Základy elementární teorie čísel
Karel Lepka

Úvodní slovo autora

Významný německý matematik Karl Friedrich Gauss napsal, že matematika je královna věd a teorie čísel je královnou matematiky. Je skutečností, že bez čísel by matematika nebyla matematikou. Samozřejmě že již nepovažujeme čísla za základ světa jako Pýthágorás a jeho škola, ale je pravdou, že čísla mají v matematice hlubší význam než je počítání. Tento učební text obsahuje základní poznatky z elementární teorie čísel.

Kapitola 1

Teorie dělitelnosti

V této kapitole se seznámíme s pojmy teorie dělitelnosti jako jsou dělitelnost čísel, nejmenší společný násobek, největší společný dělitel. Dále se seznámíme s kritérii dělitelnosti.

1.0.1 Základní pojmy a věty

Tuto část začneme letitou žertovnou hádankou. Babička má pět vnoučat a dvanáct jablíček. Jak to má udělat, aby všechna vnoučata byla spravedlivě podělena? Správná odpověď je, že jim udělá štrůdl. Ve výše uvedeném případě babička jinou možnost nemá, pokud by však přikoupila další tři jablíčka, tak by každému vnoučkovi dala tři jablíčka a mohla by si ušetřit práci se štrůdlem. Babička ovšem může dvě jablíčka dětem zatajit, ta zbudou a opět vnuky spravedlivě poděli, tentokrát ovšem jen dvěma jablíčky.

Nyní převedeme uvedený příklad do jazyka matematického a zobecníme ho, jinými slovy dokážeme následující větu. Každé celé číslo a můžeme jednoznačným způsobem vyjádřit ve tvaru

$$a = bq + r,$$

kde b je kladné číslo a r je celé číslo vyhovující podmínce $0 \geq r < b$.

Důkaz provedeme sporem. Předpokládejme, že platí $a = bq_1 + r_1$ a současně $a = bq_2 + r_2$. Odečteme-li od druhé rovnice první, obdržíme $0 = b(q_2 - q_1) + r_2 - r_1$, tedy $r_2 - r_1$ je násobkem b. Jelikož však je $|r_2 - r_1|$, musí platit $r_1 = r_2$ a tedy i $q_1 = q_2$.

Úloze, ve které se má k dané dvojici celých čísel a, b na jít dvojici čísel q, r splňující vztah (), se říká *dělení*; číslo a nazýváme *dělenec*, číslo b *dělitel*. Zaměřme nyní svou pozornost na číslo r. Pro $r > 0$ mluvíme o *dělení se zbytkem*. V tomto případě je q *částečný podíl* a q je *zbytek*. Je-li $r = 0$, mluvíme o *dělení beze zbytku*; číslo q se nazývá *podíl*. Říkáme též, že číslo a je dělitelné číslem b, což budeme znašit $b|a$. Říkáme, že a je *násobkem* b.

Pozor! Zbytek je vždy číslo nezáporné, tedy $-41 = 11.(-4) + 3$, nikoliv $-41 = (-3).11 - 8$.

Platí následující věty:

Věta 1.1 *Je-li a násobkem m a je-li současně m násobkem b, pak a je násobkem m.*

Věta 1.2 *Jsou-li v rovnosti typu $k + l + \ldots + n = p + q + \ldots + s$ všechny členy s výjimkou jednoho násobkem b, pak i tento člen je násobkem b.*

Věta 1.3 *Nechť $a|b$ a $a|c$. Pak a—$(bx+cy)$ pro libovolná celá čísla a a y.*

Důslekem této věty je skutečnost, že pokud číslo a dělí čísla b a c, pak dělí i jejich součet a rozdíl.

Věta 1.4 *Nechť $a|b$. Pak $a|bc$, kde c je libovolné celé číslo.*

Věta 1.5 *Nechť $a|b$ a současně $b|c$. Pak $a|c$.*

Této vlastnosti se říká *tranzitivita.* Důkazy těchto tvrzení jsou snadné a doporučujeme, aby si je čtenář udělal jako cvičení.

Naskýtá se otázka, jak poznat je-li číslo a dělitelné číslem b. Ve věku počítačů a kalkulaček se zdá být nejjednodušší tato čísla prostě vydělit. Autor má sice velký obdiv k moderní výpočetní technice, přesto však ani tato si neumí s mnoha otázkami teorie čísel poradit. V některých případech by bylo nasazení této techniky zbytečné, asi jako jít s kanonem na vrabce, neboť dělitelnost můžeme poznat mnohem snadněji. Uvedeme si proto několik kritérií pro dělitelnost čísel, zejména pro případy, kdy je dělitel malé číslo.

Věta 1.6 *Přirozené číslo n je dělitelné:*
a) dvěma, je-li poslední cifra sudá,
b) třemi, je-li jeho ciferný součet dělitelný třemi,
c) čtyřmi, je-li jeho poslední dvojčíslí dělitelné čtyřmi,
d) pěti, je-li jeho poslední cifra 0 nebo 5,
e) šesti, je-li sudé a dělitelné 3,
f) sedmi, je-li dvojnásobek počtu stovek zvětšený o poslední dvojčíslí dělitelný 7,
g) osmi, je-li poslední trojčíslí dělitelné 8,
h) devíti, je-li jeho ciferný součet dělitelný 9,
i) desíti, je-li jeho poslední cifra 0.

Důkaz: Každé přirozené číslo n lze v dekadické číselné soustavě vyjádřit následujícím způsobem:

$$n = c_k 10^k + \cdots + c_2 10^2 + c_1 10 + c_0,$$

kde $c_i \in \{0, 1, 2, \ldots, 9\}$ a $c_k \neq 0$. Z tohoto vyjádření okamžitě plynou tvrzení a), c), d), g) a i).

Nechť

$$s = c_k + \cdots + c_2 + c_1 + c_0$$

je ciferný součet čísla n. Pak je

$$n - s = (10^k - 1)c_k + \cdots + 99c_2 + 9c_1.$$

Jelikož každý sčítanec na pravé straně je dělitelný devíti a stejně tak je dělitelné devíti číslo s, musí být dělitelné devíti i číslo n. Tím je dokázáno h) a současně i b).

Zbývá dokázat kritérium pro dělitelnost sedmi. Dvojnásobek stovek čísla n zvětšený o poslední dvojčíslí je roven

$$m = 2c_k 10^{k-2} + \cdots + 2c_2 + 1010c_1 + c_0.$$

Rozdíl

$$n - m = 98c_k 10^{k-2} + \cdots + 98c_2$$

je dělitelný sedmi, protože $7|98$. Jelikož platí $7|m$, musí být číslo ndělitelné sedmi.

Kritérium dělitelnosti sedmi je oproti zbývajícím poměrně komplikované a pro praxi nepříliš vhodné. Uvedeme jednoduchý příklad. Chceme-li zjistit, zda je číslo 7056 dělitelné sedmi, musíme postupovat následujícím způsobem. 70.7+56=546. 546:7=48. Číslo m je dělitelné sedmi, je tedy i 7056 dělitelné sedmi. Kritéria pro dělitelnost dvojcifernými prvočísly menšími než dvacet může čtenář najít např. v [2] na str. 31 resp. 164. Nyní si uvedeme několik úloh na dělitelnost čísel.

Příklad: Určete, jaký den bude za 39 dní, je-li dnes středa.

Řešení: 39=7.5+4. Za 39 dní bude neděle

Příklad: Dokažte, že výraz $a(a+1)(2a+1)$ je dělitelný 6 pro libovolné celé číslo a.

Řešení: $a(a+1)(2a+1) = a(a+1)(a+2) + a(a+1)(a-1)$. Oba sčítance jsou součinem tří po sobě jdoucích čísel, jedno z nich musí být dělitelné 3 a nejméně jedno musí být dělitelné 2.

Příklad 1: Dokažte, že pro každé $n \in N$ platí $169|3^{3n+3} - 26n - 27$. Upravme nejdříve první člen daného výrazu. $3^{3n+3} = 27^n + 1 = (26+1)^{n+1}$. Použitím binomické věty pak obdržíme

$$(26+1)^{n+1} = \binom{n+1}{0} 26^{n+1} + \binom{n+1}{1} 26^n + \ldots + \binom{n+1}{n-1} 26^2 + 26(n+1) + 1$$

Je zřejmé, že všechny členy tohoto rozvoje s výjimkou posledních jsou dělitelné 169, neboť obsahují minimálně druhou mocninu čísla $26 = 2.13$. Poslední dva členy pak dávají $26n + 27$ a tudíž se vyruší s posledními dvěma členy daného výrazu.

1.0.2 Největší společný dělitel, nejmenší společný násobek

V této části budeme řešit dva problémy. Budeme hledat největší číslo, které současně několik různých čísel a naopak nejmenší číslo, které je současně dělitelné několika různými čísly. Definice: Každé celé číslo, dělící současně celá čísla $a, b, \ldots, l$ se nazývá jejich společným dělitelem. Je-li aspoň jedno z uvedených čísle různé od nuly, pak je počet jejich společných dělitelů konečný a tedy jeden z nich je největší. Ten se nazývá největším společným dělitelem čísel $a, b, \ldots, l$ a budeme ho značit $(a, b, \ldots, l)$. Je-li $(a, b, \ldots, l) = 1$, pak čísla $a, b, \ldots, l$ se nazývají nesoudělná. Je-li každé z čísel $a, b, \ldots, l$ nesoudělné s každým druhých z nich, pak čísla $a, b, \ldots, l$ se nazývají po dvou nesoudělná. Zřejmě čísla po dvou nesoudělná jsou vždy nesoudělná; v případě dvou čísel se pojmy nesoudělná a po dvou nesoudělná shodují.

Příklady: a) $(15, 18, 63) = 3$ b) $(15, 21, 31) = 1$ c)$(11, 18, 25) = 1$
V případech b a c jsou uvedená čísla nesoudělná, avšak pouze v případě c jsou i po dvou nesoudělná.

V dalších úvahách se budeme zabývat jen největším společným dělitelem dvou čísel, pro jednoduchost a z úsporných důvodů budeme používat zkratky NSD. Pokud tato čísla nejsou příliš velká, pak obyčejně nalezení NSD nebývá příliš složité, neboť se nám podaří rozložit obě čísla na součin prvočinitelů a pak vybereme vybereme ty, které jsou pro obě čísla společné. NSD je pak jejich součin.

Příklad: Určete NSD čísel 153 a 258. Platí $153 = 3^2.17$ a $258 = 2.3.43$. Je tedy $(153, 258) = 3$.

Ne vždy se nám podaří najít NSD tak jednoduše, zejména pro velká čísla je mnohdy obtížné najít byť jednoho dělitele, natož provést jeho rozklad na prvočinitele, příkladem budiž čísla Fermatova. Ptejme se tedy, zda pro nalezení NSD neexistuje nějaký jiný postup; ideální by bylo, pokud by se jednalo o algoritmus. Odpověď zní, že takový algoritmus existuje a je pojmenován po řeckém matematikovi Eukleidovi.

Mějme tedy čísla a a b, bez újmy na obecnosti můžeme předpokládat, že $a > b$. Podle () lze sestavit následující systém rovnic

$$a = bq_1 + r_1 b = r_1 + r_2 ..... r_{n-2} = r_{n-1}q_n + r_n r_{n-1} = r_n q_{n+1} + 0.$$

Z poslední rovnice plyne, že $r_n | r_{n-1}$, z předposlední pak $r_n | r_{n-2}$ atd. až z prvních dvou rovnic obdržíme $r|b$ a $r|a$. NSD je tedy největší nenulový zbytek v Eukleidově algoritmu.

Příklad: Určete největší společný dělitel čísel 1512 a 110. $1512 = 13 \times 110 + 82$; 110=1x82+28; 82=2x28+26; 28=1x26+2; 23=2x13. $(1512, 110) = 2$.

Příklad: Určete největší společný dělitel čísel 988 a 35. 988=28x35+8; 35=4x8+3; 8=2x3+2; 3=1x2+1; 2=1x1+1; 1=1x1+0. $(988, 35) = 1$, tato čísla jsou nesoudělná.

Příklad: Dokažte, že dvě po sobě jdoucí čísla jsou nesoudělná. řešení: $(a, a + 1)=(a, a + 1 - a)=(a, 1)=1$.

1.1 Prvočísla a čísla složená

V této části se seznámíme s pojmem prvočíslo a číslo složené. Dále uvedeme základní větu aritmetiky a některé aplikace.

Vezmeme-li v úvahu přirozená čísla větší než jedna, pak lze s jistotou tvrdit, že každé má alespoň dva dělitele, totiž jedničku a sebe sama. Nenajdeme-li již žádného dalšího dělitele, pak se toto číslo nazývá *prvočíslo*. V opačném případě mluvíme o *číslech složených*. Jedničku nezařazujeme ani do jedné skupiny, přesně v souladu s pythagorejskou školou. Ačkoliv se zdá, že se jedná jen o matematickou hříčku, byť velmi krásnou, není tomu tak. Umění rozeznat prvočíslo a číslo složené má v praxi velký význam, jak o tom bude pojednáno v dalším textu. Použití slova umění není od věci, zejména má-li číslo velký počet cifer je jeho faktorizace mnohdy velmi obtížná.

Pro malá čísla můžeme využít *Eratosthenova síta*. Dejme tomu, že máme nalézt všechna prvočísla menší než 100. Všechna čísla seřadíme podle velikosti a nejprve ponecháme dvojku a vyškrtáme všechny její násobky. Po této operaci je prvním nevyškrtnutým číslem trojka, vyškrtáme tedy všechny její násobky (pokud nejsou již vyškrtnuty při předchozí operaci. Tak postupujeme tak dlouho, až narazíme na nevyškrtnuté číslo větší než deset, to již škrtání končí a všechna nevyškrtnutá čísla jsou prvočísla.

Věta 1.7 *(První věta Eukleidova). Nechť $a, b \in N$, p je prvočíslo a $p|ab$. Pak $p|a$ nebo $p|b$.*

Důkaz: Jestliže $p|a$ jsme s důkazem hotovi. Pokud p nedělí a, je $(a, p) = 1$. Pak existují celá čísla x a y tak, že platí $ax + py = 1$. Vynásobíme-li obě strany této rovnice číslem b, obdržíme $abx + pby = b$. Jelikož oba sčítance na levé straně jsou dělitelné p, musí být dělitelné číslem p i číslo b.

Důsledkem je skutečnost, že každé každé přirozené číslo $n > 1$ lze jednoznačně rozložit na součin přirozených mocnin prvočísel $p_1 < p_2 < \ldots < p_r$. Platí tedy

$$n = P_1^{k_1} P_2^{k_2} \cdots P_r^{k_r} = \prod_{i=1}^{r}$$

Prvočíslo p_i se nazývá *prvočinitel*.

Věta 1.8 *Jestliže*

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s},$$

kde $p_1 < p_2 < \cdots < p_r, q_1 < q_2 < \cdots < q_s$ jsou prvočísla a $r, s, \alpha_i, \beta_i \in N$, pak $r = s$, $p_i = q_i$, $\alpha_i = \beta_i$ pro každé $i = 1, \ldots, r$.

Důkaz. Nechť $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$ a nechť $m = n$. Jestliže nějaké prvočíslo p dělí m, pak podle První Eukleidovy věty prvočíslo p musí dělit p_k pro nějaké $k \in \{1, \ldots, r\}$. Z definice prvočísla však plyne, že $p = p_k$. Protože $m = n$, musí p dělit také nějaké q_l pro $l \in \{1, \ldots, s\}$ a stejným způsobem dostaneme , že $p = q_l$. Odtud plyne, že $p_k = q_l$. Jelikož prvočísla p_i a q_j jsou seřazena podle velikosti, musí platit $p_1 = q_1, \ldots, p_r = q_r$ a $r = s$.

Předpokládejme dále, že $\alpha_1 > \beta_1$ pro nějaké $i \in \{1, \ldots, r\}$. Vydělíme-li rovnost $m = n$ číslem p^{β_i}, obdržíme

$$p_1^{\alpha_1} \cdots p_i^{\alpha_i - \beta_i} \cdots p_r^{\alpha_r} = p_1^{\beta_1} \cdots p_i^0 \cdots p_r^{\beta_r},$$

což je spor, neboť levá strana rovnice je dělitelná p_i, zatímco pravá strana tímto číslem dělitelná není. Analogicky postupujeme v případě, že $\alpha_i < \beta_i$. Je tedy $\alpha_i = \beta_i$ pro všechna $i \in \{1, \ldots, r\}$.

Věta o jednoznačnosti rozkladu přirozeného čísla na prvočinitele se nám zdá samozřejmá, existují však algebraické struktury, v nichž neplatí. Například v tělese $Q(\mathrm{i}\sqrt{5})$ tato věta neplatí, neboť $21 = 3 \cdot 7$ a $(1 + 2\mathrm{i}\sqrt{5})(1 - 2\mathrm{i}\sqrt{5})$. Základní věta aritmetiky je také jedním z důvodů, proč nepovažujeme jedničku za prvočíslo. Pokud by tomu tak bylo, tak by v rozkladu nebyla jednoznačnost exponentů.

Položíme-li si otázku, kolik je prvočísel, odpověď nalezneme v Eukleidových základech, kniha 9, tvrzení?. Druhá Eukleidova věta. Prvočísel je nekonečně mnoho. Důkaz provedeme sporem. Budeme předpokládat, že prvočísel je konečně mnoho. V tom případě je můžeme vyjmenovat, budou to čísla $p_1, p_2, \ldots, p_n$. Vynásobme je mezi sebou a připočtěme jedničku. Takto vzniklé číslo $m = p_1 p_2 \cdots p_n + 1$ není ani jedno z uvedených prvočísel, ani není některým z těchto prvočísel dělitelné. Je zde spor a proto je prvočísel nekonečně mnoho.

Poznamenejme, že zkonstruované číslo m je někdy prvočíslo (2.3.5.7+1=211), jindy je to číslo složené (2.3.5.7.11.13+1=30031=59.509). Podíváme-li se do Základů,

zjistíme, že Eukleides tuto větu uvedl v poněkud jiném tvaru. Jelikož řečtí matematikové pojem nekonečna ve smyslu jak ho chápeme dnes nepoužívali, museli věty formulovat opisem. Tvrzení tedy zní: Prvočísel je víc, než dané množství prvočísel. Důkaz pak je stejný, jak je uvedeno výše, jen počet známých prvočísel je mnohem nižší, Eukleides si vystačil se třemi.

1.1.1 Pythagorejské trojice

Pythagorovu větu ovládá každý, kdo se jen trochu potkal s geometrií. Každý zedník si umí udělat vingl (pravý úhel) tak, že tři latě s délkami v poměru $3 : 4 : 5$ spojí v trojúhelník a ví, že hledaný pravý úhel je oproti nejdelší lati. Pythagorova věta se obvykle uvádí slovně, říkáme že obsah čtverce nad přeponou se rovná součtu obsahů čtverců nad oběma odvěsnami. Takto formulované tvrzení má ovšem tvar implikace a Pythagorova věta nás ke konstrukci pravého úhlu výše uvedeným způsobem neopravňuje. Dá se však dokázat, že i obrácená implikace je správná, platí tedy následující věta:

Věta 1.9 *Trojúhelník s délkami stran a, b, c je pravoúhlý s přeponou délky c právě tehdy, když platí $c^2 = a^2 + b^2$.*

Definice: Nechť pro uspořádanou trojici čísel $[a, b, c]$ platí $a^2 + b^2 = c^2$. Tuto trojici nazýváme *pythagorejská trojice* a trojúhelník s těmito délkami stran *pythagorejský trojúhelník*. Jestliže navíc tato čísla nemají společného dělitele $d > 1$, mluvíme o *primitivní pythagorejské trojici*. Odpověď na otázku jak sestavit libovolnou pythagorejskou trojici nalezneme již u Diofanta.

Věta 1.10 *Uspořádaná trojice přirozených čísel $[a, b, c]$ je primitivní pythagorejskou trojicí tehdy a jen tehdy, existují-li nesoudělná přirozená čísla $m > n$ opačné parity tak, že buď*

$$a = m^2 - n^2, \qquad b = 2mn, \qquad c = m^2 + n^2$$

nebo

$$a = 2mn, \qquad b = m^2 - n^2, \qquad c = m^2 + n^2.$$

Čísla m n jsou určena jednoznačně.

Důkaz není obtížný, avšak pro jeho délku odkazujeme čtenáře např. na publikaci [2]. Ani Diofantos nebyl první, kdo se zabýval těmito trojicemi, jejich tabulky byly používány již ve staré Babylónii. S pythagorejskými trojicemi se v teorii čísel setkáváme poměrně často. Závěrem uvedeme jednu jejich aplikaci, kterou poprvé uvedl (a zřejmě i dokázal P. Fermat).

Věta 1.11 *Žádné číslo tvaru $4k - 1$ pro $k \in N$ není součtem dvou čtverců celých čísel.*

Důkaz je snadný, pokud si uvědomíme, že sudé číslo je tvaru $2l$ a liché $2m + 1$. Jejich čtverce jsou pak $4l^2$, resp. $4m^2 + 4m + 1 = 4n + 1$. Součet dvou čtverců může být tvaru $4k$, $4k + 1$ či $4k + 2$, nikdy nemůže být tvaru $4k + 3 = 4(k + 1) - 1$. Z výše uvedeného vyplývá, že číslo tvaru $4k - 1$ není ani čtvercem celého čísla.

1.2 Vlastnosti prvočísel

Pro přirozená čísla j, m a n řekneme, že m^j *přesně dělí* n, a budeme psát $m^j \| n$, jestliže $m^j | n$, ale $m^{j+1} n$. Pro $j = 0$ bude symbol $m^0 \| n$ znamenat, že mn.

Dokážeme větu, která uvádí vztah mezi prvočísly a binomickými koeficienty (kombinačními čísly).

Věta 1.12 *Přirozené číslo n je prvočíslem právě tehdy, když $n \mid \binom{n}{k}$ pro každé $k \in \{1, \ldots, n-1\}$.*

Důkaz: Nechť n je prvočíslo. Pro $k \in \{1, \ldots, n-1\}$ je $n-k$ mezi čísly 1 a $n-1$. Číslo n nedělí ani $k!$ ani $(n-k)!$, ale dělí $n!$. Jelikož $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, je toto číslo dělitelné n. Předpokládejme naopak, že n je složené a nechť p je nejmenší prvočíslo, které dělí n. Tedy je $1 < p < n$ a

$$\binom{n}{p} = \frac{n(n-1)\cdots(n-p+1)}{p(p-1)\cdots 2 \cdot 1}.$$

Dále předpokládejme, že $p^j \| n$ pro nějaké přirozené číslo j. Mezi p postupně jdoucími čísly $n, n-1, \ldots n-p+1$ je právě jedno dělitelné p. Protože $p \mid n$, platí $p(n-1)(n-2)\cdots(n-p+1)$. Platí tedy $p^j \| n(n-1)\cdots(n-p+1)$ a zřejmě i $p \| p(p-1)\cdots 2 \cdot 1$. Podle () dostaneme, že $p^{j-1} \| \binom{n}{p}$. Ale $n \binom{n}{p}$, protože $p^j \|$.

1.3 Úlohy k procvičení

1. Druhou mocninu každého přirozeného čísla je možné napsat buď ve tvaru $4k$ nebo $4k+1$. Dokažte.

2. Jestliže současně platí $a|b$ a $b|a$, pak je $|a| = |b|$. Dokažte.

3. Otec se synem jeli na dovolenou z Brna do Chorvatska autem. Jelikož cesta je dlouhá, rozhodli se, že se budou každých 80 km v řízení střídat. Kdo řídil auto při příjezdu do Splitu, je-li vzdálenost Brno - Split 888 km?

4. Nechť $a - b$ je násobkem čísla c. Pak i $a^n - b^n$ je násobkem c.

5. Dokažte, že pro libovolné přirozené číslo n platí $9|4^n + 15n - 1$.

6. Dokažte, že rozdíl čtverců dvou po sobě jdoucích přirozených čísel je dělitelný osmi.

7. Součet tří po sobě jdoucích třetích mocnin přirozených čísel je násobkem čísla 9. Dokažte.

8. Součet čtverců dvou po sobě jdoucích čísel zmenšený o jednu je dělitelný čtyřmi. Dokažte.
   item Rozdíl čtverců dvou lichých čísel je násobkem čísla 8. Dokažte.
   item Číslo $n^3 + 11n$ je dělitelné šesti pro libovolné n. Dokažte.

Kapitola 2

Některé funkce používané v teorii čísel

V této kapitole se zmíníme o některých funkcích, které se zhusta používají v teorii čísel. I my se v tomto textu budeme s těmito funkcemi setkávat, je proto nutné, abychom poznali jejich definici a základní vlastnosti.

2.1 Funkce $[x]$, $\{x\}$

První funkcí, s níž se seznámíme, je *celá část*, kterou označujeme $[x]$ a která je definována pro všechna reálná čísla x jako největší celé číslo, které není větší než x. Tak například [10]=10, [16,12]=16 a $[\pi]$=3. Uvedeme i příklady pro čísla záporná. [-4]=-4, [-5,2]=-6. Všimněme si, že pro čísla kladná je celá část v absolutní hodnotě vždy menší nebo rovna absolutní hodnotě daného čísla, kdežto u čísel záporných je tomu naopak. Je to obdobné jako v případě dělitelnosti čísel. Dělíme-li dvě kladná čísla, je součin dělitele a (neúplného) podílu vždy menší nebo roven dělenci. Dělíme-li naproti tomu záporné číslo kladným, je absolutní hodnota součinu dělitele a (neúplného) podílu vždy větší nebo rovna absolutní hodnotě dělitele.

Aby se desetinná část reálného čísla necítila odstrčená, definujeme i *lomenou částn čísla* x jako rozdíl $x - [x]$ a značíme ji $\{x\}$. Jako příklady uvedeme čísla $\{4\} = 0$, $\{1,6\} = 0,6$ a $\{-6,26\} = 0,74$.

Jako příklad využití této funkce uvedeme následující větu.

Věta 2.1 *Mocnitel, s kterým je dané prvočíslo p obsaženo v součinu $n!$ je roven*

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2 n}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

[1]

Důkaz: Počet součinitelů součinu $n!$ je $\left[\frac{n}{p}\right]$, mezi nimi je $\left[\frac{n}{p^2}\right]$ násobků čísla p^2, mezi těmito pak zase $\left[\frac{n}{p^3}\right]$ násobků čísla p^3 atd. Součet uvedených čísel tedy dá uvedeného mocnitele, nebo´t každý činitel součinu $n!$, který je násobkem čísla p^m, avšak ne čísla p^{m+1}, počítá se uvedeným způsobem $m-$krát jako násobek čísel $p, p^2, \ldots, p^m$.

[1] V publikaci [8]jsou exponenty mylně uvedeny jako koeficienty.

Příklady: V čísle 5! je prvočíslo 2 s exponentem 3, neboť $\left[\frac{5}{2}\right] + \left[\frac{5}{4}\right] = 2+1 = 3$. Snadno se vidí, že $5! = 600 = 2^3.3.5^2$. V čísle 57! je pětka $\left[\frac{57}{5}\right] + \left[\frac{57}{25}\right] = 11+2 = 13$. Jelikož třináctka je považována za číslo nešťastné, ověření přes kanonický rozklad dělat nebudeme, čtenáři v tom však nebráníme.

2.2 Součty vztahující se na dělitele čísla

velmi důležitou úlohu v teorii čísel hrají *multiplikativní funkce.* Tyto funkce můžeme definovat následujícím způsobem:

Def. 2.1 *Funkce $\vartheta(a)$ se nazývá multiplikativní, je-li definována pro všechna přirozená čísla, přičemž alespoň pro jednu hodnotu a je nenulová. Současně musí platit $\vartheta(a_1a_2) = \vartheta(a_1)\vartheta(a_2)$ je-li $(a_1, a_2) = 1$.*

Příkladem multiplikativní funkce je mocnina přirozeného čísla, neboť platí $a_1^s a_2^s = (a_1 a - 2)^s$. S dalšími multiplikativními funkcemi seznámíme čtenáře v další části kapitoly, než však k tomu dojde, uvedeme ještě některé další vlastnosti multiplikativní funkce.

Věta 2.2 *Nechť $\vartheta(a)$ je multiplikativní funkce. Pak platí $\vartheta(1) = 1$.*

Důkaz: Podle definice musí existovat alespoň jedno přirozené číslo, pro něž je funkce nenulová, nechť je to a_0. Pak máme $\vartheta(a_0) = \vartheta(1.a_0) = \vartheta(1)\vartheta(a_0)$.

Věta 2.3 *Nechť $\vartheta_1(a)$ a $\vartheta(a_2)$ jsou multiplikativní funkce. Pak i funkce $\vartheta_0(a) = \vartheta_1(a)\vartheta_2(a)$ je funkce multiplikativní.*

Důkaz: 1) $\vartheta_0(1) = \vartheta_1(1)\vartheta_2(1) = 1$
2) Předpokládejme, že je $(a_1, a_2) = 1$. pak je

$$\vartheta_0(a_1a_2) = \vartheta_1(a_1a_2)\vartheta_2(a_1a_2) = \vartheta_1(a_1)\vartheta_1(a_2)\vartheta_2(a_1)\vartheta_2(a_2) = \vartheta_1(a_1)\vartheta_2(a_1)\vartheta_2(a_1)\vartheta_2(a_2) = \vartheta_0($$

Věta 2.4 *nechť $\vartheta(a)$ je multiplikativní funkce a $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ je kanonický rozklad čísla a. Pak platí*

$$\sum_{d|a} \vartheta(d) = (1 + \vartheta(p_1) + \vartheta(p_1^2) + \dots + \vartheta(p_1^{\alpha_k}) \dots$$

$$\dots (1 + \vartheta(p_k) + \vartheta(p_k^2) + \dots + \vartheta(p_k^{\alpha_k})).$$

Je-li $a = 1$, pak i pravá strana je rovna jedné.

Důkaz: Roznásobíme-li výraz na pravé straně, dostaneme součet sčítanců tvaru

$$\vartheta(p_1^{\beta_1}(p_2^{\beta_2} \dots (p_k^{\beta_k} = \vartheta((p_1^{\beta_1}(p_2^{\beta_2} \dots (p_k^{\beta_k});$$

$$0 \le \beta_1 \le \alpha_1, \qquad 0 \le \beta_2 \le \alpha_2, \dots, \qquad 0 \le \beta_k \le \alpha_k,$$

přičemž ani jeden takový sčítanec nebude vynechán a ani se nebude opakovat, takže součty na levé i na pravé straně budou stejné.

je-li $\vartheta(a) = a^s$, má předchozí rovnost tvar

$$\sum_{d|a} d^s = (1 + p_1^s + p_1^{2s} + \ldots + p_1^{\alpha_1 s}) \ldots (1 + p_k^s + p_k^{2s} + \ldots + p_k^{\alpha_k s}) \tag{2.1}$$

Položíme-li $s = 1$, je levá strana rovnice () rovna součtu všech dělitelů čísla a, který označíme $S(a)$. Pravou stranu lze zjednodušit, takže obdržíme vztah pro součet všech dělitelů čísla a:

$$\sigma(a) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}. \tag{2.2}$$

Položíme-li $s = 0$, je levá strana rovnice () rovna počtu dělitelů čísla a, který označíme $\tau(a)$. Počet všech dělitelů tedy určíme podle vzorce

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1) \tag{2.3}$$

Příklad: Nechť $a = 36$. Pak jeho kanonický rozklad je $36 = 2^2 3^2$ a jeho dělitelé jsou čísla $1, 2, 3, 4, 6, 9, 12, 18, 36$. Sečteme-li tato čísla, obdržíme 91. Nu a toto číslo dostaneme i použijeme-li pravou stranu předchozího vzorce—$\frac{2^3-1}{2-1}\frac{3^3-1}{3-1}$. Sečteme-li všechny dělitele jako kusy, dostaneme se k číslu 9. Ale také je $(2 + 1)(2 + 1) = 9$.

S funkcemi $S(a)$ a $\tau(a)$ se budeme setkávat v dalším textu.

2.2.1 Eulerova funkce

Tato funkce se bude v tomto textu vyskytovat velmi často, je tedy nejvyšší čas, abychom ji definovali a uvedli některé její vlastnosti.

Def. 2.2 *Eulerova funkce $\varphi(a)$ je definována pro všechna přirozená čísla a jako počet těch čísel posloupnosti $0, 1, \ldots, a - 1$ kkterá jsou nesoudělná s a.*

Příklady: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(9) = 7$, $\varphi(13) = 12$.

Věta 2.5 *Nechť $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ je kanonický rozklad čísla a. Pak platí*

$$\varphi(a) = a \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right). \tag{2.4}$$

Důsledek 1: Je-li p prvočíslo, pak je $\varphi(p) = p - 1$ a $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Příklady: $\varphi(14) = 14(1 - \frac{1}{2})(1 - \frac{1}{7}) = 6$
$\varphi(512) = 8^3 - 8^2 = 448$
$\varphi(11) = 11 - 1 = 10$ Důsledek 2: Eulerova funkce je multiplikativní.

2.3 Příklady k procvičení

1. Vypočtěte mocnitele, s nímž je číslo 3 obsaženo v kanonickém rozkladu 1024!
2. Nalezněte kanonický rozklad čísla 18!
3. Vypočtěte $\sigma(51450)$ a $\tau(51450)$

4. Vypočtěte $\varphi(41)$ a $\varphi(1786050)$

5. Kanonický rozklad čísla je tvaru $2^a.7^b$, součet dělitelů pak 6000. Určete ono číslo.

Výsledky 508 $2^{16}.3^8.5.7.11.13.17$ 48, 148800 40, 408240 6000 $= (\frac{}{2}^{a+1}2-1)(\frac{7^{b+1}}{7-1})$. Po úpravě máme $2^5.3^2.5^2 = (2^{a+1})(7^{b+1})$. První závorka musí být liché číslo a navíc o jednu menší než libovolná mocnina 2. Tomuto vyhovuje číslo 15 a $a = 4$. Zbývají 4000, což je zase číslo o jedničku menší než čtvrtá mocnina sedmi, tedy $b = 3$.

Kapitola 3

Diofantické rovnice

V nejstarší česky psané matematické učebnici, jejímž autorem je Ondřej Klatovský a která vyšla v roce 1530 nalezneme tuto úlohu: *Dvacet šest osob na jednom kvasu propilo 88 penízků bílých. Při tom kvase byli muži, ženy a panny. Z mužů jedna osoba dáti měla šest penízků, z žen čtyři penízky a z pannen dva. Kolik jest při tom cechu aneb kvasu mužů bylo, kolik žen a kolik pannen.* Potlačme rozhořčení, že se tohoto kvasu zúčastnily i nevinné panny a pusťme se chutě do řešení. Tak jak je dnes zvykem, označme počet mužů x, počet žen y a konečně počet pannen z. Tímto získáme první rovnici $x+y+z = 26y$. Spočítáme-li této povedené společnosti útratu, dojdeme k druhé rovnici $6x+4y+2z = 88$. Vyjádříme-li z první rovnice z a dosadíme-li do rovnice druhé, obdržíme po úpravě rovnici $2x + y = 18$. Vidíme, že ač máme jednu rovnici, neznámé jsou dvě. Takovým rovnicím, v nichž se vyskytuje více neznámých, budeme říkat *rovnice neurčité*. Daleko častěji se však užívá název *rovnice diofantické*, a to napočest řeckého matematika Diofanta z Alexandrie.

3.1 Lineární diofantické rovnice

Abchom dovedli problém staročeské hostiny ke zdárnému konci, budeme se v této části zabývat rovnicemi tvaru

$$ax + by = c, \tag{3.1}$$

kde a, b, c jsou celá čísla, $a, b \neq 0$. Označme dále $(a, b) = d$ největší společný dělitel čísel a a b.

Nejdříve se budeme zabývat nejjednodušším případem, kdy $c = 0$. Položme $A = \frac{a}{d}$, $B = \frac{b}{d}$. Rovnici () převedeme na tvar

$$\frac{x}{y} = -\frac{b}{a} = -\frac{B}{A},$$

přičemž poslední zlomek je v základním tvaru.

Věta 3.1 *Všechna celočíselná řešení rovnice $ax + by = 0$ jsou dvojice čísel tvaru $x = Bt$, $y = -At$, kde t je libovolné celé číslo.*

Důkaz tvrzení přenecháváme čtenářům jako cvičení.

Příklad: Řešte rovnici $10x - 6y = 0$.
Jelikož $(10, 6) = 2$, jsou řešením všechny dvojice čísel $x = -\frac{6}{2}t = -3t$, $y = -\frac{10}{2}t = -5t$, kde t je libovolné celé číslo.

Nyní obrátíme svou pozornost k případu $c \neq 0$. Nejprve se podíváme, kdy má rovnice řešení.

Věta 3.2 *Rovnice $ax + by = c$ má řešení právě tehdy, když $(a, b)|c$.*

Důkaz: Předpokládejme nejdříve, že daná rovnice má řešení, které označíme x_0 a y_0, platí tedy $ax_0 + by_0 = c$. Z vlastností čísla d plyne, že dělí levou stranu rovnice, musí tedy dělit i pravou.

Předpokládejme nyní, že $d|c$. V tom případě musí existovat celá čísla x_0 a y_0 taková, že platí $ax_0 + by_0 = d$. Dále platí $c = de$, kde e je nějaké číslo. Položme $x_1 = ex_0$ a $y_1 = ey_0$. Zřejmě platí

$$ax_1 + by_1 = e(ax_0 + by_0) = ed = c.$$

Čísla x_1 a y_1 jsou řešením rovnice (), čímž je důkaz ukončen.

Hledejme nyní způsob, jak rovnici () vyřešit. Jednou z možností je využití Eukleidova algoritmu a postup ukážeme na konkrétním příkladě. nejprve si ukážeme, jak vypadá řešení, je-li $c = (a, b)$.
Příklad. Řešte rovnici $21x + 15y = 3$.
Jelikož $(21, 15) = 3$, má tato rovnice řešení. Největší společný dělitel čísel 21 a 15 nalezneme Eukleidovým algoritmem.

$$21 = 15.1 + 6$$

$$15 = 6.2 + 3$$

$$6 = 3.2 + 0$$

Z předposlední rovnice vyjádříme 3, tedy největšího společného dělitele čísel 21 a 15. Máme

$$3 = 15.1 + 6.(-2) \tag{3.2}$$

Nyní vyjádříme z první rovnice 6 a dosadíme do (), čímž obdržíme

$$3 = 15.1 + [21.1 + 15(-1)].(-2) = 21.(-2) + 15.3.$$

Jedním z řešení dané rovnice je tedy $x = -2$ a $y = 3$.

Množina řešení diofantické rovnice se nezmění, vydělíme-li všechny jejich koeficienty jejich společným dělitelem. Pokud na pravé straně je jiné číslo než d a je-li rovnice řešitelná, musí být $c = ed$. Najdeme tedy nejprve řešení rovnice kdy pravá strana je d a nalezené řešení pak vynásobíme číslem e.

Příklad: Řešte rovnici $21x + 15y = -6$.
V předchozím příkladu jsme nalezli řešení rovnice, kdy pravá strana je rovna 3. Máme $-6 = 3(-2)$, je $e = -2$ a řešení naší rovnice je $x = (-2)(-2) = 4$ a $y = 3(-2) = 6$.

Příklad: Uveďte alespoň jeden způsob, kterým lze vyplatit částku 37 Kč pouze dvoukorunovými a pětikorunovými mincemi.
Máme řešit diofantickou rovnici $2x + 5y = 37$. Protože čísla a a b jsou nesoudělná,

tak má rovnice vždy řešení. Dáme-li na pravou stranu jedničku, je $5 = 2.2+1$, tedy $1 = 5.1 + 2(-2)$ a $x = -2$, $y = 1$. Vynásobíme-li toto řešení číslem 37, získáme $x = -74$ a $y = 37$. Řešení jsme tedy našli, jenže je pro danou úlohu nepoužitelné. Je nad slunce jasné, že se nemůžeme spokojit s tím, že umíme nalézt jedno řešení diofantické rovnice a musíme se pokusit nalézt způsob, jak najít všechna její řešení.

Jedno řešení rovnice () nalézt umíme, řekněme, že je to uspořádaná dvojice $(x_0; y_0)$. Nechť i uspořádaná dvojice $(r; s)$ je řešením rovnice (). V tom případě platí

$$ar + bs = c = ax_0 + by_0,$$

což můžeme uvést na tvar

$$a(r - x_0) = -b(s - y_0)$$

a po vydělení číslem $d = (a, b)$ máme

$$\frac{a}{d}(r - x_0) = -\frac{b}{d}(s - y_0). \tag{3.3}$$

Protože $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, je zlomek $\frac{a}{d}$ dělitelem čísla $s - y_0$ a tedy je $s - y_0 = u\frac{a}{d}$. Podobnou úvahou zjistíme, že platí $r - x_0 = t\frac{b}{d}$, přičemž u a t jsou celá čísla. Po dosazení do () máme

$$\frac{a}{d}\left(\frac{b}{d}t\right) = -\frac{b}{d}\left(\frac{a}{d}u\right),$$

tedy $t = -u$. Řešením rovnice () jsou tedy čísla

$$r = x_0 + \frac{b}{d}t, \qquad s = y_0 - \frac{a}{d}t, \qquad t \in Z. \tag{3.4}$$

Nechť naopak r a s jsou dvě libovolná čísla tvaru (). Dosadíme-li je do rovnice (), máme

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = (ax_0 + by_0) + \frac{ab}{d}t - \frac{ab}{d}t = ax_0 + by_0 = c.$$

Poněkud jsme přehodili obvyklý matematický postup, neboť výše uvedené úvahy jsou důkazem následující věty:

Věta 3.3 *Nechť $x_0; y_0$ je řešením rovnice (). Pak dvojice čísel (r, s) je jejím řešením tehdy a jen tehdy, má-li tvar ().*

Poznámka: Jsou-li oba koeficienty rovnice () záporné, je třeba ji vynásobit číslem (-1). Je-li záporný jen jeden, dejme tomu a, zavedeme substituci $x = -z$, čímž dostaneme rovnici s kladnými koeficienty. Po jejím vyřešení se pak vrátíme k původní neznámé.

Takto jsouce vyzbrojeni teorií můžeme se pustit do vyřešení obou předchozích úloh. Začněme úlohou peněžní. Podle věty () budou všechna řešení ve tvaru

$$x = -74 + 5t, \qquad y = 37 - 2t,$$

kde t je libovolné celé číslo. Jelikož řešením úlohy mohou být pouze čísla přirozená, snadno se přesvědčíme, že taková řešení dostaneme pouze pro $t = 15, 16, 17, 18$.

Úkolem bylo nalézt jakékoliv řešení, my jako správní číselní teoretici si vybereme jediné prvočíslo z nabízených možností. V tomto případě můžeme 37 Kč vyplatit pomocí jedenácti dvoukorun a tří pětikorun.

Nyní již máme peníze a tak se můžeme vydat na kvas. I zde připadají jako řešení úlohy pouze přirozená čísla. Jelikož snadno zjistíme, že jedno z řešení rovnice je $x = 0$, $y = 18$, můžeme obecné řešení psát ve tvaru $x = t$, $y = 18 - 2t$. Snadno zjistíme, že úloze vyhovují pouze čísla $t = 1, \ldots, 8$. Řešení uvedeme ve formě tabulky.

x	1	2	3	4	5	6	7	8
y	16	14	12	10	8	6	4	2
z	9	10	11	12	13	14	15	16

Je zajímavé, že Klatovský uvádí pouze dvě řešení, a to případy se šesti a osmi muži. Zarážející je ovšem skutečnost, kolik pannen se onoho kvasu zúčastnilo, vždyť ve více než polovině případů panny kvasu kralovaly a vůbec: Podle našeho mínění bylo mnohem výstižnější mluvit ne o kvasu, nýbrž o dámské jízdě.

3.2 Diofantické rovnice vyššího stupně

V předchozí části jsme se naučili řešit diofantické rovnice lineární. Můžeme s klidným svědomím prohlásit, že dovedeme vyřešit každou lineární diofantickou rovnici o dvou neznámých, pokud ovšem řešení má. Ale i o řešitelnosti těchto rovnic umíme rozhodnout jednoznačně. S řešením rovnic vyššího stupně je to ovšem mnohem obtížnější, mnohdy se spokojíme s tím, že umíme alespoň rozhodnout je-li rovnice vůbec řešitelná a jásáme, nalezneme-li alespoň nějaké řešení. Z tohoto důvodu uvedeme jen dva typy rovnic, ovšem kvantitu nahradíme kvalitou a uvedeme úplné řešení těchto typů.

Některé rovnice lze převést na tvar

$$(ax + by)(cx + dy) = k \tag{3.5}$$

Předtím než ukážeme způsob řešení této rovnice, zavedeme následující pojem:

Def. 3.1 *Celá čísla u a v se nazývají sdružení dělitelé čísla w platí-li $u.v = w$.*

Příkladem budiž čísla 2 a 5, která jsou sdruženými děliteli čísla 10, neboť 10=5.2. Nebo čísla -7 a 4 jsou sdruženými děliteli čísla -28, jelikož -28=(-7).4.

Jsou-li čísla x a y celočíselným řešením rovnice (), tak čísla $ax + by$ a $cx + dy$ jsou celá a navíc jsou to sdružení dělitelé čísla k. Proto řešení rovnice () najdeme následujícím způsobem. Určíme nějakého dělitele čísla k, dejme tomu že to bude k_1. Nalezneme sdruženého dělitele k_2 a položíme

$$ax + by = k_1 \qquad cx + dy = k_2$$

To je ovšem soustava dvou lineárních rovnic o dvou neznámých. Je-li tato soustava řešitelná, pak jsou čísla x a y určena jednoznačně a jsou to současně řešení rovnice ().

Z uvedené metody vyplývá, že rovnice typu () mohou mít nejvýš konečný počet řešení. Počet dvojic sdružených dělitelů čísla k je konečný a ke každé dvojici sdružených dělitelů přísluší buď jedno nebo žádné řešení.

Podívejme se na rovnici

$$x^2 - y^2 = k \tag{3.6}$$

Snadno se přesvědčíme, že tato rovnice není řešitelná v případě $k = 4t + 2$. Každá mocnina celého čísla je totiž buď tvaru $4s$ nebo $4s + 1$. Pokud jsou obě mocniny stejného tvaru, je jejich rozdíl tvaru $4t$. Je-li $x^2 = 4s + 1$ a $y = 4v$, je jejich rozdíl $4t + 1$. Je-li naopak $x^2 = 4s$ a $y = 4v + 1$, je jejich rozdíl $4t - 1 = 4w + 3$. Naopak není-li $k = 4t+2$ je rovnice vždy řešitelná. Pro sudé $k = 4t$ je $x = \frac{k}{4}+1$ a $y = \frac{k}{4}-1$. Pro liché $k = 2s + 1$ jsou řešením čísla $x = s + 1$ a $y = s$.

Podívejme se ještě na rovnici

$$a_n x^n + \ldots + a_1 x + a_0 = ky, \tag{3.7}$$

kde a_i a k jsou celá čísla. Skutečnost, že jedna neznámá se vyskytuje pouze v první mocnině bude pro další úvahy důležitá.

Ne každá taková rovnice má řešení jak si ukážeme v následujícím příkladu. Zkusme vyřešit rovnici

$$x^2 + 2 = 4y.$$

Již bylo zmíněno, že druhá mocnina celého čísla je buď tvaru $4t$ či $4t+1$. Přičteme-li k oběma tvarům dvojku, nikdy nedostaneme číslo dělitelné čtyřmi.

Nyní dokážeme jednu větu, kterou budeme potřebovat pro řešení rovnice ().

Věta 3.4 *Nechť $x = a + kt$, kde a,k, t jsou celá čísla. Je-li $m \in N$, je x^m tvaru $kT + a^m$, kde T je celé číslo.*

Důkaz provedeme matematickou indukcí. Je-li $m = 1$, tak tvrzení evidentně platí. Budeme tedy předpokládat, že tvrzení platí pro $m = n$ a dokážeme, že za tohoto předpokladu platí i pro $m = n + 1$.

$$x^{n+1} = (a + kt)^{n+1} = (a + kt)^n (a + kt).$$

Podle indukčního předpokladu je $(a+kt)^n$ rovno $kL+a^n$, můžeme tedy pokračovat v úpravách.

$$(kL + a^n)(a + kt) = kLa + k^2Lt + kta^n + a^{n+1}.$$

Vytkneme-li z prvních tří členů k a označíme-li $T = La+kLt+ta^n$, je důkaz hotov.

Věta 3.5 *Nechť (x_0, y_0) je řešením rovnice () a t je celé číslo. Pak ke každému číslu tvaru $x = x_0 + kt$ existuje takové y, že (x, y) je řešením rovnice ().*

Při důkazu využijeme předchozí věty. Je-li (x_0, y_0) řešením rovnice (), má mocnina tvar $x^j = (x_0 + kt)^j$ tvar $kT_j + x_0^j$. Máme tedy

$$a_n(x_0 + kt)^n + \ldots + a_1(x_0 + kt) + a_0 = a_n(kT_n + x_0^n) + \ldots + a_1(x_0 + kt) + a_0 =$$

$$k(a_nT_n + \ldots + a_1t) + (a_nx_0^n + \ldots + a_1x_0 + a_0) = kT + ky_0 = k(T + y_0).$$

Dvojice $x_0 + kt$, $T + y_0$ je řešením rovnice (), čímž je důkaz hotov.

Tato věta nám říká, že známe-li jedno řešení, umíme najít nekonečně mnoho řešení, které tvoří třídu. To je sice hezké, ale umíme nějakým způsobem najít alespoň jedno řešení rovnice ()? Věta () má jeden pro nás důležitý důsledek. Je-li

rovnice () řešitelná, pak existuje takové řešení, že | X |<| k |. Skutečně, k daným nezáporným celým číslům x_0 a k existují nezáporná čísla s a r taková, že platí

$$x_0 = |k|s + r, \qquad 0 \leq r < |k|,$$

tedy

$$0 \leq x_0 - |k|s = r < |k|.$$

Je-li $k > 0$, položíme $t = -s$, pro $k < 0$ dáme $t = s$ a obdržíme číslo $X = x_0 + kt < |k|$. Nu a podle věty () existuje k tomuto číslu i Y takové, že dvojice (X, Y) je řešením rovnice ().

Díky tomuto důsledku můžeme odehnat chmury z čela. Stačí zjistit, zda některé z čísel $0, 1, \ldots, |k| - 1$ není řešením rovnice (). Pokud se nám to podaří, má rovnice () nekonečně mnoho řešení, pokud ne, řešení tato rovnice nemá.

Příklad: Řešte rovnici $x^2 + 3x + 1 = 4y$.

Do levé strany dosadíme postupně čísla $0, 1, 2, 3$. Výsledkem jsou čísla $1, 5, 11, 19$ z nichž ani jedno není dělitelné čtyřmi, tato rovnice řešení nemá.

Příklad: Řešte rovnici $x^2 + 2x + 4 = 4y$.

Zde budeme mít již více štěstí. Dosadíme-li do levé strany postupně čísla $0, 1, 2, 3$, obdržíme $4, 7, 12, 19$; první a třetí čísla v této řadě jsou násobky čtyř, máme tedy dvě třídy řešení $4t$, $4t + 2$.

3.3 Úlohy k procvičení

1. Z uvedených rovnic vyberte ty, které jsou řešitelné:
   a) $7x + 3y = 2$ b)$18x + 40y = 3$ c) $64x - 72y = 44$ d) $15x + 35y = 100$

2. Řešte rovnici $15x - 20y = 100$ Z3/40

3. Pro která x je výraz $\frac{17x-2}{15}$ celé číslo? (Z4/40

4. Jistý stařešina vedl stočlenný rod. Po sklizni se jim rozhodl dát 100 měřic obilí, přičemž muži měli dostat 3 měřice, ženy dvě a každé dítě půl měřice. Ať řekne, kdo se domnívá, že ví, kolik bylo mužů, kolik žen a kolik dětí.

5. Nějaký muž chtěl za sto zlatých koupit sto zvířat. Nařídil svému sluhovi, ať je velbloud koupen za pět zlatých, osel za jeden zlatý a dvacet ovcí za jeden zlatý. Řekni kdo chceš, kolik bylo za sto zlatých koupeno velbloudů, kolik oslů a kolik ovcí.

6. Ani mezi kleriky nepanovala rovnost, jak se můžeme přesvědčit v této úloze: Nějaký biskup kázal rozdělit klerikům 12 chlebů. Nařídil, aby každý kněz dostal dva chleby, každý jáhen polovinu chleba a každý lektor čtvrtinu chleba, přičemž kleriků bylo stejně jako chlebů. Řekni, kdo jsi s to, kolik muselo být kněží, kolik jáhnů a kolik lektorů.

7. Najděte všechny dvojice navzájem různých sdružených dělitelů čísla 36. Z1/47

8. Řešte rovnici $6x^2 - 5xy + y^2 = 21$ Z2/47

9. Řešte rovnici $2x^2 + 3xy + y^2 = 35$ Z3/35

10. Najděte všechna celočíselná řešení rovnice $x^2 - 4 = 11y$. Z8/47

11. Pro jaká x je výraz $x^3 + 2x + 2$ násobkem čísla 125? Z10/47

12. Pro jaké n je $6n + 2$ třetí mocninou celého čísla? Z11/47

13. Cvičenci nastoupili do obdélníku, přičemž na jedné straně je o pět cvičenců víc než na druhé. Po skončení cvičení nastoupili do čtyřstupu a odpochodovali z plochy. V poslední řadě však jeden cvičenec chyběl. Kolik cvičenců vystoupilo? Z12/47

Kapitola 4

Kongruence

Nechť $a, b, m \in Z$, přičemž $m > 1$. Řekneme, že číslo a je kongruentní s číslem b podle modulu m, jestliže $m|)a - b)$, neboli čísla a a b dávají po dělení číslem m týž zbytek. Píšeme $a \equiv b$. Platí tedy, že $14 \equiv 39 \mod 5$, neboť $5|(39 - 14)$. Naproti tomu $5(27 - 14)$, píšeme tedy $27 \not\equiv 14 \mod 5$.

4.1 Vlastnosti kongruencí podobné vlastnostem rovnic

Z definice plyne, že kongruence jsou tranzitivní, tedy je-li $a \equiv b \mod m$ a $b \equiv c \mod m$, pak je $a \equiv c \mod m$.

Kongruence podle téhož modulu je možné člen po členu sčítat. Důkaz: Nechť $a_1 \equiv b_1 \mod m$ a $a_2 \equiv b_2 \mod m$. V tomto případě je $a_1 = b_1 + mt_1$ a $a_2 = b_2 + mt_2$ a $a_1 + a_2 = b_1 + b_2 + m(t_1 + t_2)$, tedy $a_1 + a_2 \equiv b_1 + b_2$. Důsledkem je, že podobně jako u rovnic lze v kongruenci převádět z jedné strany na druhou. Jinými slovy ke každé straně kongruence lze přičíst totéž číslo.

Kongruence podle téhož modulu lze navzájem násobit. Důkaz: Vyjádříme opět a_1 a a_2 stejným způsobem jako v předchozím případě, pak platí $a_1 a_2 = b_1 b_2 + mN$, kde N je celé číslo. Je tedy $a_1 a_2 \equiv b_1 b_2 \mod m$. Důsledkem je, že obě strany kongruence můžeme umocnit týmž exponentem. Dalším důsledkem je, že obě strany kongruence můžeme vynásobit týmž číslem, násobíme totiž evidentně správnou kongruencí $k \equiv k \mod m$. Narozdíl od rovnic může být $k = 0$, i když o smysluplnosti této operace lze s úspěchem pochybovat.

Obě strany kongruence je možno vydělit jejich společným dělitelem, je-li nesoudělný s modulem. Důkaz: Z podmínek$a \equiv b \pmod m$, $a = a_1 d$,$b = b_1 d$, $(d, m) = 1$ plyne,že rozdíl $a = b$, rovný $(a_1 - b_1)d$, je dělitelný číslem m. Proto je $a_1 - b_1$ je dělitelné číslem m, tedy $a_1 \equiv b_1 \pmod p$.

4.2 Další vlastnosti kongruencí

Obě strany kongruence i modul je možno vynásobit týmž celým číslem. Důkaz: Z $a \equiv b \pmod p$ plyne $a = b + mt$, $ak = bk + mkt$ a tedy je $ak \equiv bk \pmod{bk}$

Obě strany kongruence i modul je možno vydělit jejich libovolným společným dělitelem. Důkaz: Nechť $a \equiv b \pmod{p}$, $a = a_1 d$, $b = b_1 d$, $m = m_1 d$. Máme $a = b + mt$, $a_1 d = b_1 d + m_1 dt$, $a_1 = b_1 + m_1 t$, z čehož plyne $a_1 \equiv b_1 \pmod{m}_1$.

Platí-li kongruence $a \equiv b$ podle několika modulů, pak platí i podle modulu, který je roven nejmenšímu společnému násobku těchto modulů. Důkaz je zřejmý, rozdíl $a-b$ je dělitelný všemi moduly, je tedy dělitelný i jejich nejmenším společným násobkem.

Platí-li kongruence podle modulu m podle modulu m, pak platí i podle modulu d, kde d je libovolný dělitel čísla d. Důkaz je zřejmý neboť je-li rozdíl $a-b$ dělitelný číslem m, je dělitelný i jeho libovolným dělitelem.

Jsou-li jedna strana kongruence a modul dělitelné kterýmkoliv číslem, pak je i druhá strana kongruence dělitelná tímto číslem. Důkaz: Platí $a = b + mt$. Je-li m a a dělitelné d, musí být tímto číslem dělitelné i b.

Je-li $a \equiv b \pmod{m}$, pak $(a, m) = (b, m)$. Důkaz plyne z ????

4.3 Úplná soustava zbytků

Čísla kongruentní podle modulu m vytvářejí *třídu čísel podle modulu m*. Z této definice plyne, že všem číslům třídy odpovídá jeden a týž zbytek r a že všechna čísla třídy dostaneme, když ve výrazu $mq+r$ bude q probíhat všechna celá čísla. V souhlasu s tím, že r může nabývat m různých hodnot, máme m tříd podle modulu m.

Libovolné číslo třídy se nazývá *zbytkem podle modulu m*. Zbytek získaný pro $q = 0$, který je roven samotnému zbytku r se nazývá *nejmenší nezáporný zbytek*. Zbytek ϱ s nejmenší absolutní hodnotou se nazývá *absolutně nejmenší zbytek*. Pro $r < \frac{m}{2}$ je zřejmě $\varrho = r$; pro $r > \frac{m}{2}$ je $\varrho = r - m$; konečně je-li m sudé a $r = \frac{m}{2}$ je za ϱ možné vzít kterékoliv ze dvou čísel $\frac{m}{2}$ a $-\frac{m}{2}$.

Vezmeme-li z každé třídy po jednom zbytku, dostaneme *úplnou soustavu zbytků podle modulu m*. Nejčastěji se používají jako úplná soustavu zbytků nejmenší nezáporné zbytky, případně absolutně nejmenší zbytky. Příklad: Úplnou soustavu zbytků podle modulu 5 můžeme vyjádřit buď jako $0, 1, 2, 3, 4$ nebo $-2, -1, 0, 1, 2$.

Věta 4.1 *Libovolných m čísel po dvou nekongruentních podle modulu m vytváří úplnou soustavu zbytků podle modulu m.*

Věta 4.2 *Nechť $(a, m) = 1$ a x probíhá úplnou soustavu zbytků podle modulu m, pak $ax + b$, kde b je libovolné celé číslo, probíhá také úplnou soustavu zbytků podle modulu m.*

Důkazy obou tvrzení jsou snadné a ponecháváme je na čtenáři jako cvičení.

4.4 Redukovaná soustava zbytků

Čísla jedné a téže zbytkové třídy podle modulu m mají s modulem jednoho a téhož největšího společného dělitele. Třídy obsahující zbytky nesoudělné s modulem tvoří *redukovanou soustavu zbytků*. Redukovanou soustavu zbytků tedy můžeme sestavit

z čísel úplné soustavy, které jsou nesoudělné s modulem. Redukovanou soustavu obvykle vytváříme ze soustavy nejmenších nezáporných zbytků. Poněvadž mezi čísly úplné soustavy je jich právě $\varphi(m)$ nesoudělných s modulem m, je počet čísel redukované soustavy stejně jako počet tříd obsahující čísla nesodělná s modulem $\varphi(m)$. Příklad: Redukovaná soustava zbytků podle modulu 16 je 1, 3, 5, 7, 9, 11, 13, 15. Je-li modul prvočíselný, pak je redukovaná soustava zbytků totožná s úplnou soustavou zbytků.

Věta 4.3 *Libovolných $\varphi(m)$ čísel, po dvou nekongruentních podle modulu m a nesoudělných s modulem, tvoří redukovanou soustavu zbytků podle modulu m.*

Věta 4.4 *Je-li $(a, m) = 1$ a x probíhá redukovanou soustavu zbytků podle modulu m, pak ax rovněž probíhá redukovanou soustavu zbytků podle modulu m.*

Důkazy obou vět jsou analogické důkazům vět ??? a rovněž je přenecháváme čtenáři jako cvičení.

4.5 Kongruence o jedné neznámé

V této kapitole budeme studovat kongruence obecného tvaru

$$f)x) \equiv 0 \pmod{m}; \quad f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0.(?)$$

Není-li a_n dělitelné číslem m, pak se n nazývá *stupeň kongruence*. Řešit kongruenci znamená najít všechny hodnoty x, které jí vyhovují. Dvě kongruence, kterým vyhovují stejné hodnoty x, se nazývají *ekvivalentní*.

Vyhovuje-li kongruenci (?) jistá hodnota x_0, pak jí vyhovují i všechna čísla x splňující kongruenci $x \equiv x_0 \pmod{m}$. Celá tato třída se považuje za jedno řešení. Za této úmluvy bude mít kongruence (?) tolik řešení, kolik zbytků úplné soustavy jí vyhovuje. Příklad: Kongruenci $x^3 + 3x^2 + 3 \equiv 0 \pmod{5}$ vyhovuje $x = 4$. Kongruence má jediné řešení $x \equiv 4 \pmod{5}$.

4.5.1 Lineární kongruence

Budeme nyní studovat lineární kongruenci, tedy kongruenci tvaru

$$ax \equiv b \mod m. \tag{4.1}$$

Předpokládejme, že je $(a, m) = 1$. Tato kongruence má právě tolik řešení, kolik zbytků úplné soustavy jí vyhovuje. Probíhá-li x úplnou soustavu sbytků podle modulu m, pak i ax probíhá úplnou soustavu zbytků podle modulu m. Z tohoto důvodu bude ax kongruentní s b právě pro jednu hodnotou x z úplné soustavy zbytků, jinými slovy kongruence () má právě jedno řešení.

Nechť nyní je $(a, m) = d > 1$. Aby kongruence () měla řešení, je nutné, aby b bylo dělitelné číslem d, jinak kongruence () není možná při žádném celém čísle x. Budeme proto předpokládat, že b je násobkem d a položíme $a = a_1 d$, $m = m_1 d$ a $b = b_1 d$. V tomto případě můžeme kongruenci zkrátit číslem d a nově vzniklá kongruence $a_1 x \equiv b_1$ bude mít jedno řešení podle moduli m_1, neboť je $(a_1, m_1) = 1$.

Nechť x_1 je nejmenší nezáporný zbytek tohoto řešení podle modulu m_1, pak všechna čísla x, tvořící toto řešení, jsou tvaru

$$x \equiv x - 1 \pmod{m_1}. \tag{4.2}$$

Podle modulu m však čísla () netvoří jedno řešení, ale právě tolik řešení, kolik se najde v řadě $0, 1, 2, \ldots, m-1$ nejmenších nezáporných zbytků podle modulu m. Sem patří všechna tato čísla)):

$$x_1,\ x_1 + m\, x_1 + 2m\ \ldots, x_1 + (d-1)m,$$

tedy celkkem d čísel (2), a tudíž kongruence () má d řešení.

Výše uvedené úvahy dokazují tuto větu:

Věta 4.5 *Nechť $(a, m) = d$. Kongruence $ax \equiv b \pmod{m}$ nemá řešení, není-li pravá strana dělitelná d. V případě, že je b násobkem d, má kongruence d řešení.*

Nyní si ukážeme některé metody řešení kongruencí. Příklad 1: Řešte kongruenci $4x \equiv 1 \pmod{6}$.
Tato kongruence nemá řešení, neboť $(4, 6) = 2$ a 21.

Pokud není modul příliš velký, lze kongruenci řešit tak, že zjistíme, která čísla jí vyhovují, obvykle ze soustavy nejmenších nezáporných zbytků.
Příklad 2: řešte kongruenci $3x \equiv 2 \pmod{5}$.
Jelikož $(3, 5) = 1$, má kongruence právě jedno řešení. Soustava nejmenších nezáporných zbytků má tvar 0, 1, 2, 3, 4. Snadno se přesvědčíme, že této kongruenci vyhovuje právě číslo 4. Řešením kongruence jsou tedy všechna čísla $x \equiv 4 \pmod{5}$.

Příklad 3: Řešte kongruenci $6x \equiv 9 \pmod{1}5$.
Jelikož $(6, 15) = 3$ a $3 \mid 9$, bude mít kongruence 3 řešení. Vydělíme-li obě strany kongruence 3, obdržíme novou kongruenci $2x \equiv 3 \pmod{5}$. Vzhledem k tomu, že modul je poměrně malé číslo, lze řešení určit postupným dosazováním čísel ze soustavy nejmenších nezáporných zbytků. Snadno zjistíme, že jejím řešením je číslo $x_1 = 4$. Dalším řešením jsou čísla $x_2 = x_1 + 5$ a $x_3 = x_1 + 2.5$. Řešení původní kongruence lze uvést ve tvaru $xqequiv4; 9; 14 \pmod{2}0$.

Při řešení kongruencí, kde $(a, m) = 1$, lze využít Eulerovu větu. Skutečně, je-li $a^{\varphi(m)} \equiv 1 \pmod{m}$, je i $a^{\varphi(m)}b \equiv b \pmod{m}$. Odsud máme $ax \equiv a^{\varphi(m)}b$, a proto je $x \equiv a^{\varphi(m)-1}b$. Stačí tedy vypočítat číslo $a^{\varphi(m)-1}b$. Toto číslo sice nebude patřit mezi nejmenší nezáporné zbytky, není však problém nejmenší nezáporný zbytek najít.
Příklad 4: Řešte kongruenci $6x \equiv 2 \pmod{7}$.
Jelikož $\varphi 7 = 6$, je $x = 6^5 \cdot 2$ a kvůli eleganci a jednoduchosti ho zapíšeme ve tvaru $x \equiv 5 \pmod{7}$.

4.5.2 Soustava lineárních kongruencí

Jelikož některé vlastnosti kongruencí jsou stejné či analogické vlastnostem rovnic, je namístě si položit otázku, zda lze řešit i soustavu lineárních kongruencí. Omezíme se na soustavu kongruencí o jedné neznámé s různými, po dvou nesoudělnými moduly, tedy na soustavu tvaru

$$a \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \ldots, x \equiv b_k \pmod{m_k}. \tag{4.3}$$

Řešit soustavu () je možno podle následující věty.

Věta 4.6 *Nechť čísla M_s a $M_s^{'}$ jsou definována podmínkami*

$$m_1 m_2 \dots m_k = M_s m_s, \qquad M_s m_s^{'} \equiv 1 \pmod{m_s}$$

a nechť

$$x_0 = M_1 M_1^{'} b_1 + M_2 M_2^{'} + \dots + M_k M_k^{'} b_k.$$

Pak souhrn hodnot x vyhovujících soustavě () je určen kongruencí

$$x \equiv x_0 \pmod{m_1 m_2 \dots m_k}. \tag{4.4}$$

Vskutku, vzhledem k dělitelnosti všech čísel M_j, různých od M_s, číslem m_s při libovolném $s = 1, 2, \dots, k$ je

$$x_0 \equiv M_s M_s^{'} b_s \equiv b_s \pmod{m_s},$$

a tedy soustavě () vyhovuje $x = x_0$. Odtud přímo plyne, že soustava () je ekvivalentní se soustavou

$$x \equiv x_0 \pmod{m_1}, \qquad x \equiv x_0 \pmod{m_2}, \dots, x \equiv x_0 \pmod{m_k}, \tag{4.5}$$

tedy soustavám () a () vyhovují tytéž hodnoty x. Soustavě () pak vyhovují jen ty hodnoty x, které vyhovují kongruenci ().

Věta 4.7 *Nechť $b_1, b_2, \dots,$ probíhají nezávisle jedno na druhém úplné soustavy zbytků podle modulů $m_1, m_2, \dots, m_k$, pak x_0 probíhá úplnou soustavu zbytků podle modulů $m_1, m_2, \dots, m_k$.*

Důkaz: Vskutku, x_0 probíhá $m_1, m_2, \dots, m_k$ hodnot, vzhledem k () mekongruentních podle modulu $m_1, m_2, \dots, m_k$.

Příklad: Řešte soustavu kongruencí

$$x \equiv b_1 \pmod{4}, \qquad x \equiv b2 \pmod{5}, \qquad x \equiv b_3$$

Platí 4.5.7=4.35=5.28=7.20, přičemž

$$35.3 \equiv 1 \pmod{4}, \qquad 28.2 \equiv 1 \pmod{5}, \qquad 20.6 \equiv 1 \pmod{7}.$$

Proto je

$$x_0 = 35.3 b_1 + 28.2 b_2 + 20.6 b_3 = 105 b_1 + 56 b_2 + 120 b_3,$$

a tedy souhrn hodnot x vyhovujících soustavě může být vyjádřen ve tvaru

$$x \equiv 105 b_1 + 56 b_2 + 120 b_3 \pmod{140}.$$

tak např. souhrn hodnot x, vyhovujících soustavě

$$x \equiv 1 \pmod{4}, \qquad x \equiv 3 \pmod{5}, \qquad , x \equiv 2 \pmod{7},$$

je

$$x \equiv 105.1 + 56.3 + 120.2 \equiv 93 \pmod{140}.$$

a souhrn hodnot x, vyhovujících soustavě

$$x \equiv 3 \pmod{4}, \qquad x \equiv 2 \pmod{5}, \qquad x \equiv 6 \pmod{7},$$

je

$$x = 105.3 + 56.2 + 120.6 \equiv 27 \pmod{140}.$$

4.6 Kongruence libovolného stupně podle prvočíselnéh modulu

Budeme se zabývat kongruencí tvaru

$$a_n x^n + a_1 x^{n-1} + \ldots + a_0 \equiv \pmod{p} \tag{4.6}$$

kde p je prvočíslo. Kongruence tvaru () je ekvivalentní s kongruencí stupně nejvýš $p-1$. Toto tvrzení plyne ze skutečnosti, že $f(x)$ lze psát jako

$$f(x) = (x^p - x)Q(x) + R(x),$$

kde $R(x)$ je zbytek po dělení $f(x)$ polynomem $x^p - x$, jehož stupeň nemůže převýšit $p-1$. Podle Malé Fermatovy věty zase máme $x^p - x \equiv 0 \pmod{p}$, je tedy $f(x) \equiv R(x) \pmod{p}$. Nechť kongruence () má více než n řešení. Pak platí, e všechny koeficienty a_i jsou násobky p. Označme zbytky všech řešení kongruence () písmeny $x_1, x_2, \ldots x_n, x_{n+1}$. Polynom $f(x)$ můžeme vyjádřit jako

$$\begin{aligned} f(x) \quad &= a(x-x_1)(x-x_2)\ldots(x- \\ &\quad b(x-x_1)(x-x_2)\ldots(x-x_ \\ &\quad +\ldots+ \\ &\quad +l(x-x_1) \\ &\quad +m. \end{aligned}$$

Sčítance na pravé straně přeměníme v mnohočleny a zvolíme b tak, aby součet koeficientů dvou prvých mnohočlenů u x^{n-1} byl a_1; známe-li b, zvolíme c tak, aby součet korficientů prvých tří mnohočlenů u x^{x-2} byl a_2 atd. klademe-li postupně $x = x_1, x_2, \ldots, x_n, x_{n+1}$, přesvědčíme se, že všechna čísla $m, l, k, \ldots, c, b, a$ jsou násobky p. Protože a_i jsou součty čísel dělitelných p, jsou také dělitelná p.

4.7 Kongruence druhého stupně

V tomto oddíle budeme vyšetřovat kongruence tvaru

$$x^2 \equiv a \pmod{p}; \qquad (a,p) = 1, \tag{4.7}$$

kde p je liché prvočíslo. Pokud má tato kongruence řešení, nazýváme číslo a *kvadratickým zbytkem*, v opačném případě *kvadratickým nezbytkem* podle modulu p.

Věta 4.8 *Nechť a je kvadratický zbytek podle modulu p. pak kongruence () má právě dvě řešení.*

Důkaz: Jelikož a je kvadratický zbytek, musí mít kongruence () alespoň jedno řešení, řekněme že je to x_1. Protože je $(-x_1)^2 = x_1^2$, má tato kongruence i druhé řešení $x \equiv -x_1 \pmod{p}$. Dále nemůže platit $x_1 \equiv -x_1 \pmod{p}$, neboť pak by bylo$2x_1 \equiv 0 \pmod{p}$. Toto však není možné, protože $(2,p) = (x_1,p) = 1$. Další řešení již tato kongruence nemůže mít, jak bylo dokázáno v ??

Věta 4.9 *Redukovaná soustava zbytků podle modulu p se skládá z $\frac{p-1}{2}$ kvadratických zbytků, které jsou kongruentní s čísly $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ a $\frac{p-1}{2}$ kvadratických nezbytků.*

Důkaz: Mezi zbytky redukované soustavy podle modulu p jsou kvadratickými zbytky ty a jenom ty, které jsou kongruentní s čtverci čísel

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2} \tag{4.8}$$

podle modulu p. přitom čtverce čísel () nejsou kongruentní podle modulu p, neboť z podmínek $k^2 \equiv l^2 \pmod{p}$, $0 < k < l \leq \frac{p-1}{2}$ by plynulo, že kongruenci $x^2 \equiv l^2 \pmod{p}$ z čísel)) vyhovují čtyři: $x \equiv -l, -k, l, k$, což je spor.

Věta 4.10 *Nechť a je kvadratický zbytek podle modulu p. Pak platí*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}; \tag{4.9}$$

Je-li a kvadratický nezbytek podle moduli p, platí

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{4.10}$$

Důkaz: Malá Fermatova věta nám říká, že $a^{p-1} \equiv 1 \pmod{p}$. Tuto kongruenci lze psát také ve tvaru

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

Jelikož rozdíl obou závorek je roven dvěma, tak platí pouze jedna z kongruencí (), (). Každý kvadratický zbytek a vyhovuje při některém x kongruenci

$$a \equiv x^2 \pmod{p}, \tag{4.11}$$

a proto vyhovuje i kongruenci (), kterou obdržíme, umocníme-li obě strany kongruence na $\frac{p-1}{2}$. Kvadratickými zbytky jsou vyčerpána všechna řešení kongruence (). Kvadratické nezbytky musí tedy nezbytky vyhovovat kongruenci ().

4.8 Legendreův symbol

Legendreův symbol $\left(\frac{a}{p}\right)$ je roven 1 je-li a kvadratický zbytek a -1, je-li a kvadratický nezbytek podle modulu p, přičemž je $)a, p) = 1$. Číslo a se nazývá čitatel a číslo p jmenovatel Legendreova symbolu. Čteme a vzhledem k p. Zřejmě platí

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Jelikož čísla jedné a téže třídy jsou současně kvadratické zbytky nebo nezbytky, platí dále následující tvrzení.

Věta 4.11 *Nechť $a \equiv a_1 \pmod{p}$. Pak platí $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$.*

Jelikož $1 = 1^2$, je jednička kvadratický zbytek pro každý modul a tedy platí:

$$\left(\frac{a}{p}\right) = 1.$$

Lichá prvočísla můžeme vyjádřit buď ve tvaru $4k + 1$ nebo $4k + 3$. V prvním případě je ale výraz $\frac{p-1}{2}$ vždy číslo sudé, ve druhém pak liché. Číslo -1 je proto kvadratickým zbytkem prvočísel tvaru $4k + 1$ a kvadratickým nezbytkem prvočísel tvaru $4k + 3$. Platí tedy

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

Pro Legendreův symbol také platí:

$$\left(\frac{ab\dots l}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{l}{p}\right).$$

Vskutku máme

$$\left(\frac{ab\dots l}{p}\right) \equiv (ab\dots l)^{\frac{p-1}{2}} \equiv (a)^{\frac{p-1}{2}}(b^{\frac{p-1}{2}}\dots(l)^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\dots\left(\frac{l}{p}\right) \pmod{p}.$$

Důsledkem je, že v čitateli můžeme vypustit každý kvadratický činitel, tedy platí

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$

Věta 4.12 *Nechť p a q jsou lichá prvočísla. Pak platí*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Tato věta je v teorii čísel známa jako *Gaussův zákon kvadratické reciprocity*. Jako první ho dokázal Gauss, který ho nazval *theorema aurea* (zlatá věta). Tento zákon nám umožňuje ve spojení s výše uvedenými vlastnostmi značně zjednodušit výpočet Legendreova symbolu jak ukážeme níže. Důkaz zákona kvdratické reciprocity neuvádíme pro jeho délku, čtenář ho může najít např. v

Příklad: vypočtěte Legendreův symbol $L = \left(\frac{111}{1999}\right)$.
Nejpre si všimneme, že 111 je číslo složené a že platí $111 = 3.37$. Platí tedy

$$\left(\frac{111}{1999}\right) = \left(\frac{3}{1999}\right)\left(\frac{37}{1999}\right).$$

Nyní využijeme zákon kvadratické reciprocity, čímž v "čitateli"Legendreova symbolu obdržíme větší číslo než ve "jmenovateli". Máme tedy

$$L = (-1)^{999}\left(\frac{1999}{3}\right) \times (-1)^{999\cdot 18}\left(\frac{1999}{37}\right)$$

Pokud dělíme číslo 1999 trojkou či třiceti sedmi, dostaneme v obou případech jedničku. Jinými slovy 1999 je kongruentní s jedničkou jak podle modulu 37, tak i podle modulu 3. Můžeme tedy výpočet ukončit.

$$L = (-1)\left(\frac{1}{3}\right)\left(\frac{1}{37}\right) = -1.$$

Naskýtá se otázka, zda by nešlo zavést podobný symbol i v případě, že ve "jmenovateli"není prvočíslo. Tímto problémem se zabýval německý matematik C. G. Jacobi, který Legendreův symbol rozšířil následujícím způsobem.

Def. 4.1 *Nechť a je celé číslo a nechť $n \geq 3$ je liché. Nechť dále $n = p_1 p_2 \dots p_r$, kde p_i jsou lichá prvočísla, nikoliv nutně různá. Jacobiho symbol je definován vztahem*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right), \tag{4.12}$$

kde $\left(\frac{a}{p_i}\right)$ je Legendreův symbol.

Vlastnosti Jacobiho symbolu jsou analogické vlastnostem symbolu Legendreova včetně zákona kvadratické reciprocity, jeden významný rozdíl však přece najdeme. Je-li Legendreův symbol roven jedné, je vždy a kvadratický zbytek modulo p, to plyne z jeho definice. V případě Jacobiho symbolu to však platit nemusí, jak se můžeme přesvědčit z následujícího příkladu.

$$\left(\frac{1}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1,$$

dvojka však není kvadratický zbytek modulo 15.

4.9 Některé důležité věty z teorie čísel

Závěrem této kapitoly uvedeme několik vět z teoreie čísel.

Věta 4.13 *Malá Fermatova věta. Nechť p je prvočíslo a platí $(a, p) = 1$. Pak je*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{4.13}$$

Dnes je známo několik důkazů této věty, autor si dovolí přihřát svou polívčičku a odkázat čtenáře na publikaci [3]. Aby čtenáři nebyli zcela ošizeni, uvedeme elegantní důkaz pro speciální případ $a = 2$. Jednou z nejdůležitějších vět turbodidaktiky je *věta Tesákova*, která praví, že $1 + 1 = 2$. Využijeme-li tuto větu, máme

$$2^p = (1+1)^p = \binom{p}{0} + \binom{p}{1} + \dots + \binom{p}{p-1} + \binom{p}{p}.$$

Jelikož p je prvočíslo, jsou všechny binomické koeficienty $\binom{p}{k}$ dělitelné p s výjimkou $k = 0$ a $k = p$. Můžeme tedy od rovnosti přejít ke kongruenci, čímž obdržíme

$$2^p \equiv 2 \pmod{p} \Rightarrow 2^{p-1} \equiv 1 \pmod{p}.$$

Poslední úprava plyne ze skutečnosti, že podle předpokladu Malé Fermatovy věty je $(2, p) = 1$.

Důsledkem Malé Fermatovy věty je skutečnost, že podíl

$$q(a) = \frac{a^{p-1} - 1}{p}$$

je celé číslo. Podíl $q(a)$ se nazývá *Fermatův kvocient*.

Malou Fermatovu větu později zobecnil Euler.

Věta 4.14 *(Euler). Nechť a a n jsou přirozená čísla a* $(a, n) = 1$. *Pak platí*

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \tag{4.14}$$

kde $\varphi(n)$ *je Eulerova funkce, kterou jsme definovali v kapitole druhé.*

Připomeneme, že výraz $n! = n.(n-1)\ldots 2.1$ nazýváme n faktoriál. Dá se dokázat věta

Věta 4.15 *(Wilson) Nechť p je prvočíslo. pak platí*

$$(p-1)! \equiv -1 \pmod{p}. \tag{4.15}$$

Jelikož byla uvedena Malá Fermatova věta, sluší se též uvést i Velkou Fermatovu větu, i když tato přímo do tematiky tohoto textu nezapadá.

Věta 4.16 *Diofantická rovnice*

$$x^n + y^n = z^n \tag{4.16}$$

nemá pro $n > 2$ *řešení v oboru celých čísel.*

Jak již bylo řečeno, tato věta se přímo netýká probírané problematiky, avšak jedná se o velmi známý problém, takže pokud by se s ním chtěl někdo blíže seznámit, doporučujeme knihu [6].

4.10 Příklady k procvičení

1. Zjistěte, které z následujících kongruencí jsou řešitelné
   a) $6x \equiv 1 \pmod{9}$ b) $9x \equiv 3 \pmod{6}$ c) $14x \equiv 21 \pmod{70}$ Z2/110

2. Řešte kongruence
   a) $20x \equiv 4 \pmod{30}$ b) $20x \equiv 30 \pmod{4}$ c) $353x \equiv 254 \pmod{400}$ Z3/110

3. Najděte nejmenší přirozené číslo větší než 1, které vyhovuje kongruencím $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$, $x \equiv 1 \pmod{7}$. Z8/111

4. Řešte soustavu kongruencí $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 5 \pmod{2}$. Z9/111

5. Řešte soustavu kongruencí $x \equiv 1 \pmod{4}$, $x \equiv 0 \pmod{3}$, $x \equiv 5 \pmod{7}$. Z10/141

6. Najděte všechna celá čísla, která při dělení čísly 3, 4 a 5 dáv ají zbytky 1, 2 a 3. Z11/141

Kapitola 5

Speciální typy přirozených čísel

V této kapitole uvedeme některé speciální typy čísel, a to jak prvočísel, tak čísel složených. Tato kapitola nebude mít charakter učebního textu jako předchozí, čtenář se v ní seznámí s některými speciálními typy čísel a pozná různé zajímavosti, které pak bude moci uplatnit ve výuce. Čísla jsou totiž velmi zajímavá a můžeme říci že i tajuplná. Jednotlivé podkapitoly budeme řadit podle abecedy.

5.1 Dokonalá čísla

Jak již bylo řečeno, má každé přirozené číslo $n > 1$ přinejmenším dva dělitele, a sice 1 a n. Označme $\sigma(n)$ součet všech dělitelů čísla n. Zřejmě platí $\sigma(n) \geq 1$, porovnejme však součet dělitelů s dvojnásobkem čísla n. Zvolíme-li tuto hranici, tak se množina přirozených čísel $n > 1$ rozloží na tři navzájem disjunkntní podmnožiny. Do první zařadíme ta čísla, pro něž $\sigma(n) < 2n$ a budeme je nazývat *deficientní* (numeri deficientes). Tato množina je nekonečná, neboť sem patří mj. všechna prvočísla. Čísla pro něž $\sigma(n) > 2n$ nazveme *abundatní* (numeri abundantes). I tato množina je nekonečná, můžeme sem zařadit čísla tvaru $n = 2^k \cdot 3, \qquad k > 1$. Důkaz je snadný pro toho, kdo ovládá vzorec pro součet prvních n členů geometrické posloupnosti. Platí

$$\sigma(n) = \frac{2^{k+1}-1}{2-1}\frac{3^2-1}{3-1} = (2^{k+1}-1)\cdot 4 > 2\cdot(2^k\cdot 3) = 2n.$$

Třetí množinu pak tvoří čísla $n > 1$, pro něž je $\sigma(n) = 2n$. Tato čísla nazýváme *čísla dokonalá* (numeri perfecti), někdy též používáme název dokonalá čísla prvního druhu. Někdy se dokonalé číslo (prvního druhu) také definuje tak, že je rovno součtu všech svých pravých dělitelů, tedy dělitelů menších než je číslo samo. Nejmenší dokonalé číslo je 6=1+2+3. Ve starověku byla známa ještě tři další dokonalá čísla, a to 28, 496 a 8128. Je zajímavé, že již v Eukleidových Základech je uvedena postačující podmínka pro to, aby sudé číslo bylo dokonalé, ověřování však bylo zřejmě nad síly tehdejších počtářů. Jak si jistě čtenáři všimli, tak uvedená dokonalá čísla jsou sudá. Uvedeme proto nutnou a postačující podmínku pro to, aby sudé číslo bylo dokonalé.

Věta 5.1 *Sudé číslo $n > 1$ je dokonalé právě tehdy, když je tvaru*

$$n = 2^{s-1}(2^s - 1), \tag{5.1}$$

kde $s > 1$ je přirozené číslo a $M_s = 2^s - 1$ je prvočíslo.

Čísla M_s se nazývají *Mersennova čísla*. V následujícím důkazu je však pro zjednodušení zápisu budeme označovat písmenem p.

Důkaz: Důkaz postačující podmínky je snazší, proto jím začneme. Nechť nějaké číslo je tvaru (); tento tvar představuje zároveň jeho kanonický rozklad. Proto je

$$\sigma(n) = \frac{2^s - 1}{2 - 1} \frac{p^2 - 1}{p - 1}.$$

Odtud jednoduchou úpravou zjistíme, že $\sigma(n) = 2^s p = 2(2^{s-1}p)$, tedy n je dokonalé.

Dokážeme dále podmínku nutnou. Nechť n je sudé dokonalé číslo. Snadno nahlédneme, že jeho kanonický rozklad musí obsahovat přinejmenším jedno liché prvočíslo, neboť pak by bylo tvaru $2^k, k \geq 1$ a $\sigma(n) = 2^{k+1} - 1$ a číslo n by tedy nebylo dokonalé. Kanonický rozklad čísla n nechť je $n = 2^\alpha p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Položme $l = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ a $\alpha = s - 1$. Jelikož n je dokonalé, musí být

$$\sigma(n) = \frac{2^s - 1}{2 - 1} \frac{p_1^{\alpha_1 + 1} - 1}{p_1 - 1} \cdots \frac{p_1^{\alpha_k + 1} - 1}{p_1 - 1} = (2^s - 1)\sigma(l) = 2^s l,$$

protože

$$\sigma(l) = \frac{p_1^{\alpha_1 + 1} - 1}{p_1 - 1} \cdots \frac{p_1^{\alpha_k + 1} - 1}{p_k - 1}.$$

Rovnost

$$(2^s - 1).\sigma(l) = 2^s.l \tag{5.2}$$

ukazuje, že 2^s dělí součin $(2^s - 1).\sigma(l)$. Číslo 2^s je však dělitelné pouze čísly $\pm 1, \pm 2^r$, kde $1 \leq r \leq s$. Jelikož $2^s - 1$ je liché, pak je zřejmé, že čísla 2^s a $2^s - 1$ jsou nesoudělná, tedy $2^s \mid \sigma(l)$. Musí tedy existovat číslo $q \geq 1$ takové, že $\sigma(l) = 2^s.q$. Dosadíme-li do předchozí rovnosti (), obdržíme po zkrácení 2^s

$$(2^s - 1).q = l \tag{5.3}$$

neboli

$$2^s.q = \sigma(l) = l + q. \tag{5.4}$$

Číslo $l > 1$ je dělitelné l a podle () i q. Z rovnosti () vyplývá, že $l \neq q$, rovnost () pak říká, že číslo l nemůže mít jiné dělitele než l a q. Pokud by totiž existovalo číslo $d \geq 1$ a současně by d bylo různé od čísel l a q, byl by součet dělitelů čísla l roven přinejmenším $l + q + d$, což je v rozporu s (). Proto l má pouze dva dělitele, a to sebe sama a $q = 1$, je to tedy prvočíslo. Podle () je $l = 2^s - 1$, dokonalé číslo n je pak tvaru $2^{s-1}.(2^s - 1)$, $s > 1$ a $2^s - 1$ je prvočíslo.

Dokonalé číslo druhého druhu je takové číslo, které je rovno součinu všech svých pravých dělitelů. Příkladem je číslo 6 (6=1.2.3), které je dokonalé i prvního druhu. I pro dokonalá čísla druhého druhu existuje jednoduchý vzorec pro jejich určení, navíc z něho vyplývá, že je jich nekonečně mnoho.

Věta 5.2 *Číslo $n > 1$ je dokonalé číslo druhého druhu právě tehdy, když je buď třetí mocninou prvočísla, nebo je součinem dvou prvočísel.*

Je-li $n = p^3$, jsou jeho dělitelé 1, p a p^2 a jejich součin je roven n. Je-li $n = p_1.p_2$, Pak jsou tato prvočísla spolu s jedničkou jediní dělitelé a jejich součin je roven číslu n.

Nechť naopak je $n > 1$ dokonalé číslo druhého druhu. Předpokládejme, že jeho kanonický rozklad je $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Všechny dělitele čísla n seřadíme podle velikosti, je tedy $1 = d_1 < d_2 \dots < d_s = n$. Položme $\tau(n) = s$. Je tedy $n = d_1.d_2 \dots d_{s=1}$. Vynásobíme-li tuto rovnost číslem $n = d_s$, obdržíme

$$n^2 = d_1.d_2 \dots d_s. \tag{5.5}$$

Je-li d dělitelem čísla n, je jeho dělitelem i $\frac{n}{d}$. Proto můžeme psát

$$n^2 = \frac{n}{d_1} \cdot \frac{n}{n_2} \cdots \frac{n}{d_s}. \tag{5.6}$$

Vynásobíme-li předchozí dvě rovnosti, máme $n^4 = n^s$, z čehož plyne $s = 4$. Jelikož je $\tau(n) = (\alpha_1 + 1) \dots (\alpha_k + 1)$, jsou všechny závorky větší nebo rovny dvěma, proto je $k \leq 2$. Jsou tedy možné pouze dva kanonické rozklady čísla n. Buď je $n = p_1^{\alpha 1}$, nebo je $n = p_1^{\alpha_1}.p_2^{\alpha_2}$. V prvním případě je $\alpha_1 = 3$, ve druhém $\alpha_1 = \alpha_2 = 1$.

5.2 Fermatova čísla

V této části se opět setkáváme se jménem Fermat. Tento pán studoval také čísla tvaru

$$F_m = 2^{2^m} + 1, \qquad m = 0, 1, 2, \dots.$$

Fermat byl přesvědčen o tom, že jsou to prvočísla, přes veškeré úsilí se mu to však nepodařilo ani dokázat, ani vyvrátit, ačkoliv nástroje k tomu měl. Prvních pět těchto čísel jsou skutečně prvočísla, uslyšíme-li pojem Fermatovo prvočíslo, pak se bude jednat právě o tato čísla.

Zdálo by se, že zápis těchto čísel je zbytečně kommplikovaný, následující tvrzení však ukáže, že Fermat dobře věděl, proč zvolil tento tvar.

Věta 5.3 *Nechť n je přirozené číslo. Je-li $n = 2^n + 1$ prvočíslo, pak $m = 2^m$ pro nějaké $m \in \{0, 1, 2, \dots\}$.*

Nechť k a l jsou přirozená čísla, přičemž l je liché a současně je $l \geq 3$. V tomto případě platí formule

$$2^{kl} + 1 = (2^k + 1)(2^{k(l-1)} - 2^{k(l-2)+\dots-2^k+1)}.$$

Číslo tvaru $2^n + 1$ je vždy složené, je-li exponent dělitelný lichým přirozeným číslem větším než jedna. Formule pro Fermatova čísla tedy zabezpečuje splnění nutné podmínky pro to, aby tato čísla byla prvočísla.

Nyní si od čísel odpočineme a podíváme se do geometrie či chcete-li do planimetrie. Eukleidovské konstrukce kružítkem a pravítkem patří mezi krásné partie matematiky. Na jedné straně máme v hlavě absolutně přesné úvahy, tyto však nelze nikdy v praxi realizovat. Je to vlastně pěkný příklad platónské filozofie, kdy na papír dáváme jen stíny či odlesky ideální geometrie. Takové ořezávátko ještě vynalezeno

nebylo a v budoucnu ani nebude, aby jím ostrouhaná tužky narýsovala přímku, tedy délku bez šířky či jiné ideální geometrické útvary. Z velkého množství geometrických konstrukcí si vybereme sestrojení pravidelného n-úhelníka. Narýsovat rovnostranný trojúhelník, čtverec či pravidelný šestiúhelník je procházka růžovým sadem, s menšími problémy zvládneme i pravidelný pětiúhelník. Ačkoliv sedmička je považována za šťastné číslo, v případě pravidelného sedmiúhelníka to neplatí. Generace geometrů se o takovou konstrukci pokoušely, leč marně. Teprve Gaussovi se podařilo tento oříšek rozlousknout, když dokázal následující větu:

Věta 5.4 *Pravidelný n-úhelník lze sestrojit pravítkem a kružítkem právě tehdy když, $n = 2^i F_{m_1} F_{m_2} \cdots F_{m_j}$, kde $n \geq 3$, $i \geq 0$, $j \geq 0$ a $F_{m_1}, \ldots F_{m_j}$ jsou navzájem různá Fermatova prvočísla.*

Důkaz této věty přesahuje rámec tohoto textu, sdělíme jen, že problém geometrický je převeden na algebraický. Například pro středový úhel pravidelného pětiúhelníka platí $\cos \frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$. Nu a kosinus je roven délce přilehlé odvěsny pravoúhlého trojúhelníka s přeponou jedna a tuto úsečku dovedeme sestrojit kružítkem a pravítkem. Jelikož jediná dosud známá prvočísla jsou 3, 5, 17, 257 a 65537, je zřejmé, že eukleidovská konstrukce pravidelného sedmiúhelníka (a samozřejmě mnoha dalších s lichým počtem stran) z principu není možná. Existují i další souvislosti mezi Fermatovými prvočísly a geometrií, jelikož přesahují rozsah obvykle probírané látky na základních či středních školách, tak je neuvádíme a zájemce odkazujeme např. na publikaci [2].

Po návratu z geometrického výletu uzavřeme část věnovanou Fermatovým číslům. Je tak trochu záhada, proč Fermat nenašel, že $F_5 = 641.6700417$, to se podařilo až Eulerovi. Na druhou stranu dnes chápeme, že tento geniální Francouz nenašel v tomto směru žádný důkaz. Ten se totiž nenašel dodnes, přestože je těmto číslům věnována současnými matematiky velká pozornost. Tato čísla jsou totiž velká, či přesněji jejich dekadický zápis obsahuje mnoho cifer (např. F_{18} jich má téměř 80 000. Byly zapojeny i počítače a vyvinuty metody na faktorizaci velkých čísel, zatím máme jedinou jistotu, a sice že pro $5 \geq m \geq 32$ se jedná o čísla složená, přestože pro F_{20} a F_{24} neznáme žádného netriviálního dělitele. Nepodařilo se zatím ani najít nějakou zákonitost, která by v tomto směru něco napověděla. Teorie čísel tedy před nás staví další výzvu.

5.3 Spřátelená čísla

Def. 5.1 *Dvě různá přirozená čísla a a b nazýváme spřátelená, jestliže součet pravých dělitelů čísla a je roven b a současně je součet pravých dělitelů čísla b roven a.*

Příkladem budiž dvojice 220 a 284, kterou znali již pythagorejci. Skutečně, praví dělitelé prvního z nich jsou čísla 1, 2, 4, 5, 10, 11, 20, 22, 44, 55 a 110; součet těchto čísel je 284. Číslo 284 nemá tolik pravých dělitelů jsou jen čísla 1, 2, 4, 71 a 142 a jejich součet je 220. Do publikace [7], která byla určena především řešitelům matematické olympiády, se vloudila malá chybička, kdy místo 71 je uvedeno 7.

Věta 5.5 *Čísla a a b jsou spřátelená právě tehdy, když $\sigma(a) = \sigma(b) = a + b$.*

Důkaz: Je zřejmé, že počet pravých dělitelů čísla m je $\sigma(m) - m$. Jsou-li a a b spřátelená je současně $\sigma(a) - a = b$ a $\sigma(b) - b = a$. Vypočítáme-li z druhé rovnice b a dosadíme do první, máme $\sigma(a) = \sigma(b)$. Je-li naopak $\sigma(a) = \sigma(b) = a + b$, snadno nahlédneme, že $\sigma(a) - a = b$ a současně $\sigma(b) - b = a$ a že tedy čísla a a b jsou spřátelená.

I v případě spřátelených čísel nebylo zatím vše objasněno. Nevíme například, zda je jich konečně či nekonečně mnoho. Zatím všechny dvojice spřátelených čísel mají největší společný dělitel větší než jedna. Známe však dvojici lichých spřátelených čísel $a = 3^3.5.7.11$ a $b = 3.5.7.139$.

Hledat spřátelená čísla můžeme podle návodu, který udal v 9. stol. arabský matematik Ben Korrah.

Věta 5.6 *Nechť existují pro $n > 1$ prvočísla tvaru $p = 3.2^{n-1} - 1$, $q = 3.2^n - 1$ a $r = 9.2^{2n-1} - 1$. Pak čísla $k = 2^n pq$ a $l = 2^n.r$ jsou spřátelená.*

Důkaz: Jako první krok dokážeme, že součet všech dělitelů čísla k je roven součtu dělitelů čísla l. Pro součet dělitelů $\sigma(k)$ platí

$$\sigma(2^n.p.q) = (2^{n+1} - 1).(p + 1).(q + 1) = (2^{n+1} - 1).9.2^{2n-1}.$$

Pro součet dělitelů $\sigma(l)$ zase platí

$$\sigma(2^n.r) = (2^{n+1} - 1)(r + 1) = (2^{n+1} - 1)9.2^{2n-1}.$$

Jako druhý krok musíme dokázat, že tento součet je roven $k + l$.

$$k + l = 2^n pq + 2^n r = 2^n(pq + r) = 9.2^{2n-1}(2^{n+1} - 1) = \sigma(k) = \sigma)l).$$

5.4 Závěr kapitoly

V závěrem této kapitoly uvedeme stručně některá další speciální prvočísla. Připomeňme si nejdříve Eukleidův důkaz o nekonečném počtu prvočísel, v němž stěžejní úlohu hrál výraz $n = p_1 p_2 \dots p_k + 1$. Číslo n může, ale také nemusí být prvočíslo. Je-li prvočíslo, pak je budeme nazývat *Eukleidovo prvočíslo*. Eukleidův důkaz můžeme lehce pozměnit tak, že místo čísla n sestavíme číslo $m = p! + 1$, kde p je největší prvočíslo, jichž předpokládáme konečný počet. Ani v tomto případě není číslo m dělitelné žádným prvočíslem, neboť pro každé $q \leq p$ je zbytek po dělení čísla m číslem q vždy roven jedné. To jsme ale zkonstruovali prvočíslo větší než p, nebo je m dělitelné prvočíslem větší než p, v každém případě jsme se dostali do sporu s předpokladem. Prvočísla tvaru $k! + 1$ nazýváme *faktoriální*. Týmž názvem se označují i prvočísla tvaru $k! - 1$. V obou případech nevyžadujeme, aby k bylo prvočíslo.

Kapitola 6

Aplikace teorie čísel

Pokud se čtenář v tomto textu propracoval až k této kapitole, tak si mohl myslet následující. Teorie čísel je velmi hezkou součástí matematiky, obsahuje řadu zajímavých tvrzení, některé důkazy jsou velmi elegantní, řada poznatků se dá využít pro zpestření výuky, zajímavá jsou i některá dosud nedokázaná ani nevyvrácená tvrzení, ale jaký to má význam pro praxi? Nejedná se zde jen o sice krásnou, ale jinak neužitečnou vědu? V této kapitole se pokusíme dokázat, že tomu tak není, že teorie čísel je pro praxi velice významná a její důležitost poslední dobou neustále roste. A začneme tím, s čím je spojen každý občan našeho státu od kolébky až po rakev. Ano, začneme rodným číslem.

6.1 Rodná čísla

Každý občan České republiky má již od narození přidělené rodné číslo, které se sestaví tak, že prvních šest čísel je dáno datem narození. První dvojčíslí udává rok, druhé měsíc a třetí den narození. Kvůli rozlišení pohlaví se druhé dvojčíslí u dívek přičítá padesátka. Rodné číslo hochů, kteří se narodili například 10. prosince 1996 začíná šestičíslím 961210, u děvčat je to 966210. Protože se denně rodí více dětí, přidávají se za tuto šestici ještě další čísla. U nás se od roku 1986 přidávají ještě další čtyři čísla, rodná čísla jsou tedy deseticiferná. Poslední čtyřčíslí se však nevolí náhodně, nýbrž tak, aby celé rodné číslo bylo dělitelné jedenácti. Jaký je k tomu důvod, nestačilo by například seřadit děti narozené v jednom dni například podle času, kdy přišly na svět a pak jim přiřadit čísla odpovídající pořadí?

Abychom mohli zodpovědět tuto otázku, dokážeme nejdříve kritérium pro dělitelnost jedenácti. Nechť k$\in \{0,1,2,\ldots\}$ a $m = \sum_{n=0}^{k} c_n 10^n$ pro $c_n \in \{0,1,2,\ldots,9\}$, $c_k \neq 0$, tedy $c_k,\ldots,c_0$ jsou cifry přirozeného čísla m v desítkové soustavě. Pak

$$11 \mid m \Leftrightarrow 11 \mid \left(\sum_{n=0}^{k} (-1)^n c_n\right). \tag{6.1}$$

Důkaz. Podle vzorce pro rozdíl dvou n-tých mocnin platí

$$10^n - (-1)^n = (10+1)[10^{n-1} + 10^{n-2}(-1) + \cdots + 10(-1)^{n-2} + (-1)^{n-1}], \tag{6.2}$$

kde hranatá závorka obsahuje právě n sčítanců. Rozdíl $10^n - (-1)^n$ je tedy dělitelný

11. Použijeme-li nyní vzorec () na každý sčítanec v () kromě posledního, pak dostaneme

$$11 \mid ((-1)^k c_k + (-1)^{k-1} c_{k-1} + \cdots + c_1 + c_0). \tag{6.3}$$

Podobně zjistíme, že když platí (), je splněn i vztah ().

Vraťme se nyní k našemu chlapci, jehož rodné číslo může být 9612107032. Dejme tomu, že se při jeho zadávání spleteme v jedné cifře. Pak rozdíl mezi správným a špatně zadaným číslem bude $\pm c \cdot 10^n$, kde $c \in \{1, 2, \ldots, 9\}$. Tento rozdíl není nikdy dělitelný číslem 11, ale může být dělitelný složenými čísly 12, 14, 15 atd. Napíšeme-li v našem rodném čísle místo sedmičky jedničku, je rozdíl mezi správným a špatným rodným číslem 6 000. Nalezení všech jeho dvojciferných dělitelů pak přenecháváme čtenáři. Protože číslo 11 nám umožňuje odhalit chybu, hovoříme o *jedenáctkovém samodetekujícím kódu*.

Při použití jednociferných prvočísel se obecně nedá odhalit chyba při vložení jedné nesprávné cifry. Použití větších dvojciferných prvočísel nám zase snižuje počet použitelných rodných čísel. Jedenáctka je tedy pro potřeby rodného čísla optimální. Závěrem přidáme ještě jednu zajímavost. Česká dvoukoruna je pravidelný jedenáctiúhelník. Položíme minci do základní polohy a pak ji střídavě otáčíme po a proti směru hodinových ručiček o tolik vrcholů, kolik je příslušná cifra. Po posledním pootočení se mince musí vrátit do původní polohy.

Na podobném principu fungují rovněž kódy ISBN a ISSN pro knihy či časopisy, identifikační čísla organizací (IČO), bankovní účty a pod. Více se lze dočíst např na [10]. Samodetekující kódy dovedou chybu najít, nikoliv opravit. Z tohoto důvodu byly vyvinuty kódy samoopravné. Ty nám umožňují pomocí redundantní (nadbytečné) informace obsažené v kódových slovech stanovit, ve kterém znaku došlo k chybě, a opravit ji. Velká budoucnost je vkládána do tzv. dvourozměrných kódů s vysokou informační kapacitou a schopností detekce a opravy chyb. Tyto kódy se používají mj. v amerických řidičských průkazech či různých identifikačních kartách. Jejich výhodou je, že se tisknou a přenášejí na papíru a že zde není nutnost vkládat data z klávesnice.

6.2 Šifrování zpráv pomocí velkých prvočísel

Potřeba utajit písemná sdělení je patrně tak stará, jako písmo samo. V průběhu tisíciletí lidé vynalezli řadu způsobů, jak zabránit nepovolané osobě, které se dostala do rukou tajná zpráva, aby ji přečetla. Jako příklad můžeme uvést šifrování pomocí mřížky, které používal Matyáš Sandorf a jeho přátelé. Stačilo však, aby se padouch Sarkany dostal k mřížce a přečtení zpráv již pro něj nepředstavovalo žádný problém. Jindy k rozluštění stačilo logické uvažování. Geniální detektiv Sherlock Holmes takové šifry luštil běžně. Šifru spočívající v tom, že každé písmeno bylo nahrazeno tančící figurkou, rozluštil pomocí frekvence výskytu jednotlivých písmen. Zatímco v české abecedě je to písmeno a, v angličtině to je litera e. Stejný postup volí i luštitelé tzv. číselných křížovek. Jiná metoda spočívá v tom, že se slovo nahradí číslem, určujícím pořadí slova na jisté stránce knihy, kterou mají obě strany k dispozici. V tomto případě se nedoporučuje, aby klíčem byly kniha o více dílech. Dobrý voják Švejk logicky nafasoval pro pány oficíry první díl knihy Hříchy otců, jenže klíčem byl díl druhý a jedenáctá marškumpanie nemohla tuto šifru používat.

Uvedené případy jsou staršího data, kdy si luštitel šifry musel vystačit jen se svým intelektem. V době počítačů se zdá, že není v lidských silách vymyslet takovou šifru, která by před řešiteli obstálo, neboť co jeden člověk vymyslí, druhý rozluští, jak pravil Sherlock Holmes. Avšak matematika není nadarmo považována za královnu věd. Pánové Rivest, Shamir a Adelman objevili v roce 1978 metodu, která se podle počátečních písmen jejich příjmení nazývá RSA. Oč je metoda jednodušší, o to je účinnější, dokonce není nutné tajit šifrovací klíč, šifrovat může každý. Zatím však bez znalosti dešifrovacího klíče není a vypadá to, že ani v budoucnu nebude možné tyto šifry rozluštit. Jádrem pudla je totiž skutečnost, že není problém vynásobit dvě velká čísla. Mnohem nesnadnější je inverzní proces, tedy rozložit číslo složené na součin prvočinitelů.

Popíšeme nyní postup při šifrování a dešifrování zprávy. Utajované sdělení převedeme nejprve na přirozené číslo x. K tomu nám mohou posloužit například kódy ASCII, ale jejich použití není podmínkou, existují i jiné a možná i efektivnější způsoby. Dále budeme předpokládat, že $x < n$, kde n je součin dvou různých prvočísel, která nejsou veřejně známa a mají více než 100 cifer. Psavci musí samozřejmě rozdělit zprávu na několik kratších tak, aby pro každou z nich byla splněna předchozí nerovnost. Zašifrovanou zprávu označíme symbolem $x*$. Toto přirozené číslo je jednoznačně dáno nerovností $x* < n$ a kongruencí

$$x* \equiv x^e \pmod{n}, \tag{6.4}$$

kde e se nazývá *šifrovací exponent* (z anglického encryption). Čísla e a n jsou veřejně známa a k zašifrování stačí.

Odšifrování probíhá zcela analogicky. Znovu se definuje číslo $(x*)^0 \in N$ splňující nerovnost $(x*)^0 < n$ tak, aby $(x*)^0 \equiv (x*)^d \pmod{n}$. *Dešifrovací exponent* d (z anglického decryption) však není veřejně znám. Je však nutno vyřešit otázku, jak zvolit exponenty e a d tak, aby $(x*)^0 = x$, tedy aby zašifrovaná zpráva byla po odšifrování totožná s původní zprávou x.

Nejdříve dokážeme následující větu: Nechť pro přirozené číslo n platí

$$(e, \varphi(n)) = 1. \tag{6.5}$$

Potom existuje právě jedno přirozené číslo $d < \varphi(n)$ takové, že

$$ed \equiv 1 \pmod{\varphi(n)}. \tag{6.6}$$

Důkaz: Pro přirozená čísla $k = 1, \ldots, \varphi(n)-1$ definujeme zbytky $z_k \in \{1, \ldots, \varphi(n)\text{-}1\}$ pomocí kongruence

$$ek \equiv z_k \pmod{\varphi(n)}.$$

Pokud se dva zbytky rovnají, například je $z_{k_1} = z_{k_2}$, je správná kongruence

$$e(k_1 - k_2) \equiv 0 \pmod{\varphi(n)}.$$

Pak podle předpokladu a věty 1. 3. (Křížek) existují celá čísla v a y tak, že $ev + \varphi(n)y = 1$, tedy je $e(k_1 - k_2)v + \varphi(n)(k_1 - k_2)y = k_1 - k_2$. Odsud plyne $k_1 - k_2 \equiv 0 \pmod{\varphi(n)}$, čili $k_1 = k_2$. Všechny zbytky z_k jsou navzájem různá čísla a proto existuje právě jedno d odpovídající zbytku 1, které splňuje ().

Dále dokážeme, že zašifrovaná zpráva $x*$ je po odšifrování totožná s původní zprávou x.

Věta 6.1 *Nechť platí* $(e, \varphi(n)) = 1$. *Pak*

$$(x*)^0 = x. \tag{6.7}$$

Důkaz: Z kongruence () plyne existence takového čísla r, že

$$ed = 1 + r\varphi(n) \tag{6.8}$$

Rozlišujeme dva případy:

1. Nechť platí $(x, n) = 1$. Potom lze Eulerův vztah umocnit na r-tou a vynásobit jej poté x, čímž obdržíme

$$x^{1+r\varphi(n)} \equiv x \pmod{n} \tag{6.9}$$

Nyní postupně z (), (), (), a (), plyne, že

$$(x*)^0 \equiv (x*)^d \equiv x^{ed} \equiv x^{1+r\varphi(n)} \equiv x \pmod{n}. \tag{6.10}$$

Vztah () tedy platí, neboť obě přirozená čísla x i $(x*)^0$ jsou menší než n.

2. Nechť je $(x, n) \neq 1$. Potom je buď $x = p$ nebo $x = q$. Bez újmy na obecnosti můžeme předpokládat druhou možnost. Jelikož $(p, q) = 1$ můžeme umocnit Fermatův vztah umocnit na $r(q-1)$, čímž obdržíme

$$x^{(p-1)(q-1)} \equiv 1 \pmod{p}.$$

Jelikož $\varphi(n) = (p-1)(q-1)$, platí

$$x^{1+r\varphi(n)} \equiv x \pmod{px}$$

To je opět vztah (), protože $px = pq = n$. Dál postupujeme jako v bodě 1.

Šifrovací exponent e se volí tak, aby $3 \leq e < \varphi(n)$ a aby platilo $(e, \varphi)n)) = 1$. Navíc je třeba zvolit e tak, aby $e^m \not\equiv 1 \pmod{\varphi(n)}$ pro malá m, aby nebylo možno odšifrovat zprávu pro $d = e-1$. Pokud neznáme hodnoty p a q, a pokud je neznáme, je téměř nemožné stanovit hodnotu dešifrovacího exponentu d. Z věty x. x. však víme, že existuje právě jedno přirozené číslo $d < \varphi(n)$ splňující kongruenci (). Naskytá se otázka jak stanovit jeho hodnotu, známe-li p a q.

Pokud umíme rozložit $\varphi(n)$ na prvočísla, pak lze jednoduše vypočítat hodnotu $\varphi(\varphi(n))$. Z Eulerovy věty plyne implikace

$$(e, \varphi(n)) = 1 \Rightarrow e^{\varphi(\varphi(n))} \equiv 1 \pmod{\varphi(n)}.$$

Vynásobíme-li předchozí kongruenci d a využijeme-li (), pak dostaneme explicitní vyjádření pro dešifrovací exponent $d < \varphi(n)$,

$$d \equiv de^{\varphi(\varphi(n))} \equiv ede^{\varphi(\varphi(n))-1} \equiv e^{\phi(\varphi(n))-1} \pmod{\varphi(n)}. \tag{6.11}$$

Pokud $\varphi(n)$ neumíme rozložit na prvočísla, lze d počítat přímo z kongruence (), a to třebas Eukleidovým algoritmem či prostě zvolíme jiné p či q.

6.3 Kouzla s čísly

Když jsem byl ještě malý hošík, bylo vždy obrovskou událostí, když na dědinu přijel kouzelník. Všichni jsme byli nadšeni z jeho triků, ať již to byla kouzla s kartami, mizení či naopak nečekané objevování se věcí a jiné a jiné zázraky, které nás fascinovaly. Kouzelník obvykle v rámci představení jeden trik prozradil, potom všichni žasli, jak je to vlastně jednoduché. Takovým iluzionistou však může být každý a nebude k tomu ani potřebovat hbité prsty, stačí jen využít některé zajímavé vlastnosti čísel. Ostatně v předchozím textu jsme se mohli přesvědčit, že čísla před námi ukrývají spoustu tajemství a je otázkou, zda se nám je vůbec podaří objasnit. Závěrem si proto uvedeme některé čáry s čísly. Další pak může čtenář nalézt v publikacích zaměřených na rekreační matematiku a pokud bude mít i dost času na listování starými novinami, tak i v zábavných okenkách nedělních či později sobotních příloh deníků.

Kouzlo první: Zvolte si libovolné trojciferné číslo tak, aby se první a poslední číslice lišily alespoň o dvě. Utvořte číslo, jehož cifry jsou v opačném pořadí a od většího čísla odečtěte menší. Ve výsledku opět zaměníme pořadí číslic a tato dvě čísla sečteme. Dejme tomu, že si vybereme číslo 115. Pak je třeba spočítat 511-115=396. Dále musíme sečíst čísla a 396 a 693. V našem případě obdržíme 1089. My narozdíl od kouzelníků vysvětlíme každý trik, budeme proto předpokládat, že zvolíme číslo $100a+10b+c$, přičemž $a \geq c+2$. Pak $100a+10b+c-100c-10b-a = 100(a-c)-a+c = 100(a-c-1)+90+(10-a+c)$. Přičteme-li k tomuto výsledku číslo $100(10-a+c)+90+(a-c-1)$, obdržíme 900+180+9=1089. Tento výsledek nezávisí na volbě cifer a výsledek 1089 bude při libovolné volbě původního čísla.

Kouzlo druhé: Zvolme dvě libovolná čísla. Utvořme posloupnost podobným způsobem jak to udělal Fibonacci, tedy každý další člen je součtem dvou předchozích. Sečtěme prvních deset členů této posloupnosti a vydělme ho členem sedmým. Například si zvolíme 3 a 7. Prvních deset členů posloupnosti bude 3, 7, 10, 17, 27, 44, 71, 115, 186, 301 a jejich součet pak 781. Vydělíme-li toto číslo 71, obdržíme 11. Toto číslo musí vyjít vždy. Je-li totiž $f_1 = m$ a $f_2 = n$, je $f_7 = 5m + 8n$ a $\sum_{i=1}^{10} f_i = 55m + 88n = 11f_7$. Ke kouzlu lze použít i komplexní čísla, je však třeba dát pozor, aby $f_7 \neq 0$.

Kouzlo třetí: Vezměme libovolné přirozené číslo, které je dělitelné třemi. Cifry umocníme na třetí a sečteme, čímž obdržíme nové přirozené číslo. Tento postup opakujeme, avšak zjistíme, že až dospějeme k číslu 153, se celý proces zacyklí. Učeně řečeno budeme-li opakovaně sčítat třetí mocniny cifer přirozeného čísla dělitelného třemi, vždy dospějeme k číslu 153. Mysleme si číslo 1422. Pak platí $1^3+4^3+2^3+2^3 = 81 \mapsto 8^3+1^3 = 513 \mapsto 5^3+1^3+3^3 = 153$. Označíme-li $n = c_k 10^k + \cdots + c_1 10 + c_0$ a $m = c_k^3 + \cdots + c_1^3 + c_0^3$, pak z předpokladu $3|n$ plyne $3|m$. Z kritéria pro dělitelnost trojkou plyne, že $n \equiv \sum_{i=0}^{k} c_i^3 \pmod 3$. Podle Malé Fermatovy věty je $c_i^3 \equiv c_i \pmod 3$. Je tedy

$$m = \sum_{i=0}^{k} c_i^3 \equiv \sum_{i=0}^{k} c_i \equiv n \pmod 3.$$

Dále je

$$n = \sum_{i=0}^{k} c_i 10^i \geq c_k 10^k \geq 10^k > (k+1)9^3 \geq \sum_{i=0}^{k} c_i^3 = m.$$

Je-li tedy $n \geq 10^4$, je součet třetích mocnin cifer vždy menší než původní číslo. Zbývá tedy prověřit, jak se řetězec bude chovat po překročení této hranice. Využitím výpočetní techniky lze ověřit, že je zde konečný počet možností aže všechny vedou k číslu 153. Závěrem dodejme, že existují i jiná čísla, která se rovnají součtu třetích mocnin přirozených čísel. Kromě singulárního případu jedničky jsou to i čísla 370, 371 a 407, žádné z nich však není dělitelné třemi.

Kouzlo čtvrté: Zvolme libovolné trojciferné číslo, jehož cifry nejsou všechny stejné. Seřaďme cifry podle velikosti v obou směrech a odečtěme tato dvě čísla. Po konečném počtu kroků dojdeme k číslu 495. Zvolíme-li 169, máme 961-169=792; 972-279=693; 963-369=594; 954-459=495. Pokud by rozdíl měl dvě cifry, je nutno ho doplni zepředu nulou. Stejná vlastnost platí i pro čtyřciferná čísla, kdy se dostaneme k číslu 6174. Toto číslo se na počest objevitele nazývá *Kaprekarova konstanta*. Vzhledem ke konečnému počtu čísel lze turo zajímavost ověřit na počítači.

Závěrem této kapitoly zabrousíme do turbodidaktiky. Euler odvodil vzorec $e^{\mathrm{i}\pi} + 1 = 0$. V tomto vzorci se vyskytují všechny aritmetické operace (sčítání, násobení, mocnění) a též nejdůležitější matematické konstanty (0, 1, i, e, π právě jednou a je proto matematickými estéty považován za nejkrásnější. (Pokud bychom použili synonymum formule, mohli bychom psát Miss formule.) Proveďme turbodidaktické kouzlo a upravujme tento vztah.

$$e^{\mathrm{i}\pi} = -1 = (-1)^3 = (e^{\mathrm{i}\pi})^3 = e^{3\mathrm{i}\pi}.$$

Jelikož levá strana rovná se pravé, můžeme odlogaritmovat a máme $\mathrm{i}\pi = 3\mathrm{i}\pi$ či $1 = 3$. Znalec funkce komplexní proměnné rozdíl mezi matematikou a turbodidaktikou odhalí hned; pro jistotu však dodáváme, pro komplexní proměnnou není logaritmus jednoznačná funkce, takže logaritmování nebylo korektní.

6.4 Úlohy na procvičení

Abychom učinili požadavkům projektu zadost, přece jen uvedeme několik úloh, na kterých si čtenář procvičí znalosti z předchozího textu.

1. Myslete si libovolné číslo od šesti do šedesáti. Toto číslo postupně dělte třemi, čtyřmi a pěti a nahlaste zbytky. Znalec čísel podle zbytků určí původní číslo. Jak je to možné?

2. Vynásobte svůj věk deseti od tohoto čísla odečtěte devítinásobek libovolného jednociferného čísla. Řekněte výsledek a já uhádnu, jak dlouho již putujete po tomto světě. Jak je to možné?

3. A ještě jednu na věk. Své mládí (stáří) vynásobte dvěma, přičtěte pět, součet opět vynásobte pěti a řekněte výsledek. I z tohoto čísla poznám, kolik let jste se dožil. Jak je to možné?

4. Nedosti však na tom, umíme uhodnout i přesné datum narození, a to následujícím způsobem. Pořadové číslo měsíce věku vynásobíme stem. K výsledku přičteme číslo značící den a výsledek vynásobíme dvěma. K výsledku přidáme osm. Dále násobíme pěti a přidáme čtyři. Tento výsledek vynásobíme desíti a

přidáme čtyři. Poslední operací je přičtení věku v rocích. Odečteme 444 a výsledek rozdělíme na skupiny po dvou cifrách od pravé strany. Kvůli vyváženosti to teď vezmeme zleva; první dvojice určuje měsíc, druhá den a třetí věk zkoumaného člověka.

5. Také umíme uhodnout dané číslo. Od myšleného čísla odečteme jedničku, zbytek násobíme dvěma a přičteme myšlené číslo. Z tohoto výsledku uhodneme myšlené číslo tak, že přičteme dvě a vydělíme třemi.

Výsledky aplikace teorie čísel. Je-li myšlené číslo x, pak máme $x = 3a + r_1$, $x = 4b + r_2$, $x = 5c + r_3$. Vyjádříme jednotlivé zbytky a spočítáme výraz $S = 40r_1 + 45r_2 + 36r_3 = 121x - 120a - 180b - 180c$. Výraz $S = 120k + x$, proto stačí podělit S 120 a zbytek je roven myšlenému číslu.

Označme věk x a myšlené číslo k. Podle postupu jsme obdrželi $10x - 9k = 10(x - k) + k$. Číslo k je na místě jednotek, zbytek tvoří rozdíl $x - k$. Z uvedeného je zřejmé, že váš oponent musí být starší devíti let.

Neznámý věk označíme opět x. Úpravy jsou tyto: $(2x + 5).5 = 10x + 25 = 10(x+2)+5$. Dál postupujeme jako v předchozím případě, na rozdíl od předchozího případu to funguje i pro mimina.

Počítáme vlastně $\{[(100m+d).2+8].5+4\}.10+4+r-444=10000m+100d+r$.

Počítáme takto: $x = 1$; $2(x - 1)$; $2(x - 1) + x = 3x - 2$; $3x - 2 + 2$.

Literatura

[1] Dobrovolný B.: Nové matematické rekreace. SNTL Praha 1967

[2] Křížek M., Somer L., Šolcová A.: Kouzlo čísel (Od velkých objevů k aplikacím. Academia Praha 2011

[3] Lepka K.: Historie Fermatových kvocientů (Fermat-Lerch). Dějiny matematiky sv. 14, Prometheus Praha 2000

[4] Novoveský Š., Križalkovič K., Lečko I.: Zábavná matematika. Státní pedagogické nakladatelství Praha 1974

[5] Sierpiński W.: Co víme a nevíme o prvočíslech. Státní pedagogické nakladatelství Praha 1966

[6] Singh S.: Velká Fermatova věta. Academia Praha 2000

[7] Šalát T.: Dokonalé a spriatelené čísla. Škola mladých matematiků. Mladá fronta Praha 1969

[8] Vinogradov, I. M.: Základy theorie čísel. Nakladatelství Československé akademie věd. Praha 1953

[9] Znám, Š.: Teória čísel. Vydavatelstvo technickej a ekonomickej literatúry Alfa Bratislava 1977.

[10] `http://www.kodys.cz`