvání nové ruské panovnice, carevny Kateřiny Veliké, která ho jmenovala ředitelem matematické třídy petrohradské Akademie. Na uvolněné místo ředitele matematické sekce na Pruské akademii po Leonhardu Eulerovi nastoupil další významný matematik, a to Joseph Lagrange.

Euler po krátké době pobývání v Rusku oslepl i na druhé oko. Tento handicap ho ale nezbrzdil ve tvorbě dalších vědeckých prací, jelikož využíval svojí jedinečnou paměť a logické myšlení. Své myšlenky diktoval dalším výborným matematikům, svému synovi a akademikům na petrohradské Akademii, kteří je zapisovali.

Ke konci života se podruhé oženil s nevlastní sestrou své první manželky a strávil zbytek času v kruhu svých 38 vnoučat, kterým předával své matematické a fyzikální znalosti.

Leonhard Euler je považován za jednoho z nejvýznamnějších matematiků všech dob. Nejvýznamnější objevy učinil v oblasti matematiky, a to v diferenciálního počtu, teorii grafů a také zavedl mnoho znaků v matematické analýze. Také je uznávám v oblasti fyziky díky svým pracím v optice, mechanice a astronomii.

Pomocí jeho metody se dají rozložit pouze čísla, které jsou součtem dvou různých čtvercových čísel. Dále také čísla, které se rovnají součinu dvou prvočísel. Tuto metodu nelze použít na lichá složená čísla s prvočíselnými faktory formy $4k + 3$ nebo $4k + 1$, protože takovéto čísla nemohou být nikdy součtem dvou čtverců. Například se jedná o číslo $3053 = 43 \cdot 71$.

Popis metody:

Mějme předpis pro číslo *N*, které chceme rozložit na součin prvočísel:

$$\boldsymbol{N} = a^2 + b^2 = c^2 + d^2$$

Poté upravíme vzorec na rovnici:

$$a^2 - c^2 = d^2 - b^2$$

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

Následně určíme konstanty:

$$k = D((a - c), (d - b))$$

$$n = D((a + c), (d + b)),$$

kde *D* znamená největší společný dělitel.

Potom tedy platí:

$$(a - c) = k \cdot l$$

$$(d - b) = k \cdot m$$

$$l \cdot (a + c) = m \cdot (\mathrm{d} + \mathrm{b})$$

$$(a + c) = m \cdot n$$

$$(d + b) = l \cdot n$$

Výsledný předpis bude vypadat takto:

$$\boldsymbol{N} = [(k/2)^2 + (n/2)^2] \cdot (m^2 + l^2)$$

Př.) Rozložte pomocí této metody číslo n = 5353.

Číslo *N* = 5353 můžeme rozložit na součet dvou čtvercových čísel $13^2 + 72^2$, také na $27^2 + 68^2$.

Dále určíme parametry *a* = 13, *b* = 72, *c* = 27, *d* = 68.

Potom platí:

$$a - c = -14$$

$$a + c = 40$$

$$d - b = -4$$

$$d + b = 140$$

Z určení největších společných dělitelů součtů a rozdílů parametrů a, b, c, d můžeme určit parametry k, l, m, n.

$$k = 2$$

$$l = 20$$

$$m = 2$$

$$n = 7$$

Tak potom číslo $\boldsymbol{N = 5353} = [(k/2)^2 + (n/2)^2] \cdot (m^2 + l^2) = 101 \cdot 53$

Dospěli jsme zde k rozkladu hledaného čísla $N = 5353$ na součin prvočísel 101 a 53 beze zbytku. Díky tomu tato metoda funguje. [5]

3) Ilustrační příklady práce vybraných algoritmů

a) Faktorizace dělením („Hrubá síla“)

Př.) Rozložte číslo 1024 na součin prvočísel.

$$n = 1024$$

1024 : 2 = 512, zbytek 0 => přidáme do rozkladu číslo 2

512 : 2 = 256, zbytek 0 => přidáme do rozkladu číslo 2

256 : 2 = 128, zbytek 0 => přidáme do rozkladu číslo 2

128 : 2 = 64, zbytek 0 => přidáme do rozkladu číslo 2

64 : 2 = 32, zbytek 0 => přidáme do rozkladu číslo 2

32 : 2 = 16, zbytek 0 => přidáme do rozkladu číslo 2

16 : 2 = 8, zbytek 0 => přidáme do rozkladu číslo 2

8 : 2 = 4, zbytek 0 => přidáme do rozkladu číslo 2

4 : 2 = 2, zbytek 0 => přidáme do rozkladu číslo 2

2 : 2 = 1, zbytek 0 => přidáme do rozkladu číslo 2

Rozklad je dokončen, tudíž nemusíme další čísla testovat, a prvočíselný rozklad čísla 1024 bude vypadat následovně:

$$\boldsymbol{n = 1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}}$$

Př.) Rozložte číslo 134 540 na součin prvočísel.

$$n = 134\,540$$

134 540 : 2 = 67 270, zbytek 0 => přidáme do rozkladu číslo 2

67 270 : 2 = 33 635, zbytek 0 => přidáme do rozkladu číslo 2

33 635 : 5 = 6 727, zbytek 0 => přidáme do rozkladu číslo 5

6 727 : 7 = 961, zbytek 0 => přidáme do rozkladu číslo 7

961 : 31 = 31, zbytek 0 => přidáme do rozkladu číslo 31

31 : 31 = 1, zbytek 0 => přidáme do rozkladu číslo 31

Rozklad je dokončen, opět nemusíme další čísla testovat, a prvočíselný rozklad čísla 134 540 bude vypadat následovně:

$$\boldsymbol{n = 134\,540 = 2 \cdot 2 \cdot 5 \cdot 7 \cdot 31 \cdot 31 = 2^2 \cdot 5 \cdot 7 \cdot 31^2}$$

Př.) Rozložte číslo 123 456 789 na součin prvočísel.

$$n = 123\,456\,789$$

123 456 789 : 3 = 41 152 263, zbytek 0 => přidáme do rozkladu číslo 3

41 152 263 : 3 = 13 717 421, zbytek 0 => přidáme do rozkladu číslo 3

13 717 421 : 3 607 = 3 803, zbytek 0 => přidáme do rozkladu číslo 3 607

3 803 : 3 803 = 1, zbytek 0 => přidáme do rozkladu číslo 3 803

Opět nemusíme další čísla testovat, jelikož je rozklad dokončen, a prvočíselný rozklad čísla 123 456 789 bude vypadat následovně:

$$n = 123\,456\,789 = 3 \cdot 3 \cdot 3\,607 \cdot 3\,803 = 3^2 \cdot 3\,607 \cdot 3\,803$$

U tohoto příkladu bylo početně i časově náročné najít prvočíselné dělitele 3 607 a 3 803, díky kterým nám musí vyjít nulový zbytek, abychom je mohli zařadit do prvočíselného rozkladu zadaného čísla.

b) Pollardův rho algoritmus

U příkladů simulujících průběh Pollardova rho algoritmu lze využít jako kontrolu výpočtu kalkulátor TI - 92 Plus, který byl vydán v roce 1999.

Obsahuje nemalou část zajímavých funkcí a příkazů. Jedním z nich je příkaz *„remain“*, který nám zjišťuje členy posloupnosti x_i při výpočtu Pollardova rho algoritmu, a také příkaz *„gcd“*, který značí největší společný dělitel, a je důležitý pro výpočet tohoto algoritmu. Jedná se o velmi rychlý proces výpočtu, tudíž dochází i k jeho časovému usnadnění. Výpočet si můžeme také díky programu TI Graph Link 89 a příslušnému kabelu vyexportovat do počítače, a tím graficky znázornit celý výpočet.

Obrázek 3: Kalkulátor TI - 92 Plus

Př.) Rozložte číslo $N = 54$ pomocí Pollardovy rho metody.

Zvolme si vhodné $x_0 = 4$. Následně vypočteme dalších deset členů posloupnosti $\{x_i\}$:

$x_1 \equiv x_0^2 + 1 \pmod{54}$ -> $x_1 \equiv 4^2 + 1 \pmod{54}$ -> $x_1 \equiv \mathbf{17} \pmod{54}$

$x_2 \equiv x_1^2 + 1 \pmod{54}$ -> $x_2 \equiv 17^2 + 1 \pmod{54}$ -> $x_2 \equiv \mathbf{20} \pmod{54}$

$x_3 \equiv x_2^2 + 1 \pmod{54}$ -> $x_3 \equiv 20^2 + 1 \pmod{54}$ -> $x_3 \equiv \mathbf{23} \pmod{54}$

$x_4 \equiv x_3^2 + 1 \pmod{54}$ -> $x_4 \equiv 23^2 + 1 \pmod{54}$ -> $x_4 \equiv \mathbf{44} \pmod{54}$

$x_5 \equiv x_4^2 + 1 \pmod{54}$ -> $x_5 \equiv 44^2 + 1 \pmod{54}$ -> $x_5 \equiv \mathbf{47} \pmod{54}$

$x_6 \equiv x_5^2 + 1 \pmod{54}$ -> $x_6 \equiv 47^2 + 1 \pmod{54}$ -> $x_6 \equiv \mathbf{50} \pmod{54}$

$x_7 \equiv x_6^2 + 1 \pmod{54}$ -> $x_7 \equiv 50^2 + 1 \pmod{54}$ -> $x_7 \equiv \mathbf{17} \pmod{54}$

$x_8 \equiv x_7^2 + 1 \pmod{54}$ -> $x_8 \equiv 17^2 + 1 \pmod{54}$ -> $x_8 \equiv \mathbf{20} \pmod{54}$

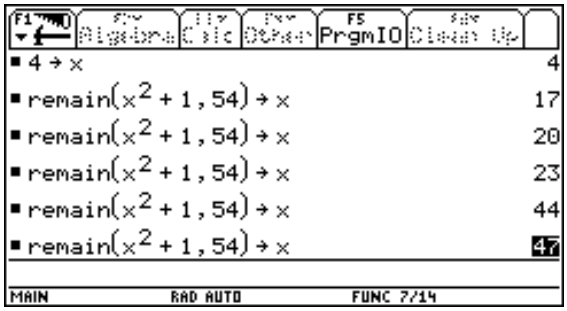
$x_9 \equiv x_8^2 + 1 \pmod{54}$ -> $x_9 \equiv 20^2 + 1 \pmod{54}$ -> $x_9 \equiv \mathbf{23} \pmod{54}$

$x_{10} \equiv x_9^2 + 1 \pmod{54}$ -> $x_{10} \equiv 23^2 + 1 \pmod{54}$ -> $x_{10} \equiv \mathbf{44} \pmod{54}$

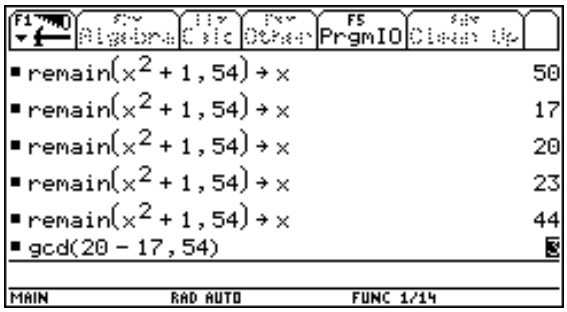
Dále si určíme největší společný dělitele:

$D(x_2 - x_1, N) = D(20 - 17, 54) = 3$.

Výpočet členů posloupnosti $\{x_i\}$a jediného největšího společného dělitele si můžeme ukázat na kalkulátoru TI - 92 Plus, kde za x ($x = x_0$) jsme si zvolili číslo 4. Poté jsme použili příkaz *„remain“* a *„gcd“*, abychom mohli zjistit všechny členy posloupnosti x_i a právě jediného společného dělitele.



Obrázek 4: Průběh výpočtu - Pollardův rho algoritmus



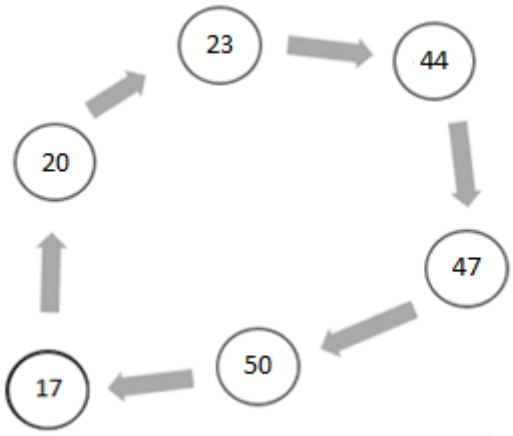
Obrázek 5: Průběh výpočtu - Pollardův rho algoritmus

Po ověření na kalkulátoru TI - 92 Plus a celém výpočtu Pollardova rho algoritmu jsme dospěli k netriviálnímu děliteli čísla $N = 54$, tj. číslo 3. Potom další největší společný dělitel hledat nemusíme.

Pak platí:

$$\boldsymbol{N = 54 = 3 \cdot 18}$$

Ze získaných členů posloupnosti $\{x_i\}$ je patrné, že dochází k zacyklení, které je ukázáno na následujícím obrázku.



Obrázek 6: Zacyklení Pollardova rho algoritmu

Tento příklad je pro výpočet Pollardovým rho algoritmem komplikovanější. Rychlejší metodou výpočtu by byla faktorizace dělením („hrubou silou“).

Př.) Rozložte číslo $N = 221$ pomocí Pollardovy rho metody.

Zvolme si vhodné $x_0 = 4$.

a) Následně vypočteme dalších čtrnáct členů posloupnosti $\{x_i\}$:

$x_1 \equiv x_0^2 + 1 \pmod{221}$ -> $x_1 \equiv 4^2 + 1 \pmod{221}$ -> $x_1 \equiv \mathbf{17} \pmod{221}$

$x_2 \equiv x_1^2 + 1 \pmod{221}$ -> $x_2 \equiv 17^2 + 1 \pmod{221}$ -> $x_2 \equiv \mathbf{69} \pmod{221}$

$x_3 \equiv x_2^2 + 1 \pmod{221}$ -> $x_3 \equiv 69^2 + 1 \pmod{221}$ -> $x_3 \equiv \mathbf{121} \pmod{221}$

$x_4 \equiv x_3^2 + 1 \pmod{221}$ -> $x_4 \equiv 121^2 + 1 \pmod{221}$ -> $x_4 \equiv \mathbf{56} \pmod{221}$

$x_5 \equiv x_4^2 + 1 \pmod{221}$ -> $x_5 \equiv 56^2 + 1 \pmod{221}$ -> $x_5 \equiv \mathbf{43} \pmod{221}$

$x_6 \equiv x_5^2 + 1 \pmod{221}$ -> $x_6 \equiv 43^2 + 1 \pmod{221}$ -> $x_6 \equiv \mathbf{82} \pmod{221}$

$x_7 \equiv x_6^2 + 1 \pmod{221}$ -> $x_7 \equiv 82^2 + 1 \pmod{1241}$ -> $x_7 \equiv \mathbf{95} \pmod{221}$

$x_8 \equiv x_7^2 + 1 \pmod{221}$ -> $x_8 \equiv 95^2 + 1 \pmod{221}$ -> $x_8 \equiv \mathbf{186} \pmod{221}$

$x_9 \equiv x_8^2 + 1 \pmod{221}$ -> $x_9 \equiv 186^2 + 1 \pmod{221}$ -> $x_9 \equiv \mathbf{121} \pmod{221}$

$x_{10} \equiv x_9^2 + 1 \pmod{221}$ -> $x_{10} \equiv 121^2 + 1 \pmod{221}$ -> $x_{10} \equiv \mathbf{56} \pmod{221}$

$x_{11} \equiv x_{10}^2 + 1 \pmod{221}$ -> $x_{11} \equiv 56^2 + 1 \pmod{221}$ -> $x_{11} \equiv \mathbf{43} \pmod{221}$

$x_{12} \equiv x_{11}^2 + 1 \pmod{221}$ -> $x_{12} \equiv 43^2 + 1 \pmod{221}$ -> $x_{12} \equiv \mathbf{82} \pmod{1241}$

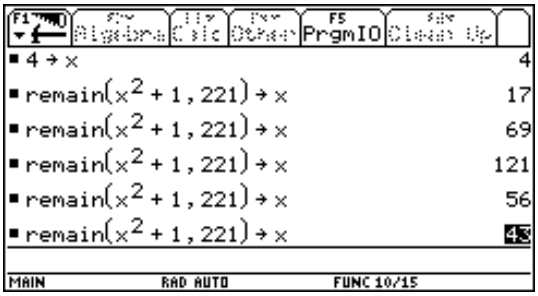
$x_{13} \equiv x_{12}^2 + 1 \pmod{221}$ -> $x_{13} \equiv 82^2 + 1 \pmod{221}$ -> $x_{13} \equiv \mathbf{95} \pmod{221}$

$x_{14} \equiv x_{13}^2 + 1 \pmod{221}$ -> $x_{13} \equiv 95^2 + 1 \pmod{221}$ -> $x_{13} \equiv \mathbf{186} \pmod{1241}$

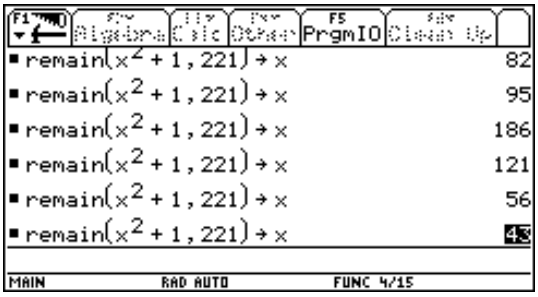
Poté určíme největší společný dělitele:

$D(x_2 - x_1, N) = D(69 - 17, 221) = 13$.

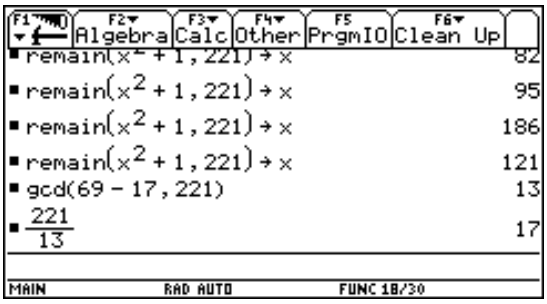
Pomůckou nám bude pro ověření výpočtu výše zmiňovaný kalkulátor TI - 92 Plus.



Obrázek 7: Průběh výpočtu (první část) - Pollardův rho algoritmus



Obrázek 8: Průběh výpočtu (druhá část) - Pollardův rho algoritmus



Obrázek 9: Průběh výpočtu (třetí část) - Pollardův rho algoritmus

Jelikož jsme nalezli jediný netriviální dělitel čísla N = 221, tj. číslo 13, potom další největší společný dělitele hledat nemusíme.

Pak platí:

$$\boldsymbol{N = 221 = 13 \cdot 17}$$

b) U dalšího způsobu řešení si nebudeme vypisovat všech čtrnáct členů posloupnosti $\{x_i\}$, ale vždy zjistíme důležité členy pro výpočty největších společných dělitelů $D(x_{2i} - x_i, N)$, což velmi ušetří čas při výpočtu.

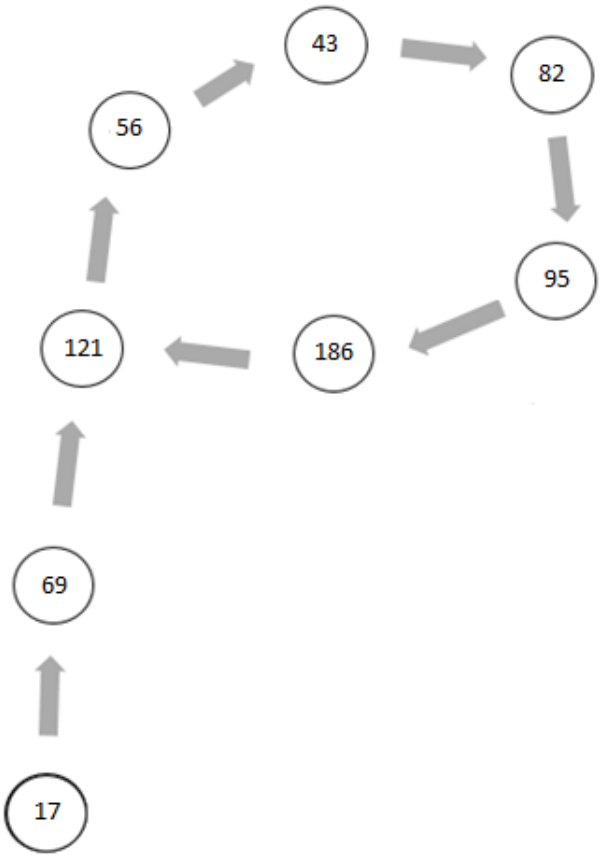
$x_1 \equiv x_0^2 + 1 \pmod{221}$ -> $x_1 \equiv 4^2 + 1 \pmod{221}$ -> $x_1 \equiv \mathbf{17} \pmod{221}$

$x_2 \equiv x_1^2 + 1 \pmod{221}$ -> $x_2 \equiv 17^2 + 1 \pmod{221}$ -> $x_2 \equiv \mathbf{69} \pmod{221}$

Jelikož $D(x_2 - x_1, N) = D(69 - 17, 221) = 13$, tj. našli jsme netriviální dělitel čísla 221, nemusíme vypisovat další členy posloupnosti $\{x_i\}$, a poté platí:

$$\boldsymbol{N = 221 = 13 \cdot 17}$$

Ze získaných členů posloupnosti $\{x_i\}$ z prvního způsobu řešení je patrné, že opět dochází k zacyklení, které znázorňuje řecké písmeno ρ, a můžeme ho vidět na následujícím obrázku.



Obrázek 10: Zacyklení Pollardova rho algoritmu

Př.) Rozložte číslo $N = 1241$ pomocí Pollardovy rho metody.

a) Zvolme si vhodné $x_0 = 7$. Následně vypočteme dalších patnáct členů posloupnosti $\{x_i\}$:

$x_1 \equiv x_0^2 + 1 \pmod{1241}$ -> $x_1 \equiv 7^2 + 1 \pmod{1241}$ -> $x_1 \equiv \mathbf{50} \pmod{1241}$

$x_2 \equiv x_1^2 + 1 \pmod{1241}$ -> $x_2 \equiv 50^2 + 1 \pmod{1241}$ -> $x_2 \equiv \mathbf{19} \pmod{1241}$

$x_3 \equiv x_2^2 + 1 \pmod{1241}$ -> $x_3 \equiv 19^2 + 1 \pmod{1241}$ -> $x_3 \equiv \mathbf{362} \pmod{1241}$

$x_4 \equiv x_3^2 + 1 \pmod{1241}$ -> $x_4 \equiv 362^2 + 1 \pmod{1241}$ -> $x_4 \equiv \mathbf{740} \pmod{1241}$

$x_5 \equiv x_4^2 + 1 \pmod{1241}$ -> $x_5 \equiv 740^2 + 1 \pmod{1241}$ -> $x_5 \equiv \mathbf{320} \pmod{1241}$

$x_6 \equiv x_5^2 + 1 \pmod{1241}$ -> $x_6 \equiv 320^2 + 1 \pmod{1241}$ -> $x_6 \equiv \mathbf{639} \pmod{1241}$

$x_7 \equiv x_6^2 + 1 \pmod{1241}$ -> $x_7 \equiv 639^2 + 1 \pmod{1241}$ -> $x_7 \equiv \mathbf{33} \pmod{1241}$

$x_8 \equiv x_7^2 + 1 \pmod{1241}$ -> $x_8 \equiv 33^2 + 1 \pmod{1241}$ -> $x_8 \equiv \mathbf{1090} \pmod{1241}$

$x_9 \equiv x_8^2 + 1 \pmod{1241}$ -> $x_9 \equiv 1090^2 + 1 \pmod{1241}$ -> $x_9 \equiv \mathbf{464} \pmod{1241}$

$x_{10} \equiv x_9^2 + 1 \pmod{1241}$ -> $x_{10} \equiv 464^2 + 1 \pmod{1241}$ -> $x_{10} \equiv \mathbf{604} \pmod{1241}$

$x_{11} \equiv x_{10}^2 + 1 \pmod{1241}$ -> $x_{11} \equiv 604^2 + 1 \pmod{1241}$ -> $x_{11} \equiv \mathbf{1204} \pmod{1241}$

$x_{12} \equiv x_{11}^2 + 1 \pmod{1241}$ -> $x_{12} \equiv 1204^2 + 1 \pmod{1241}$ -> $x_{12} \equiv \mathbf{129} \pmod{1241}$

$x_{13} \equiv x_{12}^2 + 1 \pmod{1241}$ -> $x_{13} \equiv 129^2 + 1 \pmod{1241}$ -> $x_{13} \equiv \mathbf{509} \pmod{1241}$

$x_{14} \equiv x_{13}^2 + 1 \pmod{1241}$ -> $x_{14} \equiv 509^2 + 1 \pmod{1241}$ -> $x_{14} \equiv \mathbf{954} \pmod{1241}$

$x_{15} \equiv x_{14}^2 + 1 \pmod{1241}$ -> $x_{14} \equiv 954^2 + 1 \pmod{1241}$ -> $x_{15} \equiv \mathbf{50} \pmod{1241}$

Dále si určíme největší společný dělitele:

$D(x_2 - x_1, N) = D(19 - 50, 1241) = 1$,

$D(x_4 - x_2, N) = D(740 - 19, 1241) = 1$,

$D(x_6 - x_3, N) = D(639 - 362, 1241) = 1$,

$D(x_8 - x_4, N) = D(1090 - 740, 1241) = 1$,

$D(x_{10} - x_5, N) = D(604 - 320, 1241) = 1$,

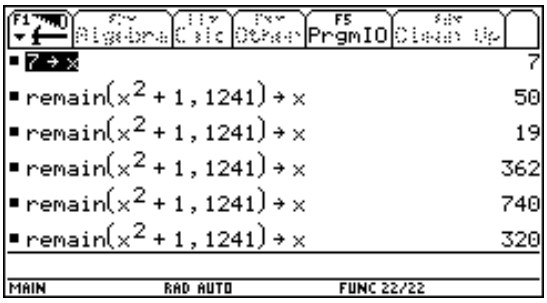
$D(x_{12} - x_6, N) = D(129 - 639, 1241) = 17$.

Dalšího společného dělitele již hledat nemusíme, jelikož jsme nalezli jediný netriviální dělitel čísla N = 1 241, tj. číslo 17. Poté další největší společný dělitele hledat nemusíme. Pak platí:

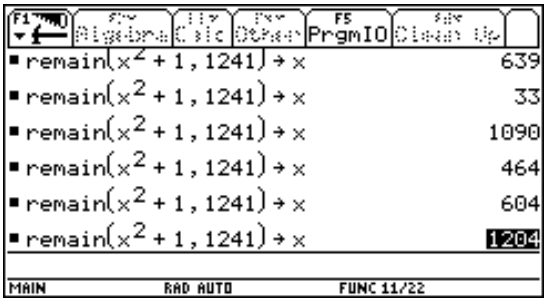
$$\boldsymbol{N = 1241 = 17 \cdot 73}$$

Patnáctý člen posloupnosti $\{x_i\}$ byl spočten z důvodu, že v tomto členu dochází k zacyklení

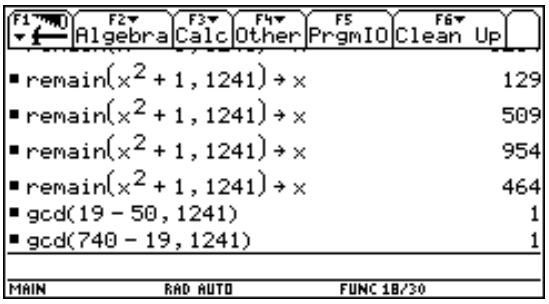
Opět si znázorníme zjištěné členy posloupnosti x_i a společné dělitele na kalkulátoru TI - 92 Plus.



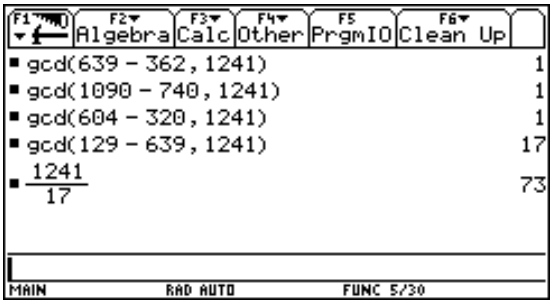
Obrázek 11: Průběh výpočtu (první část) - Pollardův rho algoritmus



Obrázek 12: Průběh výpočtu (druhá část) - Pollardův rho algoritmus



Obrázek 13: Průběh výpočtu (třetí část) - Pollardův rho algoritmus



Obrázek 14: Průběh výpočtu (čtvrtá část) - Pollardův rho algoritmus

b) U dalšího způsobu řešení si nebudeme vypisovat všech patnáct členů posloupnosti $\{x_i\}$, ale vždy zjistíme důležité členy pro výpočty největších společných dělitelů $D(x_{2i} - x_i, N)$, což v tomto případě ušetří výpočet posledních třech členů posloupnosti $\{x_i\}$.

$x_1 \equiv x_0^2 + 1 \pmod{1241}$ -> $x_1 \equiv 7^2 + 1 \pmod{1241}$ -> $x_1 \equiv \mathbf{50} \pmod{1241}$

$x_2 \equiv x_1^2 + 1 \pmod{1241}$ -> $x_2 \equiv 50^2 + 1 \pmod{1241}$ -> $x_2 \equiv \mathbf{19} \pmod{1241}$

$$D(x_2 - x_1, N) = D(19 - 50, 1241) = 1$$

$x_3 \equiv x_2^2 + 1 \pmod{1241}$ -> $x_3 \equiv 19^2 + 1 \pmod{1241}$ -> $x_3 \equiv \mathbf{362} \pmod{1241}$

$x_4 \equiv x_3^2 + 1 \pmod{1241}$ -> $x_4 \equiv 362^2 + 1 \pmod{1241}$ -> $x_4 \equiv \mathbf{740} \pmod{1241}$

$$D(x_4 - x_2, N) = D(740 - 19, 1241) = 1,$$

$x_5 \equiv x_4^2 + 1 \pmod{1241}$ -> $x_5 \equiv 740^2 + 1 \pmod{1241}$ -> $x_5 \equiv \mathbf{320} \pmod{1241}$

$x_6 \equiv x_5^2 + 1 \pmod{1241}$ -> $x_6 \equiv 320^2 + 1 \pmod{1241}$ -> $x_6 \equiv \mathbf{639} \pmod{1241}$

$$D(x_6 - x_3, N) = D(639 - 362, 1241) = 1$$

$x_7 \equiv x_6^2 + 1 \pmod{1241}$ -> $x_7 \equiv 639^2 + 1 \pmod{1241}$ -> $x_7 \equiv \mathbf{33} \pmod{1241}$

$x_8 \equiv x_7^2 + 1 \pmod{1241}$ -> $x_8 \equiv 33^2 + 1 \pmod{1241}$ -> $x_8 \equiv \mathbf{1090} \pmod{1241}$

$$D(x_8 - x_4, N) = D(1090 - 740, 1241) = 1,$$

$x_9 \equiv x_8^2 + 1 \pmod{1241}$ -> $x_9 \equiv 1090^2 + 1 \pmod{1241}$ -> $x_9 \equiv \mathbf{464} \pmod{1241}$

$x_{10} \equiv x_9^2 + 1 \pmod{1241}$ -> $x_{10} \equiv 464^2 + 1 \pmod{1241}$ -> $x_{10} \equiv \mathbf{604} \pmod{1241}$

$$D(x_{10} - x_5, N) = D(604 - 320, 1241) = 1,$$

$x_{11} \equiv x_{10}^2 + 1 \pmod{1241}$ -> $x_{11} \equiv 604^2 + 1 \pmod{1241}$ -> $x_{11} \equiv \mathbf{1204} \pmod{1241}$

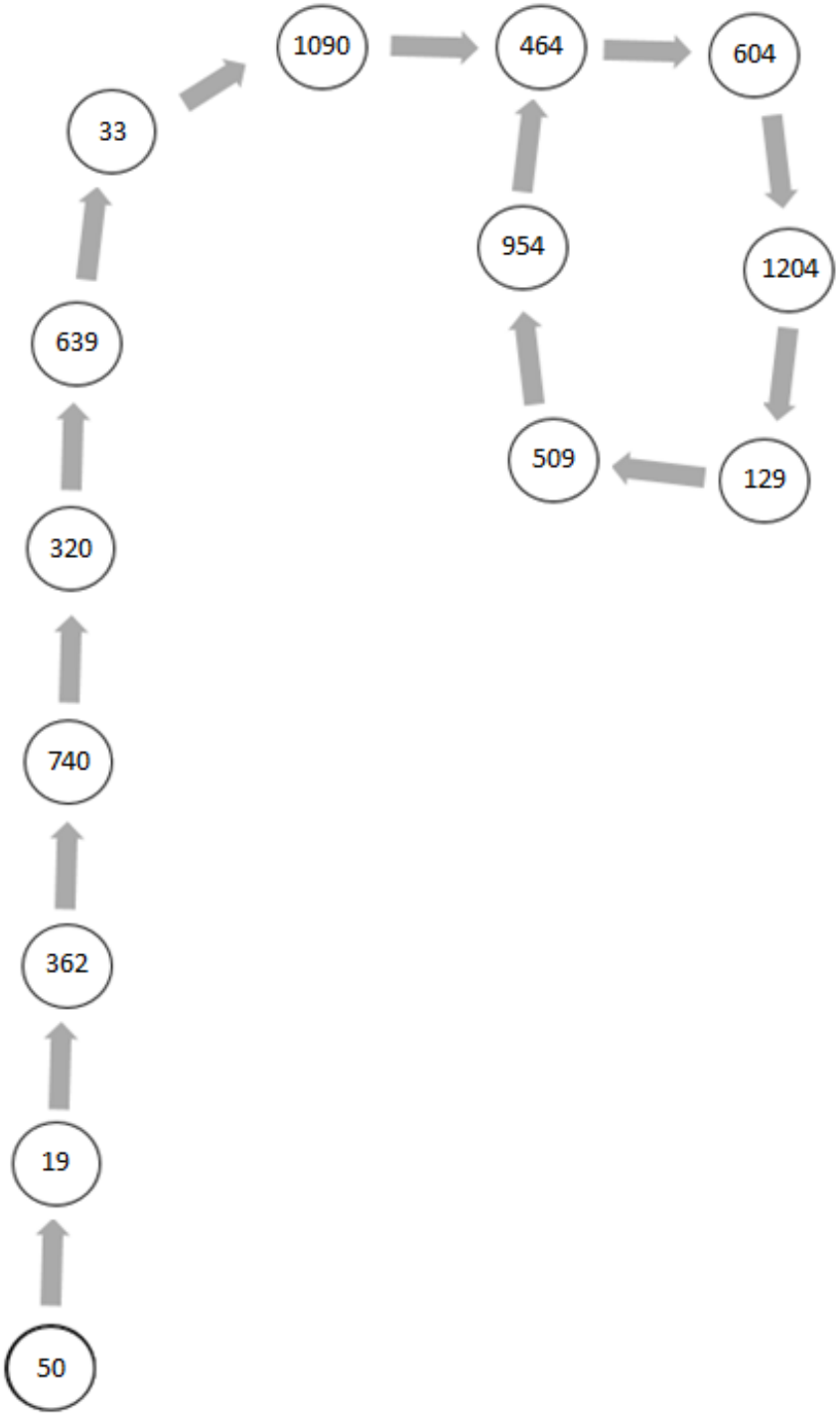
$x_{12} \equiv x_{11}^2 + 1 \pmod{1241}$ -> $x_{12} \equiv 1204^2 + 1 \pmod{1241}$ -> $x_{12} \equiv \mathbf{129} \pmod{1241}$

$$D(x_{12} - x_6, N) = D(129 - 639, 1241) = 17.$$

Jelikož $D(x_{12} - x_6, N) = D(129 - 639, 1241) = 13$, tj. našli jsme netriviální dělitel čísla 221, nemusíme vypisovat další členy posloupnosti $\{x_i\}$, a poté platí:

$$N = 1\,241 = 17 \cdot 73$$

Opět získaných členů posloupnosti $\{x_i\}$ z prvního způsobu řešení je jasné, že dochází k zacyklení, které znázorňuje řecké písmeno ρ, které můžeme ho vidět na následujícím obrázku.



Obrázek 15: Zacyklení Pollardova rho algoritmu

c) Pollardův p - 1 algoritmus

Př.) Rozložte číslo *N* = 299 pomocí Pollardovo *p - 1* algoritmu.

Zvolíme si hodnotu *B* = 5 a poté vybereme hodnotu *a* = 2.

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

$$2^{2!} \equiv 4 \ (mod\ 299)$$

Vypočteme největší společný dělitel $d = D(4 - 1, 299) = 1$, tudíž můžeme pokračovat ve výpočtu dále.

$$2^{3!} \equiv 64 \ (mod\ 299)$$

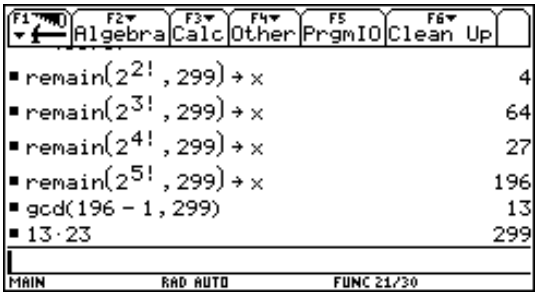
Dále zjišťujeme největšího společného dělitele, a to $d = D(64 - 1, 299) = 1$

$$2^{4!} \equiv 27 \ (mod\ 299)$$

Opět vypočítáme $d = D(27 - 1, 299) = 13$

Je tedy jasné, že je rozklad čísla 299 = 13 · 23 na součin prvočísel. Výraz 13 – 1 = $2^2 \cdot 3$, kde *B* = 3 je hladké číslo a žádný z jeho prvočíselných dělitelů není větší než 3.

Pro ověření výpočtu můžeme použít, jako u příkladů Pollardova rho algoritmu, kalkulátor TI - 92 Plus.



Obrázek 16: Průběh výpočtu - Pollardův p - 1 algoritmus

Př.) Rozložte číslo *N* = 2 993 pomocí Pollardovo *p - 1* algoritmu.

Zvolíme si hodnotu *B* = 5 a poté vybereme hodnotu *a* = 2.

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

$$2^{2!} \equiv 4 \ (mod\ 2\ 993)$$

$$d = D(4 - 1, 2\,993) = 1$$

$$2^{3!} \equiv 64\ (mod\ 2\,993)$$

$$d = D(64 - 1, 2\,993) = 1$$

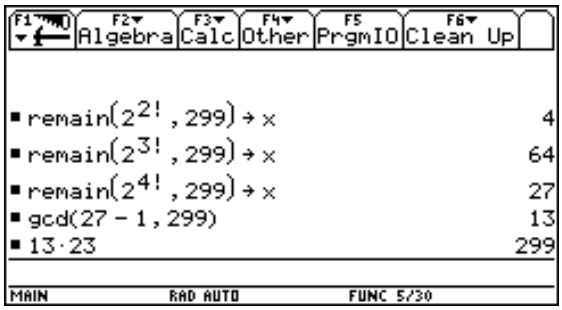
$$2^{4!} \equiv 1\,451\ (mod\ 2\,993)$$

$$d = D(1\,451 - 1, 2\,993) = 1$$

$$2^{5!} \equiv 1\,395\ (mod\ 2\,993)$$

$$d = D(1\,395 - 1, 2993) = 41$$

Mějme tedy rozklad čísla 2 993 = 41 · 73 na součin prvočísel. Výraz 41 – 1 = $2^3 \cdot 5$, kde *B* = 5 je hladké číslo a žádný z jeho prvočíselných dělitelů není větší než 5.



Obrázek 17: Průběh výpočtu - Pollardův p - 1 algoritmus

Př.) Rozložte číslo *N* = 6 994 241 pomocí Pollardovo *p - 1* algoritmu.

Zvolíme si hodnotu *B* = 7 a poté vybereme hodnotu *a* = 2.

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

$$2^{2!} \equiv 4\ (mod\ 6\,994\,241)$$

$$d = D(4 - 1, 6\,994\,241) = 1$$

$$2^{3!} \equiv 64\ (mod\ 6\,994\,241)$$

$$d = D(64 - 1, 6\,994\,241) = 1$$

$$2^{4!} \equiv 2\,788\,734\ (mod\ 6\,994\,241)$$

$$d = D(2\,788\,734 - 1, 6\,994\,241) = 1$$

$$2^{5!} \equiv 3\,834\,705\ (mod\ 6\,994\,241)$$

$$d = D(3\,834\,705 - 1, 6\,994\,241) = 1$$

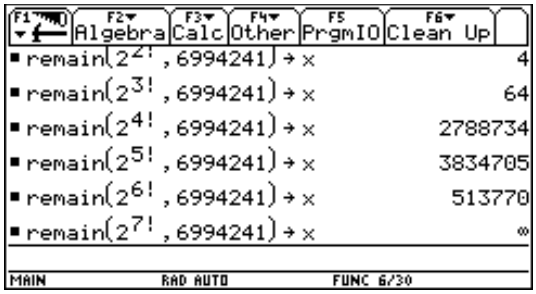
$$2^{6!} \equiv 513\,770\ (mod\ 6\,994\,241)$$

$$d = D(513\,770 - 1, 6\,994\,241) = 1$$

$$2^{7!} \equiv 443\,653\ (mod\ 6\,994\,241)$$

$$d = D(443\,653 - 1, 6\,994\,241) = 3\,361$$

Mějme tedy rozklad čísla 6 994 241 = 3 361 · 2081 na součin prvočísel. Výraz 3 361 – 1 = $2^5 \cdot 3 \cdot 5 \cdot 7$, kde *B* = 7 je hladké číslo a žádný z jeho prvočíselných dělitelů není větší než 7.



Obrázek 18: Průběh výpočtu - Pollardův p - 1 algoritmus

Při snaze výpočtu Pollardova p - 1 algoritmu u příkladů s vyšší hodnotou *B* není kalkulátor TI - 92 Plus vhodnou kontrolou, jelikož při zvolení *B* = 7 kalkulátor zobrazuje hodnotu nekonečna.

d) Eulerova metoda

Př.) Pomocí Eulerovy metody rozložte číslo *N* = 221.

Víme, že pro číslo *N* = 221 platí rozklad:

$$221 = 11^2 + 10^2$$

Toto číslo lze rozložit i na čtvercová čísla s jinou hodnotou:

$$221 = 5^2 + 14^2$$

Takže můžeme ponechat *a* = 11, *b* = 10, *c* = 5, *d* = 14.

Potom platí:

$$a - c = 6$$

$$a + c = 16$$

$$d - b = 4$$

$$d + b = 24$$

Z určení součtů a rozdílů největších společných dělitelů parametrů a, b, c, d můžeme určit parametry k, l, m, n.

$$k = 2$$

$$l = 3$$

$$m = 2$$

$$n = 8$$

Nyní dosadíme do vzorce pro výpočet rozkladu čísla $N = 221$ na součin dvou prvočísel.

$$\boldsymbol{N = 221} = [(2/2)^2 + (8/2)^2] \cdot (2^2 + 3^2) = (1^2 + 4^2) \cdot (2^2 + 3^2) = 17 \cdot 13$$

Číslo $N = 221$ tedy můžeme rozložit na součin prvočísel 17 a 13 beze zbytku, a díky tomu lze metodu na tento příklad aplikovat.

Př.) Pomocí Eulerovy metody rozložte číslo $N = 2\,501$.

Je jasné, že číslo $N = 2\,501$ platí:

$$2\,501 = 50^2 + 1^2$$

Toto číslo lze rozložit i na čtvercová čísla s jinou hodnotou:

$$2\,501 = 49^2 + 10^2$$

Takže můžeme ponechat $a = 1$, $b = 50$, $c = 49$, $d = 10$.

Potom platí:

$$a - c = -48$$

$$a + c = 50$$

$$d - b = -40$$

$$d + b = 60$$

Z určení součtů a rozdílů největších společných dělitelů parametrů a, b, c, d můžeme určit parametry k, l, m, n.

$$k = 8$$

$$l = 6$$

$$m = 5$$

$$n = 10$$

Nyní dosadíme do vzorce pro výpočet rozkladu čísla $N = 2501$ na součin dvou prvočísel.

$$\boldsymbol{N = 2\,501} = [(8/2)^2 + (10/2)^2] \cdot (5^2 + 6^2) = (4^2 + 5^2) \cdot (5^2 + 6^2) = 41 \cdot 61$$

Tudíž číslo $N = 2\,501$ lze rozložit na součin prvočísel 41 a 61 beze zbytku a můžeme tuto metodu na tento příklad aplikovat.

Př.) Pomocí Eulerovy metody rozložte číslo $N = 1\,000\,009$.

Pro číslo $N = 1\,000\,009$ platí:

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

Poté ponecháme parametry $a = 1000$, $b = 3$, $c = 972$, $d = 235$.

Potom platí:

$$a - c = 28$$

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

$$d - b = 232$$

$$d + b = 238$$

Z určení součtů a rozdílů největších společných dělitelů parametrů a, b, c, d určíme parametry k, l, m, n.

$$k = 4$$

$$l = 7$$

$$m = 58$$

$n = 34$

Dále dosadíme do vzorce pro výpočet rozkladu čísla *N* = 1 000 009 na součin dvou prvočísel.

$$\boldsymbol{N = 1\,000\,009} = [(4/2)^2 + (34/2)^2] \cdot (7^2 + 58^2) = (2^2 + 17^2) \cdot (7^2 + 58^2) = 293 \cdot 3\,413$$

Číslo *N* = 1 000 009 můžeme tedy rozložit na součin prvočísel 293 a 3 413.

4) Krátké porovnání algoritmů po stránce jejich výpočetní náročnosti

a) Faktorizace dělení („Hrubá síla“)

Jedná se o jednu z časově nejnáročnější metod pro zjištění prvočíselného rozkladu nějakého zadaného čísla, které má velmi vysokou hodnotu.

Pokud bychom měli zadané nějaké vyšší číslo *n*, které bychom chtěli rozložit na součin prvočísel, museli bychom najít všechna prvočísla do hodnoty $\sqrt{n}$. Po získání těchto prvočísel zkoušíme jimi dělit zadané číslo *n*. Jestliže by vyšlo dělení beze zbytku, potom víme, že daný dělitel by byl součástí prvočíselného rozkladu. Pokud vyjde zbytek, museli bychom se posunout na další prvočíslo v daném číselném seznamu, u kterého když dojdeme ke konci, tak by měl být rozklad hotový. Tudíž pro velmi vysoká čísla je tato metoda neefektivní jak z hlediska času, tak i výpočetní náročnosti.

b) Pollardův rho algoritmus

Tento algoritmus je v jisté části podobný jako předchozí metoda faktorizace dělením, ale při výpočtu Pollardovým rho algoritmem nehledáme všechny členy prvočíselného rozkladu, ale jen jeden. Pokud nebude právě nalezený člen prvočíselného rozkladu prvočíslem, potom musíme na výstup z toho algoritmu použít ještě faktorizaci dělením. Tím opět může dojít k časové i výpočetní náročnosti.

Pokud bychom v příkladech použili malé *N*, mohl by být tato metoda vhodná i pro žáky základní školy, jelikož dochází k provádění operací s přirozenými čísly, které žáci již znají. Pro další stupně škol má tento algoritmus využití ve výpočetní technice a programování.

V dnešní době ale Pollardův rho algoritmus nepatří mezi nejlepší faktorizační metody, ale začátkem 80. let 20. století byl nejlepším známým algoritmem pro faktorizaci přirozených čísel.

c) Pollardův p - 1 algoritmus

U Pollardova p - 1 algoritmu hraje důležitou roli pro časové zkrácení a usnadnění výpočtu volba hodnot *a* a *B*.
Volba hodnoty *a* nemá vliv na průběh výpočtu algoritmu, ale ztěžuje výpočet právě s hodnotou *a*. Tudíž je vhodné za *a* volit nízké hodnoty, jako například číslo 2 či 3. Za to hodnota *B* ovlivňuje, jak složitost, tak výsledek výpočtu. Zvýšení hodnoty *B* zvýšíme pravděpodobnost nalezení faktoru *N*, ale také zvýší časovou náročnost výpočtu. Pokud jsou zadaná velká čísla, je vhodné za *B* volit taková velká čísla, jako největší prvočíslo dělící *N*. V ostatních případech by samozřejmě měla být hodnota $B < N$. Kdybychom *B* zvolili jinak, potom $D = N$.

d) Eulerova metoda

Jelikož se touto metodou dají rozložit jen čísla, která jsou součtem dvou různých čtvercových čísel, je zapotřebí si buďto zjistit hned před začátkem výpočtu, jestli je dané číslo součtem dvou čtvercových čísel, anebo nám tato metoda v závěru nevyjde. Už zde dochází, jak k časovému zdržení před výpočtem, tak k případnému zbytečnému výpočtu Eulerovy metody pro dané číslo.

Tyto a mnoho dalších algoritmů pro faktorizaci je používáno v nejrůznějších matematických programech a nástrojích, jako například stolní kalkulátor TI - 92 Plus či webové prostředí WolframAlpha.

Porovnání algoritmů z hlediska časové náročnosti

Algoritmy zmiňované v této práci budeme v této kapitole srovnávat pomocí pojmu složitost algoritmu. Jedná se o rychlost algoritmu v závislosti na počtu vykonaných operací.

Každému algoritmu přísluší některá ze tříd složitosti.

Faktorizace dělením:

$O(\frac{2^{\frac{n}{2}}}{(\frac{n}{2}) \cdot log(2)})$ -> charakter jako: $O(k^n)$

Pollardův rho algoritmus:

$O(n^{\frac{1}{4}})$ -> charakter jako: $O(n^k)$

Pollardův p - 1 algoritmus:

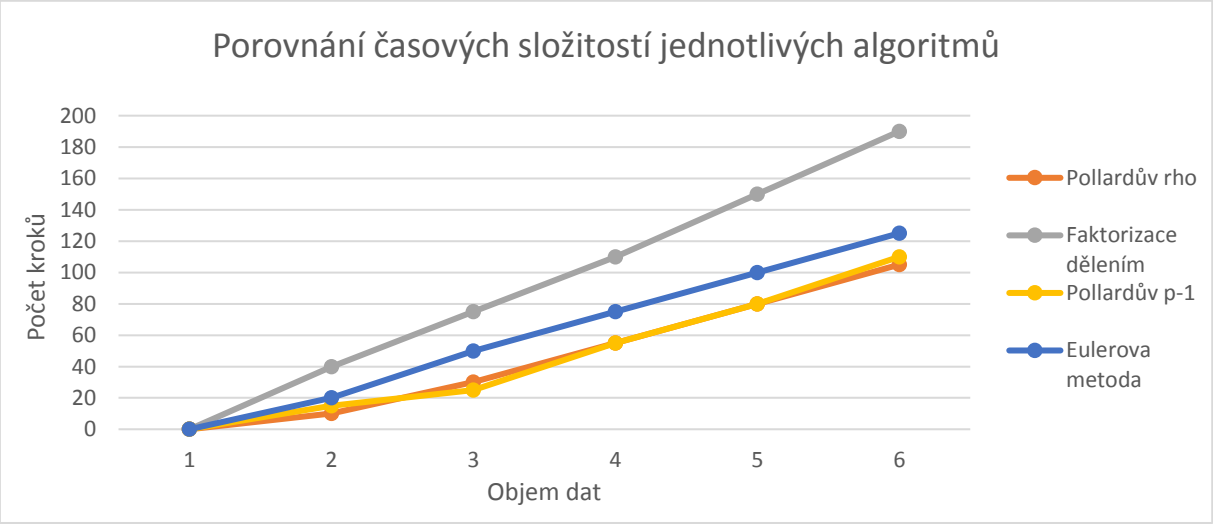
$O(B \cdot log(B) \cdot log^2(n))$ -> charakter jako: $O(n \cdot \log(n))$

Eulerova metoda:

$O(n^{\frac{1}{3}+\varepsilon})$ -> charakter jako: $O(n^k)$

Následující graf se řídí nerovnicí pro porovnání časových složitostí algoritmů v nekonečnu.

$$1 \ll log(n) \ll n \ll n \cdot log(n) \ll n^k \ll k^n \ll n! \ll n^n$$



Obrázek 19: Porovnání časových složitostí

Jak je patrné, Pollardův rho a Pollardův p - 1 algoritmus patří mezi rychlejší metody pro nalezení prvočíselného rozkladu. U Eulerovy metody a metody faktorizací dělením už výrazně roste časová náročnost.

Dle autora textu [10] z Oregonské Univerzity vychází jako srovnání s jejich grafem vizualizace výše uvedeného grafu, který ukazuje porovnání časových složitostí

jednotlivých algoritmů. Mezi podmínky testu, ze kterého vzešel graf z výše uvedeného internetového zdroje, patří například:

a) Každý algoritmus byl otestován celkem stokrát

b) Čísla pro zjišťování prvočíselného rozkladu byla vybírána náhodně z množiny celých čísel

Závěr

Jedním z cílů této práce je seznámení s prvočíselností a faktorizačních metod. Nejprve je vysvětlen důležitý pojem pro tuto práci, tj. prvočíslo, a také prvočíselný rozklad. Tyto pojmy hrají důležitou roli u faktorizačních metod pro nalezení prvočíselného rozkladu u celých čísel.

V druhé kapitole jsou mezi popsanými faktorizačními metodami faktorizace dělením („hrubá“ síla), Pollardův rho algoritmus, Pollardův p - 1 algoritmus a Eulerova metoda. Některé z algoritmů lze využít i pro zvídavé žáky v učitelské praxi.

K těmto metodám bylo v následující kapitole vypočteno několik ilustračních příkladů, které se snažili ukázat početní i časovou náročnost těchto algoritmů, ale také jejich možnosti pro zrychlení výpočtu i jejich úskalí.

Během výpočtů byla použita řada sofistikovanějších zařízeních pro rychlejší výpočet příkladů, a to stolní kalkulátor TI - 92 Plus či webové prostředí WolframAlpha.

Právě časová náročnost je podstatou poslední kapitoly, kde se zabývám pojmy jako složitost algoritmu a třídy složitosti, pomocí kterých můžeme porovnávat algoritmy právě z hlediska času jejich výpočtu.

Resumé

One of the aims of this thesis is to get acquainted with prime numbers and factorization methods. First, an important concept for this thesis, i.e. a prime number, is also explained, as well as a prime quote. These terms play an important role in factorization methods for finding prime numbers in integers.

In the second chapter, there are described the following factoring methods: Trial Factorization, Pollard rho algorithm, Pollard p - 1 algorithm and Euler's method. Some of the algorithms can also be used for inquisitive pupils in teaching practice.

Several illustrative examples have been computed in these chapters, which have attempted to show both the numerical and time demands of these algorithms, but also their possibilities for speeding up the calculations and their obstacles.

During the calculations, a number of more sophisticated devices were used to quickly compute examples, such as the TI - 92 Plus Desktop Calculator and the WolframAlpha Web Environment.

Time-consuming is the essence of the last chapter where I deal with concepts such as the complexity of the algorithm and the complexity class, by which we can compare the algorithms precisely in terms of the time of their calculation.

Seznam obrázků

Obrázek 1: Grafické schéma prvočíselného rozkladu 9
Obrázek 2: Zacyklení Pollardova rho algoritmu 18
Obrázek 3: Kalkulátor TI - 92 Plus 26
Obrázek 4: Průběh výpočtu - Pollardův rho algoritmus 27
Obrázek 5: Průběh výpočtu - Pollardův rho algoritmus 28
Obrázek 6: Zacyklení Pollardova rho algoritmu 28
Obrázek 7: Průběh výpočtu (první část) - Pollardův rho algoritmus 29
Obrázek 8: Průběh výpočtu (druhá část) - Pollardův rho algoritmus 30
Obrázek 9: Průběh výpočtu (třetí část) - Pollardův rho algoritmus 30
Obrázek 10: Zacyklení Pollardova rho algoritmu 31
Obrázek 11: Průběh výpočtu (první část) - Pollardův rho algoritmus 33
Obrázek 12: Průběh výpočtu (druhá část) - Pollardův rho algoritmus 33
Obrázek 13: Průběh výpočtu (třetí část) - Pollardův rho algoritmus 33
Obrázek 14: Průběh výpočtu (čtvrtá část) - Pollardův rho algoritmus 33
Obrázek 15: Zacyklení Pollardova rho algoritmu 35
Obrázek 16: Průběh výpočtu - Pollardův p - 1 algoritmus 36
Obrázek 17: Průběh výpočtu - Pollardův p - 1 algoritmus 37
Obrázek 18: Průběh výpočtu - Pollardův p - 1 algoritmus 38
Obrázek 19: Porovnání časových složitostí 43

Seznam použité literatury a webových zdrojů:

[1] HORA, Jaroslav. *Pollardův ρ - algoritmus pro faktorizaci přirozených čísel*, 2017. South Bohemia Mathematical Letters. Volume 25, No. 1, 34 - 38.

[2] GATHEN, Joachim von zur a Jürgen GERHARD. *Modern Computer Algebra*. 2nd ed. Cambridge: Cambridge University Press, 2003, xiii, 785 s. ISBN 05-218-2646-2.

[3] VERNER, Pavel. *Faktorizace pomocí Pollardovy p - 1 metody*. Praha, 2014. Bakalářská práce. ČVÚT v Praze. Vedoucí práce Ing. Daniel Kobrle.

[4] HILL, Joshua. *Pollard´s p - 1 Factoring Algorithm* [online].

Dostupné z: http://www.untruth.org/~josh/math/pollard-p-1.pdf

[5] VOJÁČEK, Jakub. *Matematika pro každého - Prvočíselný rozklad* [online], 2008.

Dostupné z: https://maths.cz/clanky/118-prvociselny-rozklad, 2008

[6] PRINCE, Jason R.. *Prime Factorization* [online]. Texas A&M University, 2011.

Dostupné z:
http://www.math.tamu.edu/~mpilant/math646/MidtermProjects/Prince_midterm.pdf

[7] *Wikipedia: John M. Pollard* [online]. San Francisco (CA): Wikimedia Foundation, 2001.

Dostupné z: https://de.wikipedia.org/wiki/John_M._Pollard

[8] *Wikipedia: Eratosthénovo síto* [online]. San Francisco (CA): Wikimedia Foundation, 2001.

Dostupné z: https://cs.wikipedia.org/wiki/Eratosthenovo_s%C3%ADto

[9] ŠTUBŇA, Ivan. *Klasické metody faktorizace čísel*. Praha, 2007. Bakalářská práce. Matematicko-fyzikální fakulta, Univerzita Karlova v Praze. Vedoucí práce: RNDr. David Stanovský, Ph.D.

[10] BARNES, Connelly. *Integer Factorization Algorithms* [online], Oregon State University, 2014.

Dostupné z: http://connellybarnes.com/documents/factoring.pdf

[11] Vývojový tým Mendelovy univerzity v Brně. *Přehled typických složitostí algoritmu* [online], 2018.

Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=27620