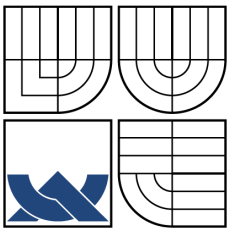
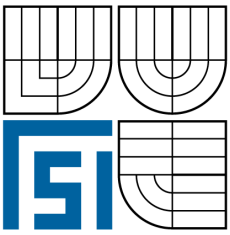


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV MATEMATIKY
FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF MATHEMATICS

UŽITÍ POČÍTAČŮ V TEORII ČÍSEL

THE USE OF COMPUTERS IN THE NUMBER THEORY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

ZDENĚK KONEČNÝ

VEDOUCÍ PRÁCE
SUPERVISOR

prof. RNDr. LADISLAV SKULA, DrSc.

BRNO 2009

Abstrakt
PARI/GP je poměrně málo známý matematický software, který byl navržen především pro rychlé výpočty v teorii čísel, ale našel své uplatnění i v dalších oblastech matematiky. Práce uvádí přehled základních příkazů PARI/GP a na jednoduchých příkladech je ukázáno jejich možné použití. PARI/GP je dále užit k hledání velkých prvočísel speciálních tvarů.

Summary
PARI/GP is a relatively obscure mathematical software that was designed especially for quick calculations in the number theory, but which has also found its application in other areas of mathematics. This work gives an overview of the basic commands of PARI/GP, and some simple examples to show their potential use. PARI/GP is then used for looking for large primes of special forms.

Klíčová slova
Největší společný dělidel, Euklidův algoritmus, prvočíslo, rozklad na prvočísla, PARI/GP

Keywords
Highest common divisor, Euclid's algorithm, prime, integer factorization, PARI/GP

KONEČNÝ, Z. *Užití počítačů v teorii čísel*. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2009. 31 s. Vedoucí prof. RNDr. Ladislav Skula, DrSc.

Prohlašuji, že jsem bakalářskou práci *Užití počitačů v teorii čísel* vypracoval samostatně pod vedením prof. RNDr. Ladislava Skuly, DrSc. s použitím materiálů uvedených v seznamu literatury.

Zdeněk Konečný

Děkuji svému školiteli prof. RNDr. Ladislavu Skulovi, DrSc. za vedení, cenné rady a připomínky při zpracování mé bakalářské práce.

Zdeněk Konečný

Obsah

1 Úvod

Matematický software, v dnešní době nepostradatelný pomocník při řešení většiny úloh inženýrské praxe. Nejčastěji používané programy jsou Maple a Matlab, které mají uplatnění ve všech oblastech matematiky. Vedle těchto univerzálních matematických programů byly vyvinuty programy pro jednotlivé disciplíny matematiky. Tato práce je zaměřena na PARI/GP. Jedná se o algebraický systém určený především pro rychlé výpočty v teorii čísel.

Druhá kapitola je věnována základům aritmetiky celých čísel. Zavedeme zde matematický aparát, který využijeme v následujících kapitolách. Nejdříve připomeneme základní vlastnosti celých čísel. Uvedeme a dokážeme věty o existenci a jednoznačnosti největšího společného dělitele a nejmenšího společného násobku. Ukážeme, že každé celé číslo lze vyjádřit ve tvaru formálně nekonečného součinu a pomocí vlastností exponentů dokážeme existenci největšího společného dělitele a nejmenšího společného násobku na libovolné podmnožině celých čísel.

Ve třetí kapitole je naším cílem podrobněji představit systém PARI/GP. Ukážeme, jak v programu zadávat vektory, matice a polynomy. Uvedeme stručný přehled základních příkazů a na příkladech různé obtížnosti ukážeme jejich použití.

Poslední kapitola je zaměřena na různé varianty důkazu nekonečného počtu prvočísel. Na základě principu každého důkazu se pokusíme pomocí systému PARI hledat prvočísla, jejichž typ vychází z konstrukce důkazu. Prvočísla tvaru $n! \pm 1$ a $p\# \pm 1$ hledali matematikové již v době, kdy ještě nebyl k dispozici počítač. Symbol $p\#$ pro prvočíslo p značí součin všech prvočísel $\leq p$. Užití počítače hledání prvočísel velmi usnadnilo. V současné době mají největší známá prvočísla jednotlivých typů přes 100000 cifer. S využitím systému PARI se pokusíme znovu vyhledat prvočísla těchto typů a ověřit tím výzkum našich předchůdců. V hledání se poté budeme soustředit na prvočísla typu $p\#/2 \pm 2$, o kterých v námi studovaných pramenech není zmínka.

2 Základy aritmetiky celých čísel

2.1 Algebraické vlastnosti celých čísel

Množina celých čísel $\mathbf{Z}$ spolu s operacemi $+$, $\cdot$ tvoří obor integrity – označení $(\mathbf{Z}, +, \cdot)$. Má tedy tyto vlastnosti:

1. $(\mathbf{Z}, +)$ je komutativní grupa.

2. $(\mathbf{Z}, \cdot)$ je komutativní pologrupa s jedničkou 1 s tzv. omezeným zákonem o krácení:

$$ab = ac \Rightarrow b = c \text{ pro každé } a, b, c \in \mathbf{Z}, a \neq 0.$$

3. Pro každé a, b, $c \in \mathbf{Z}$ platí:
   $a \cdot (b + c) = ab + ac$ ... pravý distributivní zákon,
   $(b + c) \cdot a = ba + ca$ ... levý distributivní zákon.

Množina celých čísel $\mathbf{Z}$ s relací $\geq$ tvoří lineární uspořádání.
Pro $(\mathbf{Z}, \geq)$ platí následující pravidla:

$$\begin{array}{lcll} a \geq b & \Rightarrow & a + c \geq b + c & \text{pro každé } a, b \in \mathbf{Z}, c \in \mathbf{R}, \\ a \geq b & \Rightarrow & ac \geq bc & \text{pro každé } a, b \in \mathbf{Z}, c \in \mathbf{R} : c > 0, \\ a \geq b & \Rightarrow & ac \leq bc & \text{pro každé } a, b \in \mathbf{Z}, c \in \mathbf{R} : c < 0, \\ a \geq b & \Rightarrow & ac = bc = 0 & \text{pro každé } a, b \in \mathbf{Z}, c = 0. \end{array}$$

Každému celému číslu a můžeme přiřadit jeho absolutní hodnotu $|a|$ definovanou následovně:

$$|a| = \begin{cases} a & \text{pro } a \geq 0 \\ -a & \text{pro } a < 0 \end{cases}.$$

Pro každé $a, b \in \mathbf{Z}$ platí:

$$|ab| = |a| \cdot |b|.$$

Množinu celých čísel $\mathbf{Z}$ můžeme vyjadřit jako sjednocení tří po dvou disjunktních množin – přirozených čísel $\mathbf{N}$, nuly $\{0\}$ a záporných celých čísel $\mathbf{Z}^-$: $\mathbf{Z} = \mathbf{N} \cup \{0\} \cup \mathbf{Z}^-$.

Při budování aritmetiky přirozených čísel se dokazuje platnost následující věty:

Věta 2.1.1 *Neexistuje nekonečná klesající posloupnost přirozených čísel, tj. posloupnost* $\{a_i\}_0^\infty, a_i \in \mathbf{N} : a_i > a_{i+1}$ *pro každé* $i = 1, 2, \ldots$.

Zřejmě je tato věta ekvivalentní s tvrzením, že každá neprázdná podmnožina množiny přirozených čísel má nejmenší prvek.

2.2 Definice pojmů dělitelnosti a jejich základní vlastnosti

Definice 2.2.1 Nechť a, b jsou celá čísla, řekneme, že a *dělí* b – označení $a|b$, jestliže existuje celé číslo z takové, že

$$b = az.$$

Říkáme také, že a je dělitel b nebo b je násobek a.

Zřejmě $|$ je relace na množině $\mathbf{Z}$, která se nazývá *relace dělitelnosti*.

Tvrzení 2.2.1 *Relace dělitelnosti je reflexivní a tranzitivní.*

Důkaz: 1. Dokážeme reflexivitu: Nechť $a \in \mathbf{Z}$. Jelikož $a = a \cdot 1$, pak $a|a$.
2. Dokážeme tranzitivitu: Nechť $a|b \wedge b|c; a, b, c \in \mathbf{Z}$. Pak existují celá čísla z_1, z_2 s vlastnostmi: $b = az_1, c = bz_2$, tedy $c = a \cdot (z_1 z_2)$. Odtud plyne $a|c$.

Tvrzení 2.2.2 *Nechť $a, b, x, y, z \in \mathbf{Z}, z|x, z|y$. Pak platí:*

$$z|ax + by.$$

Důkaz: Jelikož $z|x, z|y, \exists c, d \in \mathbf{Z}$ taková, že $x = cz, y = dz$. Pak $ax + by = z \cdot (ac + bd)$, tudíž $z|ax + by$.

Definice 2.2.2 Nechť ε je celé číslo. Řekneme, že ε je *jednotka* oboru integrity celých čísel $\mathbf{Z}$, jestliže ε dělí jedničku 1. Množina všech jednotek oboru integrity $\mathbf{Z}$ se označuje symbolem $U(\mathbf{Z})$.

Tvrzení 2.2.3 *Množina všech jednotek celých čísel $U(\mathbf{Z}) = \{1, -1\}$.*

Důkaz: Jedná se o důkaz množinové rovnosti $U = U(\mathbf{Z})$, kde $U = \{1, -1\}$. Jelikož $1|1$ a $(-1)|1$, máme $U \subseteq U(\mathbf{Z})$. Nechť $x \in U(\mathbf{Z})$. Pak existuje $y \in \mathbf{Z}$ takové, že $xy = 1$. Odtud plyne $1 = |1| = |xy| = |x| \cdot |y|$ a z aritmetiky přirozených čísel dostáváme, že $|x| = 1$, neboli $x = \pm 1$. Tudíž $x \in U$.

Definice2.2.3 Celá čísla a, b se nazývají *asociovaná* – označení $a \sim b$, jestliže $\exists \varepsilon \in U(\mathbf{Z})$ takové, že $a = b\varepsilon$.

Zřejmě $\sim$ je relace na množině $\mathbf{Z}$, která se nazývá *relace asociovanosti*.

Tvrzení 2.2.4 *Relace $\sim$ je relace ekvivalence na $\mathbf{Z}$.*

Důkaz: Ekvivalence je relace, která je reflexivní, symetrická a tranzitivní. Musíme tedy dokázat, že relace $\sim$ má tyto vlastnosti. Reflexivita a tranzitivita plyne z vlastností dělitelnosti. Zbývá dokázat symetri. Nechť $a, b \in \mathbf{Z} : a \sim b$, pak $\exists \varepsilon \in U(\mathbf{Z})$ takové, že $a = \varepsilon b$. Vynásobením rovnice jednotkou ε dostáváme: $a\varepsilon = \varepsilon^2 b$. Jelikož platí, že $\varepsilon^2 = 1$, máme $a\varepsilon = b$, tudíž $b \sim a$.

Tvrzení 2.2.5 *Pro $a, b \in \mathbf{Z}$ platí:*

$$a \sim b \Leftrightarrow a|b \wedge b|a.$$

Důkaz: "$\Rightarrow$" Nechť $a \sim b$. Pak $\exists \varepsilon \in U(\mathbf{Z})$ tak, že $a = b\varepsilon$, tudíž $b|a$. Analogicky se ukáže $a|b$.
"$\Leftarrow$" Nechť $a|b, b|a \Rightarrow \exists c, d \in \mathbf{Z}$ tak, že $b = ac, a = bd$, odkud dostáváme $a = acd$. Z toho plyne $cd = 1$. Pak $d, c \in U(\mathbf{Z})$ a platí $a \sim b$.

Věta 2.2.1 (Věta o dělení dvou celých čísel se zbytkem) *Nechť $a, b \in \mathbf{Z}, b \neq 0$. Pak existují celá čísla q, r s vlastnostmi:*

$$a = bq + r, \quad 0 \leq r < |b|.$$

Čísla q, r s těmito vlastnostmi jsou určena jednoznačně.

Důkaz: 1. Dokážeme existenci vyjádření: Položme $M = \{a - bz, z \in \mathbf{Z},\ a - bz \geq 0\}$. Ukážeme, že $a - b \cdot (-\operatorname{sgn} b) \cdot |a| \in M$: $a - b \cdot (-\operatorname{sgn} b) \cdot |a| = a + |b| \cdot |a| \geq a + |a| \geq 0$, jelikož $|b| \geq 1$. Množina M je tedy neprázdná a podle věty 2.1.1 má nejmenší prvek r. Pak existuje celé číslo q takové, že $a - bq = r$, tedy $a = bq + r$. Je-li $|b| \leq r$, pak $0 \leq \leq r - |b| = a - b \cdot (q + \operatorname{sgn} b)$ a tudíž $r - |b| \in M$, což je spor, neboť r byl nejmenší prvek M. Odtud dostáváme $r < |b|$.
2. Dokážeme jednoznačnost čísel q, r: Nechť pro celá čísla q, q_1, r, r_1 platí:

$$\begin{array}{lll} a & = bq & +r, \quad 0 \leq r < |b| \\ a & = bq_1 & +r_1, \quad 0 \leq r_1 < |b|. \end{array}$$

Odečtením obou rovnic obdržíme:

$$0 = b \cdot (q - q_1) + (r - r_1),$$

odkud vyplývá, že $b|(r - r_1)$. Jelikož $0 \leq r < |b|$, $0 \leq r_1 < |b|$, pak také $|r - r_1| < |b|$. Podmínky $b|(r - r_1)$ a $|r - r_1| < |b|$ platí pouze pro $(r - r_1) = 0$, tj pro $r = r_1$. Získáváme $0 = b \cdot (q - q_1)$. Jelikož $b \neq 0$, předcházející rovnice platí pouze pro $q = q_1$. Celá čísla q, r jsou tudíž určena jednoznačně.

Definice 2.2.4 Nechť $a, b \in \mathbf{Z}$, pak celé číslo d se nazývá *společný dělitel* celých čísel a, b, jestliže platí:

$$d|a \wedge d|b.$$

Definice 2.2.5 Nechť $a, b \in \mathbf{Z}$, pak celé číslo d se nazývá *největší společný dělitel* celých čísel a, b, jestliže platí:

1. $d|a \wedge d|b$
2. jestliže $k|a \wedge k|b$ pro nějaké $k \in \mathbf{Z}$, potom $k|d$.

Zřejmě je-li jedno z celých čísel a, b rovno 0, pak je druhé z těchto čísel jejich největší společný dělitel.

Největší společný dělitel celých čísel a, b se dá vypočítat metodou, která se nazývá *Euklidův algoritmus*. Tento algoritmus uvedeme v následující definici a ukážeme, že skutečně udává nějvětšího společného dělitele čísel a, b.

Definice 2.2.6 (Euklidův algoritmus) Nechť $a, b \in \mathbf{Z} - \{0\}$. Podle věty 2.2.1 existuje přirozené číslo n a celá čísla $r_2, \ldots, r_n, q_2, \ldots, q_{n+1}$ s následujícími vlastnostmi:

$$\begin{array}{lll} a & = bq_2 & +r_2, \quad 0 < r_2 < |b| \\ b & = r_2 q_3 & +r_3, \quad 0 < r_3 < r_2 \\ r_2 & = r_3 q_4 & +r_4, \quad 0 < r_4 < r_3 \\ & & \vdots \\ r_{n-2} & = r_{n-1} q_n & +r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} & = r_n q_{n+1}. & \end{array}$$

Jelikož $b > r_2 > \ldots > r_n$, musí být tento proces podle věty 2.1.1 ukončen, tedy uvedený algoritmus je korektní. Pak r_n je největší společný dělitel celých čísel a, b, což nyní dokážeme:

Důkaz: Vyjdeme-li od poslední rovnosti Euklidova algoritmu, dostaneme, že r_n dělí r_{n-1} podle tvrzení 2.2.2. Podobně z předposlední rovnosti obdržíme, že $r_n|r_{n-2}$. Postupně pak dostáváme: $r_n|r_3$ a $r_n|r_2$. Z druhé rovnosti Euklidova algoritmu vyplývá, že $r_n|b$. Z první rovnosti pak dostáváme, že r_n je společným dělitelem a, b.

Nechť $c \in \mathbf{Z}$ je společným dělitelem čísel a, b. Pak z první identity Euklidova algoritmu vyplývá, že c dělí r_2. Z následující identity dostáváme, že c dělí r_3. Postupným užitím dalších rovností dostaneme relaci: c dělí r_n, čímž je dokázáno, že r_n je největším společným dělitelem celých čísel a, b.

Z předchozího důkazu plyne následující věta:

Věta 2.2.2 (Věta o existenci největšího společného dělitele) *Nechť a, b jsou libovolná celá čísla, pak existuje jejich největší společný dělitel.*

Věta 2.2.3 (Věta o „jednoznačnosti“ největšího společného dělitele) *Nechť d je největší společný dělitel celých čísel a,b, pak množina všech největších společných dělitelů je rovna množině*

$$\{\varepsilon \cdot d : \varepsilon \in U(\mathbf{Z})\} = \{d, -d\}.$$

Říkáme, že *největší společný dělitel dvou celých čísel je určen jednoznačně až na asociovanost.*

Důkaz: Položme $A = \{\varepsilon \cdot d : \varepsilon \in U(\mathbf{Z})\}$, $B = \{D \in \mathbf{Z} : D$ je největší společný dělitel celých čísel $a, b\}$. Máme ukázat množinovou rovnost $A = B$.

1. Nechť $\alpha \in A$. Pak $\alpha = \varepsilon d$. Jelikož $d|a$, $d|b$, existují celá čísla c_1, c_2 s vlastností $a = dc_1$, $b = dc_2$. Odtud plyne $a = \varepsilon^{-1}\alpha c_1$, $b = \varepsilon^{-1}\alpha c_2$, tedy $\alpha|a, \alpha|b$.

Nechť $\alpha' \in \mathbf{Z}$, $\alpha'|a$, $\alpha'|b$. Protože d je největší společný dělitel celých čísel a, b platí $\alpha'|d$. Tudíž existuje $c \in \mathbf{Z}$ tak, že $d = \alpha' c$. Odtud $\alpha = \varepsilon\alpha' c$, tedy $\alpha'|\alpha$. Tím jsme dokázali, že $\alpha \in B$ neboli $A \subseteq B$.

2. Nechť $\beta \in B$. Jelikož celá čísla β, d jsou největší společní dělitelé čísel a, b, máme $\beta|d, d|\beta$. Tudíž β, d jsou asociovaná. Existuje tedy $\varepsilon \in U(\mathbf{Z})$ tak, že $\beta = \varepsilon d$. Tím jsme dokázali, že $\beta \in A$ neboli $B \subseteq A$.

Jestliže požadujeme, aby největší společný dělitel bylo číslo nezáporné, pak je určen (striktně) jednoznačně a značí se pro $a, b \in \mathbf{Z}$ symbolem (a, b).

Tvrzení 2.2.6 *Nechť $a, b \in \mathbf{Z}$, pak existují celá čísla x, y tak, že platí:*

$$(a, b) = x \cdot a + y \cdot b.$$

Důkaz: Nechť $a, b \in \mathbf{Z}$. Označme $l(a, b) = \{a \cdot u + b \cdot v : u, v \in \mathbf{Z}\}$.

Dá se ukázat, že pro $e, f, g, z \in \mathbf{Z}$ platí:

$(*)$ jestliže $z \in l(e, f), e \in l(f, g)$, pak $z \in l(f, g)$.

Jestliže b je nulové nebo b dělí a, pak tvrzení zřejmě platí. Nechť $b \neq 0$ a b nedělí a. Pro výpočet (a, b) užijeme Euklidova algoritmu. Pak $(a, b) = r_n$ a z rovnosti $r_{n-2} = r_{n-1}q_n + r_n$, dostáváme $r_n \in l(r_{n-1}, r_{n-2})$. Jelikož $r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$, máme $r_{n-1} \in l(r_{n-2}, r_{n-3})$ a z $(*)$ plyne $r_n \in l(r_{n-2}, r_{n-3})$.

Pro přirozené číslo $k = n-3, \ldots, 3$ pak postupně dostáváme $r_n \in l(r_k, r_{k-1})$. V posledním kroku $(k = 3)$ obdržíme $r_n \in l(r_3, r_2)$. Z druhé rovnosti dostáváme, že $r_3 \in l(r_2, b)$, tudíž podle $(*)$ $r_n \in l(r_2, b)$. Z první rovnosti Euklidova algoritmu získáme, že $r_2 \in l(b, a)$, tudíž $r_n \in l(b, a)$, čímž je tvrzení dokázáno.

Příklad: Nalezněte největšího společného dělitele čísel 17766 a 3066. Dále určete celá čísla x, y, pro která platí:

$$x \cdot 17766 + y \cdot 3066 = (17766, 3066).$$

Řešení: K nalezení největšího společného dělitele použijeme Euklidův algoritmus. Použijeme-li stejné označení jako v definici 1.2.6, máme $a = 17766$, $b = 3066$.

$$\begin{array}{rcrcrcl}
17766 & = & 3066 \cdot 5 & + & 2436 & , & q_2 = 5, r_2 = 2436 \\
3066 & = & 2436 \cdot 1 & + & 630 & , & q_3 = 1, r_3 = 630 \\
2436 & = & 630 \cdot 3 & + & 546 & , & q_4 = 3, r_4 = 546 \\
630 & = & 546 \cdot 1 & + & 84 & , & q_5 = 1, r_5 = 84 \\
546 & = & 84 \cdot 6 & + & 42 & , & q_6 = 6, r_6 = 42 \\
84 & = & 42 \cdot 2 & & & &
\end{array}$$

Poslední nenulový zbytek Euklidova algoritmu je největší společný dělitel čísel 17766 a 3066 $\Rightarrow (17766, 3066) = r_6 = 42$.

Nyní určíme celá čísla x, y, pro která platí:

$$x \cdot 17766 + y \cdot 3066 = (17766, 3066) = r_6 = 42.$$

Rovnice Euklidova algoritmu upravíme na následující identity:

$$\begin{array}{rcrcl}
r_2 & = & a & - & bq_2 \\
r_3 & = & b & - & r_2q_3 \\
r_4 & = & r_2 & - & r_3q_4 \\
r_5 & = & r_3 & - & r_4q_5 \\
r_6 & = & r_4 & - & r_5q_6.
\end{array}$$

Dosadíme do druhé identity za r_2 z první rovnosti. Dostáváme

$$r_3 = -q_3a + b \cdot (q_2q_3 + 1).$$

V dalším kroku dosadíme do třetí rovnosti za r_2 a r_3, čímž dostáváme

$$r_4 = (q_3q_4 + 1) \cdot a - (q_2q_3q_4 + q_4 + q_2) \cdot b$$

Takto pokračujeme, dokud nevyjádříme největšího společného dělitele r_n (v našem případě r_6) jako lineární kombinaci a, b. Získáváme identitu

$r_6 = (q_3q_4q_5q_6 + q_5q_6 + q_3q_6 + q_3q_4 + 1) \cdot a - (q_2q_3q_4q_5q_6 + q_4q_5q_6 + q_2q_5q_6 + q_2q_3q_6 + q_6 + q_4 + q_2) \cdot b$, tudíž

$x = q_3q_4q_5q_6 + q_5q_6 + q_3q_6 + q_3q_4 + 1 = 34$
$y = -(q_2q_3q_4q_5q_6 + q_4q_5q_6 + q_2q_5q_6 + q_2q_3q_6 + q_6 + q_4 + q_2) = -197.$

Definice 2.2.7 Nechť $a, b \in \mathbf{Z}$, pak celé číslo c se nazývá *společný násobek* celých čísel a, b, jestliže platí:

$$a|c \wedge b|c.$$

Definice 2.2.8 Nechť $a, b \in \mathbf{Z}$, pak celé číslo c se nazývá *největší společný násobek* celých čísel a, b, jestliže platí:

1. $a|c \wedge b|c$
2. jestliže $a|k \wedge b|k,$ pro nějaké $k \in \mathbf{Z},$ pak $c|k.$

Zřejmě jestliže je jedno z celých čísel a, b rovno 0, pak je jejich nejmenší společný násobek 0.

2.3 Rozklad celého čísla na prvočísla

Každé celé číslo c má za dělitele čísla $1, -1, c, -c$. Vzhledem k této vlastnosti zavedeme následující definici:

Definice 2.3.1 Nechť $c \in \mathbf{Z} - \{0\}$ a $d \in \mathbf{Z}$ je dělitel čísla c. Dělitel d se nazývá *vlastní dělitel čísla* c, jestliže $d \notin \{1, -1, c, -c\}$, což je ekvivalentní s vlastností $1 < |d| < |c|$. Jestliže $d \in \{1, -1, c, -c\}$, pak se nazývá *nevlastní dělitel čísla* c.

Definice 2.3.2 Celé číslo $c \neq 0$ se nazývá *složené číslo*, jestliže má vlastního dělitele.

Zřejmě $c \in \mathbf{Z} - \{0\}$ je složené číslo, jestliže $\exists a, b \in \mathbf{Z} - \{1, -1, c, -c\}$ s vlastností $c = a \cdot b$, pak a, b jsou vlastní dělitelé čísla c.

Definice 2.3.3 *Prvočíslo* je celé číslo > 1, které není složené.

Příklady: Protože neexistuje celé číslo d takové, že $1 < |d| < |2|$, je 2 nejmenší prvočíslo. Další prvočísla menší než 20 jsou: $3, 5, 7, 11, 13, 17, 19$.

Číslo 4 je číslo složené, neboť $4 = 2 \cdot 2$.

Číslo 117763 je prvočíslo a číslo 372101 je číslo složené, neboť $372101 = 1597 \cdot 233$.

K důkazu hlavní věty tohoto odstavce o rozkladu celého čísla na prvočísla použijeme tvrzení 2.3.1, 2.3.2 a 2.3.3.

Tvrzení 2.3.1 *Každé celé číslo $n > 1$ lze vyjádřit jako součin prvočísel.*

Důkaz: Důkaz provedeme úplnou indukcí vzhledem k n. Jestliže $n = 2$, pak je n prvočíslo a tvrzení platí. Předpokládejme, že $n \geq 2$ a tvrzení platí pro každé celé číslo c, $2 \leq c \leq n$. Ukážeme, že tvrzení platí pro celé číslo $n + 1$. Jestliže $n + 1$ je prvočíslo, pak zřejmě tvrzení platí. Není-li $n + 1$ prvočíslo, pak podle definice 2.3.3 je $n + 1$ číslo složené. Z toho plyne, že existují vlastní dělitelé a, b čísla $n + 1$ tak, že $n + 1 = a \cdot b$. Odtud $2 \leq a, b \leq n$, což znamená, že podle indukčního předpokladu jsou čísla a, b součiny prvočísel, čímž je tvrzení dokázáno.

Tvrzení 2.3.2 *Nechť $a, b, c \in \mathbf{Z} - \{0\}$. Pak platí:*

$$(a, b) = 1, a|bc \Rightarrow a|c.$$

Důkaz: Jestliže $(a, b) = 1$, pak podle tvrzení 2.2.6 existují celá čísla x, y tak, že $1 = ax + by$. Rovnost rozšíříme číslem c. Dostáváme

$$(*) \quad c = acx + bcy.$$

Jelikož $a|bc$, pak exisuje celé číslo z tak, že $bc = az$. Dosadíme za bc z předchozí identity do rovnosti $(*)$.

$$c = acx + azy = a \cdot (cx + zy)$$

Odtud plyne, že $a|c$.

Tvrzení 2.3.3 *Nechť $p, b_1, ..., b_k \in \mathbf{Z}, k \in \mathbf{N}$ a p je prvočíslo. Pak platí:*

$$p|b_1 \cdot \ldots \cdot b_k \Rightarrow \exists i \in \mathbf{Z}, 1 \leq i \leq k : p|b_i.$$

Důkaz: Důkaz provedeme sporem. Nechť $p \nmid b_j$, $j = 1, \ldots, k$. Jelikož $p \nmid b_1$, pak $(p, b_1) = 1$ a podle tvrzení 2.3.2 dostáváme $p|b_2 \ldots b_k$. Po $k - 1$ krocích dostáváme $p|b_k$, což je spor.

Věta 2.3.1 (O jednznačnosti rozkladu celého čísla na prvočísla) *Každé celé číslo $c \notin \{0, 1, -1\}$ se dá vyjádřit ve tvaru*

$$c = \varepsilon p_1 \cdot \ldots \cdot p_k,$$

kde $\varepsilon \in \{1, -1\} = U(\mathbf{Z})$, $k \in \mathbf{N}$, $p_1, \ldots, p_k$ jsou prvočísla. Přičemž toto vyjádření je jednoznačné až na pořadí prvočísel $p_1, \ldots, p_k$.

Důkaz: Můžeme předpokládat, že $c \geq 1$. Nechť $c = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_h$, kde $k, h \in \mathbf{N}$ a $p_1, \ldots, p_k, q_1, \ldots, q_h$ jsou prvočísla.

Jestliže $p_1|q_1 \cdot \ldots \cdot q_h$, pak podle tvrzení 2.3.3 existuje $i \in \mathbf{Z}$, $1 \leq i \leq h$ tak, že $p_1|q_i$. Z toho plyne, že $p_1 = q_i$. Prvočísla $q_1, \ldots, q_h$ uspořádáme tak, že q_i bude na prvním místě, tedy $i = 1$. Pak

$$p_1 p_2 \cdot \ldots \cdot p_k = p_1 q_2 \cdot \ldots \cdot q_h \Rightarrow p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_h.$$

Jestliže $k = h$, pak po $k - 1$ krocích získáme $p_1 = q_1, \ldots, p_k = q_k$. Bez újmy na obecnosti předpokládejme, že $k < h$. Pak po k krocích dostaneme

$$p_k = p_k q_{k+1} \cdot \ldots \cdot q_h \Rightarrow 1 = q_{k+1} \cdot \ldots \cdot q_h,$$

což je spor.

Definice 2.3.4 Z věty 2.3.1 plyne, že každé celé číslo $c \notin \{0, 1, -1\}$ lze napsat ve tvaru

$$c = \varepsilon p_1^{a_1} \cdot \ldots \cdot p_l^{a_l},$$

kde $\varepsilon \in \{1, -1\} = U(\mathbf{Z})$, $l \in \mathbf{N}$, $p_1, \ldots, p_l$ jsou navzájem různá prvočísla a $a_1, \ldots, a_l \in \mathbf{N}$.

Toto vyjádření se nazývá *kanonický tvar čísla c*. Z věty 2.3.1 plyne, že toto vyjádření je jednoznačné až na pořadí prvočísel $p_1, \ldots, p_l$.

Pro prvočíslo p_i $(1 \leq i \leq l)$ označíme exponent a_i symbolem $v_{p_i}(c)$ a nazveme *exponent čísla c vzhledem k prvočíslu* p_i. Pro prvočíslo $p \notin \{p_1, \ldots, p_l\}$ položíme $v_p(c) = 0$. Dále položíme $v_p(1) = v_p(-1) = 0$ pro každé prvočíslo p.

Pak můžeme číslo c psát ve tvaru takzvaného *formálně nekonečného součinu*:

$$c = \varepsilon \prod_{p \in \mathcal{P}} p^{v_p(c)},$$

kde $\mathcal{P}$ je množina všech prvočísel a pro $c = \pm 1$ je $\varepsilon = c$. Ve formálně nekonečném součinu se všichni činitelé s výjimkou konečně mnoha rovnají jedné. Součin nekonečně mnoha jedniček klademe roven 1.

Pro exponenty platí následující tvrzení:

Tvrzení 2.3.4 *Pro $a, b \in \mathbf{Z} - \{0\}$ a každé prvočíslo p platí:*

$$v_p(a \cdot b) = v_p(a) + v_p(b).$$

Důkaz: Celá čísla $a, b \neq 0$ si vyjádříme ve tvaru formálně nekonečného součinu.

$$a = \varepsilon_a \prod_{p \in \mathcal{P}} p^{v_p(a)}, \ b = \varepsilon_b \prod_{p \in \mathcal{P}} p^{v_p(b)},$$

kde $\varepsilon_a, \ \varepsilon_b \in \{1, -1\}$. Pro součin $a \cdot b$ platí:

$$\varepsilon_{ab} \prod_{p \in \mathcal{P}} p^{v_p(ab)} = a \cdot b = \varepsilon_a \prod_{p \in \mathcal{P}} p^{v_p(a)} \cdot \varepsilon_b \prod_{p \in \mathcal{P}} p^{v_p(b)} = \varepsilon_a \varepsilon_b \prod_{p \in \mathcal{P}} p^{v_p(a)} \cdot p^{v_p(b)} = \varepsilon_a \varepsilon_b \prod_{p \in \mathcal{P}} p^{v_p(a)+v_p(b)},$$

kde $\varepsilon_{ab} = \varepsilon_a \varepsilon_b \in \{1, -1\}$. Odtud $v_p(a \cdot b) = v_p(a) + v_p(b)$.

Tvrzení 2.3.5 *Pro $a, b \in \mathbf{Z} - \{0\}$ platí:*

$$a|b \Leftrightarrow v_p(a) \leq v_p(b) \text{ pro každé } p \in \mathcal{P}.$$

Důkaz: "⇒" Jelikož $a|b$, existuje celé číslo c tak, že $b = a \cdot c$. Podle tvzení 1.3.4 dostáváme $v_p(a \cdot c) = v_p(a) + v_p(c)$. Tedy $v_p(b) = v_p(a) + v_p(c)$. Exponent $v_p(c)$ je číslo nezáporné (plyne z definice 2.3.4). Tudíž $v_p(a) \leq v_p(b)$.
"⇐" Nechť $v_p(a) \leq v_p(b)$ pro každé $p \in \mathcal{P}$. Ostrá nerovnost $v_p(a) < v_p(b)$ platí pro nejvýše konečně mnoho p (plyne z definice 2.3.4). Buď $c \in \mathbf{Z}$ takové, že $v_p(a) + v_p(c) = v_p(b)$. Pak z tvzení 1.3.4 plyne, že $ac = b$. Odtud $a|b$.

Tvrzení 2.3.6 *Pro $a, b \in \mathbf{Z} - \{0\}$ a každé prvočíslo p platí:*

$$v_p((a, b)) = min\{v_p(a), v_p(b)\}.$$

Důkaz: Položme $d = \prod_{p \in \mathcal{P}} p^{min\{v_p(a), v_p(b)\}}$. Platí tedy, že $v_p(d) = min\{v_p(a), v_p(b)\}$ pro každé $p \in \mathcal{P}$. Zřejmě $v_p(d) \leq v_p(a) \wedge v_p(d) \leq v_p(b)$. Podle tvrzení 2.3.5 $d|a \wedge d|b$, tudíž d je společný dělitel a, b.

Nechť c je společný dělitel a, b. Pak $c|a \wedge c|b$ a podle tvrzení 2.3.5 platí, že $v_p(c) \leq$ $\leq v_p(a) \wedge v_p(c) \leq v_p(b)$ pro každé $p \in \mathcal{P}$. Odtud $v_p(c) \leq min\{v_p(a), v_p(b)\}$. Tedy $v_p(c) \leq$ $\leq v_p(d)$ a podle tvrzení 2.3.5 dostáváme $c|d$, čímž je dokázáno, že d je největší společný dělitel celých čísel a, b.

Tvrzení 2.3.7 *Nechť $a, b \in \mathbf{Z} - \{0\}$, pak existuje jejich nejmenší společný násobek c a pro každé prvočíslo p platí:*

$$v_p(c) = max\{v_p(a), v_p(b)\}.$$

Důkaz: Položme $c = \prod_{p \in \mathcal{P}} p^{max\{v_p(a), v_p(b)\}}$. Platí tedy, že $v_p(c) = max\{v_p(a), v_p(b)\}$ pro každé $p \in \mathcal{P}$. Zřejmě $v_p(a) \leq v_p(c) \wedge v_p(b) \leq v_p(c)$. Podle tvrzení 2.3.5 $a|c \wedge b|c$, tudíž c je společný násobek a, b.

Nechť m je společný násobek a, b. Pak $a|m \wedge b|m$ a podle tvrzení 2.3.5 platí, že $v_p(a) \leq$ $\leq v_p(m) \wedge v_p(b) \leq v_p(m)$ pro každé $p \in \mathcal{P}$. Odtud $v_p(m) \geq max\{v_p(a), v_p(b)\}$. Tedy $v_p(m) \geq v_p(c)$ a podle tvrzení 2.3.5 dostáváme $c|m$, čímž je dokázáno, že c je nemenší společný násobek celých čísel a, b.

Věta 2.3.2 *Nechť c je nejmenší společný násobek celých čísel a, b, pak množina všech nejmenších společných násobků je rovna množině*

$$\{\varepsilon \cdot c : \varepsilon \in U(\mathbf{Z})\} = \{c, -c\}.$$

Říkáme, že *nejmenší společný násobek dvou celých čísel je určen jednoznačně až na asociovanost.*

Důkaz: Položme $A = \{\varepsilon \cdot c : \varepsilon \in U(\mathbf{Z})\}$, $B = \{C \in \mathbf{Z} : C$ je nejmenší společný násobek celých čísel $a, b\}$. Máme ukázat množinovou rovnost $A = B$.

1. Nechť $\alpha \in A$. Pak $\alpha = \varepsilon c$. Jelikož $a|c$, $b|c$, existují celá čísla k_1, k_2 s vlastností $c = ak_1$, $c = bk_2$. Předchozí identity pro c rozšíříme ε. Dostáváme $\varepsilon c = \varepsilon ak_1$, $\varepsilon c = \varepsilon bk_2$, tedy $\alpha = \varepsilon ak_1$, $\alpha = \varepsilon bk_2$. Odtud $a|\alpha,\ b|\alpha$.

Nechť $\alpha' \in \mathbf{Z}$, $a|\alpha'$, $b|\alpha'$. Protože c je nejmenší společný násobek celých čísel a, b platí $c|\alpha'$. Tudíž existuje $k \in \mathbf{Z}$ tak, že $\alpha' = ck$. Odtud $\alpha' = \varepsilon^{-1}\alpha c$, tedy $\alpha|\alpha'$. Tím jsme dokázali, že $\alpha \in B$ neboli $A \subseteq B$.

2. Nechť $\beta \in B$. Jelikož celá čísla β, c jsou nejmenší společné násobky čísel a, b, máme $\beta|c, c|\beta$. Tudíž β, c jsou asociovaná. Existuje tedy $\varepsilon \in U(\mathbf{Z})$ tak, že $\beta = \varepsilon c$. Tím jsme dokázali, že $\beta \in A$ neboli $B \subseteq A$.

Jestliže požadujeme, aby nejmenší společný násobek bylo číslo nezáporné, pak je určen (striktně) jednoznačně a značí se pro $a, b \in \mathbf{Z}$ symbolem $[a, b]$.

Lemma 2.3.1 *Pro $x, y \in \mathbf{Z}$ platí:*

$$x + y = min\{x, y\} + max\{x, y\}.$$

Důkaz: Bez újmy na obecnosti předpokládejme, že $x \leq y$. Pak $min\{x, y\} = x$ a $max\{x, y\} = y$. Odtud $min\{x, y\} + max\{x, y\} = x + y$.

Věta 2.3.3 *Pro $a, b \in \mathbf{Z}$ platí:*

$$a \cdot b = (a, b) \cdot [a, b].$$

Důkaz: 1. Buď jedno z celých čísel a, b rovno 0. Bez újmy na obecnosti předpokládejme $a = 0$, pak $a \cdot b = 0, (a, b) = b$ a $[a, b] = 0$. Odtud plyne $a \cdot b = (a, b) \cdot [a, b] = 0$.

2. Nechť $a, b \in \mathbf{Z} - \{0\}$. Podle tvrzení 2.3.4 pro součin ab platí: $v_p(ab) = v_p(a) + v_p(b)$ pro každé $p \in \mathcal{P}$. Tvrzení 2.3.4 použijeme i na pravou stranu dokazované rovnosti. Dostáváme $v_p((a, b) \cdot [a, b]) = v_p((a, b)) + v_p([a, b])$ pro každé $p \in \mathcal{P}$. Pomocí tvrzení 2.3.6 a 2.3.7 převedeme předchozí rovnost na tvar $v_p((a, b) \cdot [a, b]) = min\{v_p(a), v_p(b)\} + max\{v_p(a), v_p(b)\}$. Užitím lemmatu 2.3.1 dostáváme $v_p((a, b) \cdot [a, b]) = v_p(a) + v_p(b)$. Odtud $v_p(ab) = v_p((a, b) \cdot [a, b])$. Z čehož plyne $a \cdot b = (a, b) \cdot [a, b]$.

Definice 2.3.5 Nechť $M \subseteq \mathbf{Z}$, pak celé číslo d se nazývá *společný dělitel* množiny M, jestliže pro každé $m \in M$ platí:

$$d|m.$$

Definice 2.3.6 Nechť $M \subseteq \mathbf{Z}$, pak celé číslo d se nazývá *největší společný dělitel* množiny M, jestliže pro každé $m \in M$ platí:

1. $d|m$
2. jestliže $k|m$ pro nějaké $k \in \mathbf{Z}$, potom $k|d$.

Je-li $M = \emptyset$, klademe $d = 0$.

Věta 2.3.4 *Nechť $M \subseteq \mathbf{Z}$, pak existuje její největší společný dělitel d. Jestliže $M - \{0\} \neq \emptyset$, pak pro každé prvočíslo p platí:*

$$v_p(d) = min\{v_p(m) : m \in M - \{0\}\}.$$

Je-li $M - \{0\} = \emptyset$, pak $d = 0$.

Důkaz: Pro $M - \{0\} = \emptyset$ je tvrzení zřejmé. Položme $d = \prod_{p \in \mathcal{P}} p^{min\{v_p(m) : m \in M\}}$. Platí tedy, že $v_p(d) = min\{v_p(m) : m \in M\}$ pro každé $p \in \mathcal{P}$. Exponent $v_p(d)$ je různý od 0 jen pro konečně mnoho prvočísel. Jelikož $v_p(d) \leq v_p(m)$ pro každé $m \in M$, dostáváme podle tvrzení 2.3.5 $d|m$, tudíž d je společný dělitel M.

Nechť c je společný dělitel množiny M. Pak $c|m$ pro každé $m \in M$ a podle tvrzení 2.3.5 dostáváme $v_p(c) \leq v_p(m)$ pro každé $m \in M, p \in \mathcal{P}$. Tedy $v_p(c) \leq min\{v_p(m) : m \in M) = v_p(d)$. Odtud podle tvrzení 2.3.5 plyne $c|d$. d je tedy největší společný dělitel množiny M.

Nechť $0 \in M$. Jelikož každé celé číslo dělí 0, platí, že největší společný dělitel množiny M je roven největšímu společnému děliteli $M - \{0\}$. Odtud $v_p(d) = min\{v_p(m) : m \in M - \{0\}\}$.

Definice 2.3.7 Nechť $M \subseteq \mathbf{Z}$, pak celé číslo c se nazývá *společný násobek* množiny M, jestliže pro každé $m \in M$ platí:

$$m|c.$$

Definice 2.3.8 Nechť $M \subseteq \mathbf{Z}$, pak celé číslo c se nazývá *nejmenší společný násobek* množiny M, jestliže pro každé $m \in M$ platí:

1. $m|c$
2. jestliže $m|k$ pro nějaké $k \in \mathbf{Z}$, potom $c|k$.

Je-li $M = \emptyset$, klademe $c = 1$.

Věta 2.3.5 *Nechť $M \subseteq \mathbf{Z}$, pak existuje její nejmenší společný násobek c. Jestliže $M \neq \emptyset$ a $0 \notin M$,pak pro každé prvočíslo p platí:*

$$v_p(c) = max\{v_p(m) : m \in M\}.$$

Je-li $M = \emptyset$, pak nejmeší společný násobek množiny M je roven 1. Jestliže $0 \in M$, pak nejmeší společný násobek množiny M je roven 0.

Důkaz: Pro $M = \emptyset$ a $0 \in M$ je tvrzení zřejmé. Položme $c = \prod_{p \in \mathcal{P}} p^{\max\{v_p(m):m\in M\}}$. Platí tedy, že $v_p(c) = max\{v_p(m) : m \in M\}$ pro každé $p \in \mathcal{P}$. Exponent $v_p(c)$ je různý od 0 jen pro konečně mnoho prvočísel. Jelikož $v_p(c) \geq v_p(m)$ pro každé $m \in M$, dostáváme podle tvrzení 2.3.5 $m|c$, tudíž c je společný násobek M.

Nechť x je společný násobek množiny M. Pak $m|x$ pro každé $m \in M$ a podle tvrzení 2.3.5 dostáváme $v_p(x) \geq v_p(m)$ pro každé $m \in M, p \in \mathcal{P}$. Tedy $v_p(x) \geq max\{v_p(m) : m \in M) = v_p(c)$. Odtud podle tvrzení 2.3.5 plyne $c|x$. c je tedy největší společný násobek množiny M.

Poznámka: Množina $\mathbf{N}_0 = \mathbf{N} + \{0\}$ spolu s relací dělitelnosti tvoří uspořádání- označení $(\mathbf{N}_0, |)$. Dále pro každé $a, b \in \mathbf{N}_0$ platí:

- $(a, b) = \inf\{a, b\}$
- $[a, b] = \sup\{a, b\}$.

Z toho plyne, že každé dva prvky a, b z uspořádané množiny $(\mathbf{N}_0, |)$ mají infimum a supremum. $(\mathbf{N}_0, |)$ je tedy svaz s nejmenším prvkem 1 a největším prvkem 0.

Svaz $(\mathbf{N}_0, |)$ je úplný. To znamená, že každá $M \subseteq \mathbf{N}_0$ ma infimum a supremum. Pro každou $M \subseteq \mathbf{N}_0$ platí:

- $\inf M$ = největší společný dělitel množiny M
- $\sup M$ = nejmenší společný násobek množiny M.

Je-li $M = \emptyset$, pak

- $\inf M$ = největší prvek $(\mathbf{N}_0, |) = 1$
- $\sup M$ = nejmenší prvek $(\mathbf{N}_0, |) = 0$.

3 PARI/GP

PARI/GP je široce užívaný algebraický systém navržený pro rychlé výpočty v teorii čísel (faktorizace, eliptické křivky, ...). Obsahuje také velké množství užitečných funkcí pro počítání s matematickými objekty jako jsou matice, polynomy, mocninné řady, atd., a mnoho transcendetních funkcí.

Původní verzi vyvinul Henri Cohen se svými spolupracovníky. V současné době je PARI volně šiřitelný software. Ve své práci používám nejnovější verzi PARI 2.3.4 z roku 2008.

3.1 Užitečné příkazy a příklady jejich použití

Nejdříve si ukážeme, jak se v PARI vytváří některé matematické objekty.

- Řádkové vektory se zadávají do hranatých závorek, kde jednotlivé prvky oddělujeme čárkou.
```
> [5,-7,123]
%1 = [5, -7, 123]
```

- Sloupcový vektor se vytváří obdobně jako řádkový, jen s tím rozdílem, že za vektor přidáváme znak ~.
```
> [5,-7,123]~
%1 = [5, -7, 123]~
```

- Matice zadáváme do hranatých závorek, přičemž prvky v řádku oddělujeme čárkou a řádky středníkem.
```
> [13,-17;23,121;-9,93]
%1 =
[13 -17]
[23 121]
[-9 93]
```

- Polynomy zapisujeme následovně: $a_n * x\hat{}n + a_{n-1} * x\hat{}(n-1) + \ldots + a_1 * x + a_0$, kde $a_0, a_1, \ldots, a_n$ jsou reálná čísla a $n \in \mathbf{N}$.
```
> x^5-4*x^3+7
%1 = x^5 - 4*x^3 + 7
> -x^11+6*x^7+12/7*x^3+113/29*x
%2 = -x^11 + 6*x^7 + 12/7*x^3 +113/29*x
```

Nyní uvedeme přehled užitečných příkazů systému PARI a na příkladech ukážeme jejich použití.

Divrem, syntaxe: *divrem*(x, y), provede dělení se zbytkem čísla x číslem y. Vrací dvousložkový sloupcový vektor $[a, b]$, kde první složka je kvocient ($a = [x/y]$) a druhá zbytek ($b = x - [x/y] \cdot y$). Tento příkaz můžeme použít i v případě, když x, y jsou polynomy. Pak a, b jsou polynomy takové, že $x = a \cdot y + b$ a stupeň polynomu b je menší než stupeň polynomu y.

```
> divrem(100,17)
%1 = [5, 15]~
> divrem(154568,1454)
%2 = [106, 444]~
> divrem(5^11,11^5-12)
%3 = [303, 33308]~
> divrem(3*x^8-11*x^6+9*x^3+3*x-3,x^4-2*x^3+4)
%4 = [3*x^4 + 6*x^3 + x^2 + 2*x - 8, -31x^3 - 4*x^2 - 5*x +29]~
```

Max, *max(x, y)*, určí maximum z čísel x a y.

```
> max(87,94)
%1 = 94
> max(5^6-4^7+369,7^5-2^8-11^2)
%2 = 16430
> 7^5-2^8-11^2
%3 = 16430
```

Min, *min(x, y)*, určí minimum z čísel x a y.

```
> min(25,37)
%1 = 25
> min(19^4-16^5+29^2*1084,8^5-7^6+8*3^9)
%2 = -6611
> 19^4-16^5+29^2*1084
%3 = -6611
```

Vecmax, *vecmax(x)*, zjistí maximum z prvků vektoru či matice x.

```
> vecmax([763,-845,965,764-863,368+412,23^2])
%1 = 965
```

Vecmin, *vecmin(x)*, zjistí minimum z prvků vektoru či matice x.

```
> vecmin([763,-845,965,764-863,368+412,23^2])
%1 = -845
```

Mod, *Mod(x, y)*, určí nejmenší nezáporné číslo, s kterým je x kongruentní modulo y.

```
> Mod(81,18)
%1 = Mod(9, 18)
> Mod(604799887,3651)
%2 = Mod(784, 3651)
> Mod(93^3-45^4, 23)
%3 = Mod(0, 23)
```

Lift, *lift(x)*, vrací zbytek z $x = \mathrm{Mod}(a, b)$.

```
> lift(Mod(91,17))
%1 = 6
> lift(Mod(6^7-11^3+200356,136))
%2 = 105
```

Simplify, *simplify(x)*, zjednoduší objekt x.

```
> simplify([18/15,156/12,96/14])
%1 = [6/5, 13, 48/7]
> simplify(7^3/28+537/15)
%2 = 961/20
> simplify([3850/150,-653/296;(-9^4+1)/123,856/34])
%3 =
[77/3 -653/296]
[-160/3 428/17]
```

Denominator, *denominator(x)*, vypočte nejmenšího jmenovatele x. V případě, že x je vektor nebo matice, určí nejmenšího společného jmenovatele.

```
> denominator(3216/4827)
%1 = 1609
> denominator([99,14103,729]/63)
%2 = 7
```

Numerator, *numerator(x)*, vypočte nejmenšího čitatele x.

```
> numerator(96/42)
%1 = 16
> numerator(16-8667/972)
%2 = 85
```

Random, *random(N)*, vybere náhodné celé číslo z intervalu $\langle 0, N-1\rangle$. V případě, že N není uvedeno, je voleno automaticky $N = 2^{31}$.

```
> random(100)
%1 = 59
> random()
%2 = 1634689150
```

Round, *round(x)*, zaokrouhlí x na celé číslo.

```
> round(3.49999)
%1 = 3
> round(-99.662347)
%2 = -100
```

Floor, *floor(x)*, vrací celou část x– označení $[x]$, tj. největší celé číslo a takové, že $a \leq x$.

```
> floor(-7.1)
%1 = -8
> floor(1632/711+2.78^4-3.652)
%2 = 58
```

Ceil, *ceil(x)*, vrací nejmenší celé číslo b takové, že $b \geq x$. Platí $b = [x] + 1$.

```
> ceil(-7.1)
%1 = -7
> ceil(9635.138-7448.954-365.25)
%2 = 1821
```

Frac, *frac(x)*, určí lomenou část x– označení $\{x\}$. Platí $\{x\} = x - [x]$.

```
> frac(-17.21)
%1 = 0.79000000000000000000000000
> frac(96325/6597-7^3/11)
%2 = 30443/72567
```

Sqr, *sqr(x)*, spočítá druhou mocninu x.

```
> sqr(-2.5)
%1 = 6.25000000000000000000000000
> sqr(576/126)
%2 = 1024/49
```

Sqrt, *sqrt(x)*, zjistí druhou odmocninu x.

```
> sqrt(5)
%1 = 2.23606797749978969640917366
> sqrt(173^3/61^2)
%2 = 37.302618586362321985467381 71
```

Sqrtn, *sqrtn(x, n)*, spočte n-tou odmocninu x, $n \in \mathbf{Z}$.

```
> sqrtn(2,-1)
%1 = 1/2
> sqrtn(27^4+63^5,9)
%2 = 9.9921621208361180386183042 02
> sqrtn(153^3,-6)
%3 = 0.0808452083454444506302154 04
```

Gcd, *gcd(x, y)*, určí největšího společného dělitele celých čísel či polynomů x, y.

```
> gcd(9690,24871)
%1 = 323
> gcd(24^5-12^3,9093-2361)
%2 = 612
> gcd(x^4-9*x^3-18x^2-239*x-105,5*x^4+4*x^3-191*x^2+202*x+140)
%3 = x^2 + 2*x - 35
```

Lcm, *lcm(x, y)*, vypočte nejmenší společný násobek celých čísel či polynomů x, y.

```
> lcm(9690,24871)
%1 = 746130
> lcm(67^3-541^2,118087)
%2 = 2125566
> lcm(x^3+4*x^2-51*x-54,2*x^4-4*x^3-42*x^2-36*x)
%3 = 2*x^5 + 14*x^4 - 78*x^3 -414*x^2 - 324*x
```

Bezout, *bezout(x, y)*, dává třírozměrný vektor $[u, v, d]$, kde d je největší společný dělitel x, y a u, v jsou nejmenší celá čísla taková, že $u \cdot x + v \cdot y = d$. Příkaz bezout můžeme použít i pro polynomy.

```
> bezout(33,54)
%1 = [5, -3, 3]
> bezout(96044,51744)
%2 = [2843, -5277, 4]
```

Factor, *factor(x)*, provede kanonický rozklad x.

```
> factor(-5525)
%1 =
[-1 1]
[5 2]
[13 1]
[17 1]
> factor(2^71-1)
%2 =
[228479 1]
[48544121 1]
[212885833 1]
```

Divisors, *divisors(x)*, dává vektor, jehož prvky jsou kladní dělitelé x, seřazeni dle velikosti.

```
> divisors(980)
%1 = (1, 2, 4, 5, 7, 10, 14, 20, 28, 35, 49, 70, 98, 140, 196, 245, 490, 980)
> divisors(30317)
%2 = [1, 7, 61, 71, 427, 497, 4331, 30317]
```

Moebius, *moebius(x)*, spočte Möbiovu funkci $\mu(x)$.

```
> moebius(18)
%1 = 0
> moebius(7^5-12^4)
%2 = -1
```

Eulerphi, *eulerphi(x)*, určí Eulerovu funkci $\varphi(x)$. Eulerova funkce $\varphi(x)$ udává počet čísel posloupnosti $0, 1 \ldots, x-1$ nesoudělných s x.

```
> eulerphi(53)
%1 = 52
> eulerphi(166400)
%2 = 61400
```

Issquare, *issquare(x)*, výsledek je 1, pokud x je druhá mocnina (čtverec). Když x není druhá mocnina, vrací 0.

```
> issquare(83)
%1 = 0
> issquare(87534736)
%2 = 1
```

Prime, *prime(n)*, zjistí n-té prvočíslo.

```
> prime(30)
%1 = 113
> prime(9999)
%2 = 104723
```

Primes, *primes(n)*, vrátí vektor prvních n prvočísel.

```
> primes(25)
%1 = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,
67, 71, 73, 79, 83, 89, 97]
```

Isprime, *isprime(x)*, vrací 1, pokud x je prvočíslo. V případě, že x není prvočíslo, obdržíme 0.

```
> isprime(17)
%1 = 0
> isprime(27^4+11^5+477^2-3460)
%2 = 1
> isprime(2^prime(963)-1)
%3 = 0
```

Nextprime, *nextprime(x)*, určí nejmenší prvočíslo větší nebo rovno x.

```
> nextprime(24)
%1 = 29
> nextprime(86547.456)
%2 = 86561
```

Fibonacci, *fibonacci(x)*, dává x-té Fibonacciho číslo.

```
> fibonacci(11)
%1 = 89
> fibonacci(38)
%2 = 39088169
```

Sum, *sum(*$X = a, b, expr, \{x\}$*)*, provede součet výrazu *expr* v proměnné x pro $x = a, a+1, \ldots, b$.

```
> sum(x=1,5,sqr(x))
%1 = 55
> sum(x=1,20,(x^3+2*x)*isprime(x))
%2 = 15957
```

Prod, *prod(*$X = a, b, expr, \{x\}$*)*, provede součin výrazu *expr* v proměnné x pro $x = a, a+1, \ldots, b$.

```
> prod(x=1,5,x)
%1 = 120
> prod(x=3,10,(x^2+fibonacci(x))/x)
%2 = 21596288725/1512
```

4 Varianty důkazu o nekonečném počtu prvočísel

Věta 4.1 *Prvočísel je nekonečně mnoho.*

Existuje mnoho způsobů, jak dokázat předchozí větu. V této kapitole uvedeme některé varianty důkazu a pomocí systému PARI se pokusime nalézt velká prvočísla, jejichž tvar je založen na principech důkazů.

4.1 Euklidův důkaz

Důkaz: Předpokládejme, že množina všech prvočísel $\mathcal{P} = \{p_1, p_2, \ldots, p_r\}$ je konečná, $p_1 = 2 < p_2 = 3 < \ldots < p_r, r \in \mathbf{N}$. Položme $P = p_1 p_2 \cdot \ldots \cdot p_r + 1$. Nechť p je prvočíslo dělící P. Pokud $p \in \mathcal{P}$, pak $p|p_1 p_2 \cdot \ldots \cdot p_r$. Užitím tvrzení 2.2.2 dostáváme $p|1$, což je spor. Z toho plyne, že prvočíslo $p \notin \mathcal{P}$, tedy množina $\mathcal{P}$ neobsahuje všechna prvočísla, což je spor s předpokladem.

Další způsob, jak dokázat větu 4.1 spočívá v lehké modifikaci Euklidova důkazu.

Důkaz: Předpokládejme, že množina všech prvočísel $\mathcal{P} = \{p_1, p_2, \ldots, p_r\}$ je konečná, $p_1 = 2 < p_2 = 3 < \ldots < p_r, r \in \mathbf{N}$. Položme $P = p_1 p_2 \cdot \ldots \cdot p_r - 1$. Nechť p je prvočíslo dělící P. Pokud $p \in \mathcal{P}$, pak $p|p_1 p_2 \cdot \ldots \cdot p_r$. Odtud podle tvrzení 2.2.2 dostáváme $p|-1$, což je spor. Z toho plyne, že prvočíslo $p \notin \mathcal{P}$, tedy množina $\mathcal{P}$ neobsahuje všechna prvočísla, což je spor s předpokladem.

Pro každé prvočíslo p zavedeme funkci $p\#$. Funkce $p\#$ je definována jako součin všech prvočísel q takových, že $q \leq p$. V anglické literatuře se funkce $p\#$ nazývá *primorial function*.

Euklidův důkaz je velmi jednoduchý, ale nedává nám žádné informace o dalším prvočísle, víme jen, že je nejvýše rovno číslu $P = p_r\# + 1$, ale může být i menší.

4.2 Hledání velkých prvočísel

Při hledání velkých prvočísel se matematikové zaměřili na hledání prvočísel konkrétních tvarů. Zjišťovali, pro která prvočísla p jsou čísla $P = p\# \pm 1$ prvočísly. Pro tato prvočísla se v anglickém jazyce užívá termín *primorial primes*. Dalším zajímavým typem prvočísel jsou prvočísla tvaru $n! \pm 1, n \in \mathbf{N}$, anglický termín: *factorial primes*. Ověření, zda získané číslo je skutečně prvočíslem, vyžaduje velké množství výpočtů.

Největší pokrok v hledání velkých prvočísel umožnil až objev počítače. V roce 1972 vyšel v časopise Mathematics of Computation článek Alana Borninga, ve kterém zveřejnil své výsledky v hledání prvočísel typu $p\# \pm 1$ a $n! \pm 1$. Ke všem výpočtům použil počítač IBM 1130. Určil všechna prvočísla typu $n! \pm 1$ pro $n = 2, 3, \ldots, 100$ a typu $p\# \pm 1$ pro všechna prvočísla $p \leq 307$. Předchozí výsledky, které poskytl Sierpiński, byly pouze pro všechna $n \leq 26$ v případě $n! + 1$, pro typ $n! - 1$ jen pro $n \leq 22$ a $n = 25$. Dále Kraitchik určil kanonické rozklady $n! + 1$ pro $n \leq 22$, $n! - 1$ pro $n \leq 21$, $p\# + 1$ pro $p \leq 53$ a $p\# - 1$

pro všechna $p \leq 47$. Pomocí počítače Alan Borning verifikoval výsledky, které poskytli Sierpiński a Kraitchik. Zjistil ve výpočtech matematiků následující chyby:

1. Sierpiński vynechal v seznamu prvočísel typu $n! + 1$ prvočíslo $3! + 1$.

2. Sierpiński i Kraitchik chybně označili číslo $20! - 1$ jako prvočíslo.

3. Kraitchik opomněl uvést činitele 5171 kanonického rozkladu čísla $21! - 1$.

Užijme nyní systém PARI k ověření závěrů Alana Borninga.

```
> isprime(3!+1)
%1 = 1
> isprime(20!-1)
%2 = 0
> factor(21!-1)
%3 =
[23 1]
[89 1]
[5171 1]
[4826713612027 1]
```

Naše výpočty potvrzují výsledky, které zveřejnil Alan Boring.

Významné úspěchy v hledání velkých prvočísel typu $p\#\pm1$ a $n!\pm1$ zaznamenal Harvey Dubner. Své výsledky zveřejnil v článku Factorial and primorial primes, který vyšel v roce 1987 v časopise Journal of Recreational Mathematics. Sestavil tabulky prvočísel typu $p\# + 1$ pro všechna prvočísla $p \leq 17159$, $p\# - 1$ pro $p \leq 16699$, $n! + 1$ pro všechna $n \leq$ ≤ 2662 a $n! - 1$ pro $n \leq 2063$. V tabulce 4.2.1 jsou uvedena největší prvočísla jednotlivých typů, která objevil Harvey Dubner. Ve své době to byla největší známá prvočísla daných typů vůbec. U prvočísel $15877\# - 1$ a $1963! - 1$ si nebyl zcela jistý. Jednalo se pouze o předpovědi, které byly později potvrzeny.

Prvočíslo	Počet cifer
$13649\# + 1$	4591
$15877\# - 1$	6845
$1477! + 1$	4042
$1963! - 1$	5614

Tabulka 4.2.1: Největší prvočísla jednotlivých typů objevená Harvey Dubnerem

4.3 Vyhledávání prvočísel pomocí PARI

V této části se pokusíme zopakovat výzkum, který provedl Harvey Dubner. Ukážeme, jak lze pomoci PARI hledat prvočísla typu $n! \pm 1$ a $p\# \pm 1$.

Zaměřme se nejdříve na prvočísla typu $n!+1$. Naším cílem bude určit včechna prvočísla $n!+1$ pro $n \leq 1000$. V PARI lze velmi jednoduše zjistit, zda pro konkrétní n je číslo $n!+1$ prvočíslo. Výpočet si ukážeme pro případ $n = 732$.

```
> isprime(732!+1)
%1 = 0
```

Vidíme, že číslo $732! + 1$ je číslo složené. Tento způsob hledání je ale velmi nepraktický, protože pro každé n musíme příkaz zadávat znovu. Bylo by velmi výhodné, kdybychom mohli provést výpočt pro více n současně. Toho docílíme pomocí příkazu *sum*. Díky příkazu *sum*, můžeme určit počet prvočísel pro všechna přirozená čísla na libovolném intervalu. Příklad výpočtu uvedeme pro $n = 100, 101, \ldots, 300$.

```
> sum(n=100,200,expr=isprime(n!+1))
%2 = 2
```

Tímto jsme zjistili, že číslo $n! + 1$ je prvočíslem právě pro dvě přirozená čísla n z intervalu $\langle 100, 300\rangle$. Přesnou hodnotu těchto čísel můžeme určit metodou půlení intervalu. Tímto postupem nalezneme prvočísla $116! + 1$ a $154! + 1$. Takto určíme i zbylá prvočísla pro $n \leq 1000$. V tabulce 4.3.1 jsou uvedena všechna $n \leq 1000$, pro která je $n! + 1$ prvočíslo. Doba výpočtu udává čas potřebný k ověření, zda číslo $n!+1$ je prvočíslo příkazem *isprime*. Počet cifer určíme pomocí vlastnosti logaritmu– ukážeme pro $154! + 1$.

```
> ceil(log((154!+1)+1)/log(10))
%3 = 272
```

n	Počet cifer	Čas výpočtu
1	1	0 ms
2	1	0 ms
3	1	0 ms
11	8	0 ms
27	29	0 ms
37	44	0 ms
41	50	16 ms
73	106	47 ms
77	114	63 ms
116	191	312 ms
154	272	891 ms
320	665	18,344 s
340	715	24,031 s
399	867	42,672 s
427	940	56,516 s
872	2188	17 min 17,406 s

Tabulka 4.3.1: Hodnoty $n \leq 1000$, pro které je $n! + 1$ prvočíslo

Naprosto stejným způsobem jako prvočísla typu $n! + 1$ nalezneme i všechna prvočísla typu $n! - 1$ pro $n \leq 1000$, viz tabulka 4.3.2. Prvočíslo $974! - 1$ nelze v PARI ověřit, jelikož číslo $974! - 1$ je příliš velké– dochází k tzv. přetečení.

n	Počet cifer	Čas výpočtu
3	1	0 ms
4	2	0 ms
6	3	0 ms
7	4	0 ms
12	9	0 ms
14	11	0 ms
30	33	16 ms
32	36	16 ms
33	37	15 ms
38	45	32 ms
94	147	1,234 s
166	298	18,735 s
324	675	7 min 43,609 s
379	815	15 min 1,250 s
469	1051	45 min 57,172 s
546	1260	1 h 44 min 58,297 s
974	2490	v PARI neurčeno

Tabulka 4.3.2: Hodnoty $n \leq 1000$, pro které je $n! - 1$ prvočíslo

Nyní se budeme zabývat hledáním prvočísel typu $p\# \pm 1$. Nejprve ukážeme, jak v PARI určit číslo $p\#$ pro konkrétní prvočíslo p– např. pro $p = 53$. Pro jistotu se nejdříve pomocí příkazu *isprime* ujistíme, že 53 je skutečně prvočíslo.

```
> isprime(53)
%4 = 1
```

Uspořádejme prvočísla podle velikosti. Dostáváme posloupnost $(p_k)_{k=1}^{\infty} = 2, 3, 5, \ldots$, kde $p_k \in \mathcal{P}$ a pro každé $i, j \in \mathbf{N}$, takové, že $i < j$ platí: $p_i < p_j$. Kombinací příkazů *prod* a *prime* spočteme součin všech prvočísel $q \leq p = 53$. Příkaz *prime*(n) vrací n-té prvočíslo, tedy člen p_n posloupnosti $(p_k)_{k=1}^{\infty}$. Potřebujeme tedy zjistit index prvočísla 53. K tomu použijeme příkaz *primepi*(x), který vrací index největšího prvočísla, které je menší nebo rovno x.

```
> primepi(53)
%5 = 16
```

Zjistili jsme, že prvočíslo 53 je prvek p_{16} posloupnosti $(p_k)_{k=1}^{\infty}$. Nyní spočteme pomocí příkazů *prod* a *prime* součin členů $p_1, \ldots, p_{16}$ posloupnosti prvočísel $(p_k)_{k=1}^{\infty}$, což odpovídá číslu $53\#$.

```
> prod(x=1,16,expr=prime(x))
%6 = 32589158477190044730
```

Pomocí PARI jsme spočetli, že $53\# = 32589158477190044730$.

Když umíme zadat číslo $p\#$ pro libovolné p, nic nám již nebrání v hledání prvočísel typu $p\# \pm 1$. Hledání provedeme pro všechna prvočísla $p \leq 5000$, tj. pro prvočísla $p_1 =$

$2, p_2 = 3, \ldots, p_{668} = 4993, p_{669} = 4999$. Ověření, zda číslo $p\# + 1$ (respektive $p\# - 1$) je prvočíslo, můžeme provést stejně jako v případě prvočísel typu $n! + 1$ (respektive $n! - 1$). Opět můžeme výpočet provádět postupně pro konkrétní prvočísla nebo pomocí příkazu *sum* zjistit počet prvočísel daného typu pro větší počet p současně a metodou půlení intervalu dohledat konkrétní hodnoty p. Výpočet pomocí příkazu *sum* ukážeme pro prvočísla $p_{100}, p_{101}, \ldots, p_{200}$ a typ $p\# + 1$.

```
> sum(a=100,200,expr=isprime(prod(x=1,a,expr=prime(x))+1))
%7 = 2
```

Tímto jsme zjistili, že $p\#+1$ je prvočíslo právě pro dvě prvočísla z posloupnosti $(p_a)_{a=100}^{200}$. Metodou půlení intervalu nalezneme přesné hodnoty indexu a– 171 a 172. Číslo $p\# + 1$ je tedy prvočíslo pro $p_{171} = prime(171) = 1019$ a pro $p_{172} = prime(172) = 1021$. Takto určíme i zbylá prvočísla p, pro která je $p\# + 1$ (respektive $p\# - 1$) prvočíslo, viz tabulka 4.3.3. Tabulka 3.2.3 dále uvadí počet cifer prvočísla daného typu a dobu trvaní výpočtu potřebného k ověření, zda se skutečně jedná o prvočíslo příkazem *isprime*.

$p\# + 1$			$p\# - 1$		
p	Počet cifer	Čas výpočtu	p	Počet cifer	Čas výpočtu
2	1	0 ms	3	1	0 ms
3	1	0 ms	5	2	0 ms
5	2	0 ms	11	4	0 ms
7	3	0 ms	13	5	0 ms
11	4	0 ms	41	15	0 ms
31	12	0 ms	89	35	16 ms
379	154	62 ms	317	131	937 ms
1019	425	2,328 s	337	136	1,032 s
1021	428	2,406 s	991	413	1 min 22,968 s
2657	1115	1min 4.203 s	1873	790	13 min 8,688 s
3229	1368	2 min 8,391 s	2053	866	19 min 5,797 s
4547	1939	7 min 27,765 s	2377	1077	41 min 51,062 s
4787	2038	8 min 54,953 s	4093	1750	6 h 47 min 19,094 s
			4297	1844	5 h 33 min 2,656 s
			4583	1953	v PARI neurčeno

Tabulka 4.3.3: Prvočísla typu $p\# + 1$ a $p\# - 1$ pro $p < 5000$

Vývoj informační technologie umožňuje nalézání stále větších a větších prvočísel. Tabulka 4.3.4 uvádí přehled největších, doposud známých, prvočísel daných typů.

Prvočíslo	Počet cifer	Rok objevení
$392113\# + 1$	169966	2001
$15877\# - 1$	6845	1992
$26951! + 1$	107707	2002
$34790! - 1$	142891	2002

Tabulka 4.3.4: Největší známá prvočísla jednotlivých typů

4.4 Další typy prvočísel

Vraťme se zpět k důkazu věty 4.1. Nejdříve uvedeme další variantu důkazu, ketrá je opět založena na Euklidově důkazu a na závěr se větu 4.1 pokusíme dokázat obecněji.

Důkaz: Předpokládejme, že množina všech prvočísel $\mathcal{P} = \{p_1, p_2, \ldots, p_r\}$ je konečná, $p_1 = 2 < p_2 = 3 < \ldots < p_r, r \in \mathbf{N}$. Položme $P = p_2 p_3 \cdot \ldots \cdot p_r + 2$ (tzn. P je rovno součinu všech lichých prvočísel +2). Jelikož $\mathcal{P}$ je množina všech prvočísel, existuje prvočíslo $p \in \mathcal{P}$ takové, že $p|P$.

Nechť $p = 2$, pak podle tvrzení 2.2.2 dostáváme $2|p_2 p_3 \cdot \ldots \cdot p_r$, což neplatí, jelikož součin lichých čísel je číslo liché. Z toho plyne $p \neq 2$.

Nechť $p \neq 2$, tedy $p \in \mathcal{P} - \{2\}$. Užitím tvrzení 2.2.2 obdržíme $p|2$, což ale neplatí, jelikož jsme předpokládali, že p je liché prvočíslo. Odtud $p \notin \mathcal{P} - \{2\}$.

Zjistili jsme, že $p \notin \mathcal{P} - \{2\} \wedge p \neq 2$. Tedy prvočíslo $p \notin \mathcal{P}$, což je spor s předpokladem.

Stejným způsobem bychom důkaz provedli i pro případ $P = p_2 p_3 \cdot \ldots \cdot p_r - 2$.

Pomocí funkce $p\#$ můžeme číslo $P = p_2 p_3 \cdot \ldots \cdot p_r \pm 2$ zapsat ve tvaru $P = p_r\#/2 \pm 2$. Pokusíme se nyní pomocí systému PARI určit všechna prvočísla $p < 5000$, pro která je $p\#/2 + 2$ (respektive $p\#/2 - 2$) prvočíslo. Hledání provedeme podobně jako v případě prvočísel typu $p\# \pm 1$. Opět použijeme příkazu *sum* a metody půlení intervalu. Ukážeme pro prvočísla $p_{100}, \ldots, p_{200}$ a typ $p\#/2 - 2$.

```
> sum(a=100,200,expr=isprime(prod(x=2,a,expr=prime(x))-2))
%1 = 4
```

Číslo $p\#/2 - 2$ je tedy prvočíslo právě pro čtyři prvočísla z posloupnosti $p_{100}, \ldots, p_{200}$. Přesnou hodnotu indexů určíme metodou půlení intervalu. Nalezli jsme tak prvočísla $p_{103}\#/2 - 2, p_{122}\#/2 - 2, p_{128}\#/2 - 2, p_{145}\#/2 - 2$, kde $p_{103} = 563, p_{122} = 673, p_{128} = 723, p_{145} = 829$. Tímto způsobem určíme i zbývající prvočísla $p < 5000$, pro která je $p\#/2 + 2$ (respektive $p\#/2 - 2$) prvočíslo, viz tabulka 4.4.1.

Větu 4.1 jsme ve všech případech dokazovali konstrukcí čísla P, pro které jsme vždy sporem ukázali, že je dělitelné „novým“ prvočíslem, které neleží v uvažované množině všech prvočísel $\mathcal{P}$. V následujícím důkazu provedeme konstrukci čísla P obecněji.

Důkaz: Předpokládejme, že množina všech prvočísel $\mathcal{P} = \{p_1, p_2, \ldots, p_r\}$ je konečná, $p_1 = 2 < p_2 = 3 < \ldots < p_r, r \in \mathbf{N}$. Nechť $\mathcal{P}_1, \mathcal{P}_2 \subseteq \mathcal{P}$, $\mathcal{P}_1 \cup \mathcal{P}_2 = \mathcal{P}$ a $\mathcal{P}_1 \cap \mathcal{P}_2 = \emptyset$. Položme $P = \prod_{p_i \in \mathcal{P}_1} p_i \pm \prod_{p_j \in \mathcal{P}_2} p_j$. Pro případ $\mathcal{P}_k = \emptyset$ definujeme $\prod_{p_k \in \mathcal{P}_k} p_k = 1$. Jelikož $\mathcal{P}$ je množina všech prvočísel, existuje prvočíslo $p \in \mathcal{P}$ takové, že $p|P$.

Nechť $p \in \mathcal{P}_1$. Užitím tvrzení 2.2.2 dostáváme $p| \prod_{p_j \in \mathcal{P}_2} p_j$. Pak podle tvrzení 2.3.3 existuje $p_j \in \mathcal{P}_2$ takové, že $p|p_j$. Neboť p i p_j jsou prvočísla, musí platit $p = p_j$, což je spor, protože $p \in \mathcal{P}_1, p_j \in \mathcal{P}_2$ a $\mathcal{P}_1 \cap \mathcal{P}_2 = \emptyset$. Odtud plyne $p \notin \mathcal{P}_1$.

Stejným způsobem bychom dokázali, že $p \notin \mathcal{P}_2$. Ukázali jsme, že $p \notin \mathcal{P}_1 \wedge p \notin \mathcal{P}_2$. Tedy $p \notin \mathcal{P}_1 \cup \mathcal{P}_2 = \mathcal{P}$, což je spor s předpokladem.

$p\#/2+2$		$p\#/2-2$	
p	Počet cifer	p	Počet cifer
3	1	5	2
5	2	7	3
7	3	11	4
13	5	13	5
29	10	17	6
31	12	19	7
37	13	23	9
47	18	31	12
59	21	41	15
109	45	53	20
223	87	71	27
307	123	103	41
389	159	167	66
457	188	431	174
1117	473	563	228
1151	482	673	281
2273	959	723	301
–	–	829	347
–	–	1801	764
–	–	2699	1146
–	–	4481	1909

Tabulka 4.4.1: Prvočísla typu $p\#/2+2$ a $p\#/2-2$ pro $p < 5000$

Z předchozího důkazu vyplývá, že číslo P můžeme zkonstruovat mnoha způsoby. Má-li množina všech prvočísel $\mathcal{P}$ r prvků, pak podmnožinu $\mathcal{P}_1$ množiny P můžeme sestavit 2^r způsoby a $\mathcal{P}_2 = \mathcal{P} - \mathcal{P}_1$. Na základě těchto konstrukcí čísla P lze potom odvodit další typy prvočísel a následně pomocí systému PARI hledat jejich reprezentanty.

Zvolme například $\mathcal{P}_1 = \{p_{2i-1} : p_{2i-1} \in \mathcal{P}, i = 1, 2, \ldots, [(r+1)/2]\}$ (tj. množina všech prvočísel z $\mathcal{P}$, jejichž index je lichý) a $\mathcal{P}_2 = \{p_{2i} : p_{2i} \in \mathcal{P}, i = 1, 2, \ldots, [r/2]\}$ (tj. množina všech prvočísel z $\mathcal{P}$, jejichž index je sudý). Hledejme, pro která $p = p_r$ je číslo $P^* = \prod_{p_i \in \mathcal{P}_1} p_i + \prod_{p_j \in \mathcal{P}_2} p_j$ prvočíslo. Hledání provedeme pro všechna $p \leq p_{800} = 6133$. Určení pomocí PARI ukážeme pro prvních 100 prvočísel.

```
> sum(r=1,100,expr=isprime(prod(x=1,floor((r+1)/2),expr=prime(2*x-1))+
prod(x=1,floor(r/2),expr=prime(2*x))))
%2 = 22
```

$P^* = \prod_{p_i \in \mathcal{P}_1} p_i + \prod_{p_j \in \mathcal{P}_2} p_j$, kde $\mathcal{P}_1 = \{p_{2i-1} : p_{2i-1} \in \mathcal{P}, i = 1, 2, \ldots, [(r+1)/2]\}$ a $\mathcal{P}_2 = \{p_{2i} : p_{2i} \in \mathcal{P}, i = 1, 2, \ldots, [r/2]\}$, je tedy prvočíslo právě pro 22 prvočísel p z posloupnosti $p_1, \ldots, p_{100}$. Přesné hodnoty p určíme opět metodou půlení intervalu. Tímto způsobem nalezneme všechna prvočísla $p \leq 6133$, pro která je $P^* = \prod_{p_i \in \mathcal{P}_1} p_i + \prod_{p_j \in \mathcal{P}_2} p_j$ prvočíslo, viz tabulka 4.4.2.

p	Počet cifer P^*	p	Počet cifer P^*
2	1	101	20
3	1	109	23
5	2	137	28
7	2	157	32
11	3	271	56
13	3	379	78
17	4	701	147
19	4	709	149
23	5	863	182
29	6	1259	265
31	7	2393	511
41	8	2939	628
43	9	3527	747
47	10	4943	1053
59	12	5023	1077
79	16	5237	1120

Tabulka 4.4.2: Prvočísla $p \leq 6133$, pro která je P^* prvočíslo

5 Závěr

Práce je rozdělena na tři hlavní části. První část je věnována základům aritmetiky celých čísel. Autor si zde osvojil základy elementární teorie čísel, tvorbu matematických textů a především problematiku důkazů vět a tvrzení.

Druhá část je zaměřena na matematický program PARI/GP. Cílem bylo představit čtenáři tento algebraický systém, který patří mezi méně známé matematické programy a nachází své uplatnění především v teorii čísel. Byl uveden přehled základních příkazů systému PARI/GP a na jednoduchých příkladech bylo ukázáno jejich možné použití.

Cílem poslední části bylo ukázat uplatnění systému PARI/GP při řešení úloh z teorie čísel. Byly uvedeny různé varianty důkazu nekonečného počtu prvočísel. Pomocí systému PARI/GP byla hledána prvočísla, jejichž tvar byl založen na principu jednotlivých důkazů. Prvočísly typu $n!\pm 1$ a $p\#\pm 1$ se zabývali matematikové již dříve. Největší průlom v hledání těchto prvočísel zaznamenal Harvey Dubner, jehož výzkum byl v této práci pomocí PARI verifikován. Dále bylo ukázáno, že lze hledat prvočísla i dalších typů– například typu $p\#/2 \pm 2$, jejichž vyšetřováním se v autorem studované litratuře nikdo nezabýval. Takto byla určena prvočísla, jejichž délka nepřevyšuje 3000 cifer. Hledání větších prvočísel už pomocí PARI není možné– dochází k tzv. přetečení.

Literatura

[1] BORNING, A.: Some results for $k! \pm 1$ and $2 \cdot 3 \cdot 5 \cdots p \pm 1$. *Mathematics of Computation*, 1972, vol. 26, s. 567-570.

[2] BUHLER, J.P., Crandall, R. E., Penk, M. A.: Primes of the form $n! \pm 1$ and $2 \cdot 3 \cdot 5 \cdots p \pm 1$. *Mathematics of Computation*, 1982, vol. 38, s. 639-643.

[3] DUBNER, H.: Factorial and primorial primes. *Journal of Recreational Mathematics*, 1987, vol. 19(3), s. 197-203.

[4] DUBNER, H., DUBNER, R.: The development of a powerful, low-cost computer for number theory. *Journal of Recreational Mathematics*, 1985-86, vol. 18(2), s. 81-86.

[5] HORÁK, P.: *Algebra a teoretickká aritmetika I.* Brno: MU, 1991. 196 s. ISBN 80-210-0320-0.

[6] KARÁSEK, J., SKULA, L.: *Obecná algebra.* Brno: Akademické nakladatelství CERM, 2008. 64 s. ISBN 978-80-214-3794-4.

[7] KUČERA, R., SKULA, L.: *Číselné obory.* Brno: MU, 1998. 95 s. ISBN 80-210-1965-4.

[8] RIBENBOIM, P.: *The book of prime number records.* New York: Springer-Verlag, 1988.

[9] VINOGRADOV, I.M.: *Základy theorie čísel.* Praha: Československá akademie věd, 1953. 173 s.

[10] *PARI/GP.* [online]. Poslední revize 16. 1. 2008.
URL: <http://pari.math.u-bordeaux.fr/>, [cit. 5. 4. 2009].

[11] *The top twenty.* [online]. Poslední revize 19. 4. 2009.
URL: <http://primes.utm.edu/top20/home.php>, [cit. 20. 4. 2009].

6 Seznam použitých zkratek a symbolů

$\mathbf{N}$	množina všech kladných celých čísel
$\mathbf{Z}$	množina všech celých čísel
$\mathcal{P}$	množina všech prvočísel
$p\#$	součin všech prvočísel menších nebo rovných prvočíslu p, viz strana 21