Gymnázium Christiana Dopplera, Zborovská 45, Praha 5

ROČNÍKOVÁ PRÁCE

Teorie čísel a RSA algoritmus

Vypracoval: Vojtěch Lengál
Třída: 8.M
Školní rok: 2017/18
Seminář: Matematický seminář

Prohlašuji, že jsem svou ročníkovou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím s využíváním práce na Gymnáziu Christiana Dopplera pro studijní účely.

V Praze dne 30.1.2018 Vojtěch Lengál

Obsah

1. Úvod

2. Teorie čísel

Teorie čísel je odvětví matematiky, které se zabývá čísly a jejich vlastnostmi. Číslem budeme, pokud nebude v zadání řečeno jinak, rozumět přirozené číslo.
Praktické využití tohoto oboru je překvapivě velké, s aplikací teorie čísel se rozhodně nesetkáme jen v ostatních oborech matematiky. Zejména v kryptografii a šifrování má teorie čísel velký význam. Např. jeden z nejznámějších šifrovacích algoritmů RSA je (zjednodušeně řečeno) postaven na předpokladu, že rozložit velké číslo na součin prvočísel je velmi obtížná úloha. Z čísla $n = pq$ je tedy v rozumném čase prakticky nemožné zjistit činitele p a q, oproti tomu násobení dvou velkých čísel je triviální úloha.

2.1 Dělitelnost a kongruence

V této sekci se budeme zabývat dělitelností a kongruencemi. K tomu se nám bude hodit, pokud se nejdříve seznámíme s několika základními pojmy a tvrzeními.

Říkáme, že číslo a dělí číslo b (zapisujeme $a \mid b$), pokud existuje takové celé číslo c, že $b = ac$. Můžeme také říct, že číslo b je dělitelné číslem a nebo číslo b je násobek čísla a. V opačném případě a nedělí b ($a \nmid b$).

Pro každé celé číslo n platí: $1 \mid n$ a $n \mid n$.

Pokud $a \mid b$ a zároveň $b \mid c$, tak $a \mid c$.

Pokud $a \mid b$ a zároveň $a \mid c$, tak pro $b \geq c$ platí: $a \mid (b \pm c)$.

Pokud $a \mid b$ a zároveň $c \mid d$, tak $ac \mid bd$.

Pokud $a \mid b$, tak $a \leq b$.

Pokud $a \mid b$, tak $a \mid kb$, $k \in \mathbb{N}$.

Prvočíslo je takové číslo, které má pouze 2 kladné dělitele: jedničku a samo sebe. Číslo, které má více kladných dělitelů, nazýváme číslo složené. Číslo 1 tedy není ani prvočíslo, ani číslo složené.

Základní věta aritmetiky: Každé přirozené číslo větší než 1 lze jednoznačně rozložit na součin prvočísel.

Číslo x s prvočíselným rozkladem $x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ má právě $(a_1 + 1)(a_2 + 1) \dots (a_n + 1)$ dělitelů. Proč toto platí? Pro vytvoření libovolného dělitele můžeme použít prvočíslo p_x právě $a_x + 1$ způsoby $(p_x^0, p_x^1, \dots, p_x^{a_x})$. Tuto úvahu můžeme zopakovat pro libovolné prvočíslo v rozkladu a získáme tedy výše uvedený vztah.

Největší společný dělitel čísel a, b (značíme $NSD(a,b)$, popř. $D(a,b)$) je největší číslo, které dělí současně a i b. Pokud $NSD(a,b) = 1$, říkáme, že čísla a, b jsou nesoudělná. V opačném případě jsou čísla a, b jsou soudělná. Tedy např. čísla 6 a 15 jsou soudělná a čísla 4 a 21 jsou nesoudělná.

Pokud $a \mid bc$ a čísla a, b jsou nesoudělná, tak $a \mid c$. Pokud jsou ale čísla a, b soudělná, tak tvrzení nemusí platit (př. $6 \nmid 4$ a $6 \nmid 9$, ale $6 \mid 4 \cdot 9 = 36$).

Pro čísla a, b, $a \geq b$ platí: $NSD(a,b) = NSD(a-b,b)$. Na tomto faktu je založen tzv. Euklidův algoritmus, který slouží pro zjištění největšího společného dělitele 2 čísel. Čísla a, b můžeme tedy snižovat, aniž bychom změnili jejich NSD. Po konečném počtu kroků skončíme ve stavu $NSD(z,0) = z$.

Nejmenší společný násobek čísel a, b je nejmenší číslo, které je dělitelné číslem a i číslem b. Značíme $nsn(a,b)$, popř. $n(a,b)$.

Čtvercem nazýváme druhou mocninu přirozeného čísla.

Pokud pro prvočíslo a platí $a \mid b^2$, pak i $a \mid b$. Toto tvrzení platí, protože v prvočíselném rozkladu čísla b^2 je prvočíslo a aspoň v druhé mocnině, takže je i v rozkladu čísla b. Pokud a není prvočíslo, tak tvrzení samozřejmě nemusí platit, př. $8 \mid 12^2 = 144$, ale $8 \nmid 12$.

Pokud mají čísla a, b stejný zbytek po dělení m, říkáme, že a je kongruentní s b modulo m. Zapisujeme $a \equiv b \pmod{m}$. Tedy př. $7 \equiv 1 \equiv -2 \pmod{3}$. Ekvivalenteně lze říci, že $m \mid (a-b)$,
tedy $a - b \equiv 0 \pmod{m}$.

Pokud $a \equiv 0 \pmod{m}$, pak $m \mid a$.

Pokud $a \equiv b \pmod{m}$ a zároveň $b \equiv c \pmod{m}$, potom $a \equiv c \pmod{m}$.

Pokud $a \equiv b \pmod{m}$, potom $a + km \equiv b \pmod{m}$, $k \in \mathbb{Z}$.

Pokud $a \equiv b \pmod{n}$ a $c \equiv d \pmod{m}$ a k je přirozené číslo, platí:

$$a \pm c \equiv b \pm d \pmod{m}$$

$$ka \equiv kb \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

$$a^k \equiv b^k \pmod{m}$$

Kromě těchto tvrzení nám často při řešení úlohy může pomoci nějaký vhodný rozklad na součin nebo rozlišení více případů (př. sudé/liché).
Pokud je zadání úlohy typu: *Najděte všechna čísla, která mají právě x dělitelů a zároveň platí*

..., tak se vyplatí využít výše uvedený vzorec pro počet dělitelů a poté si napsat prvočíselný rozklad čísla.
Docela často se můžeme setkat i s tzv. diofantickými rovnicemi, tedy rovnicemi, které máme řešit v oboru celých, popř. přirozených čísel. U těchto typů rovnic se často snažíme řešení omezit na nějakých pár hodnot nebo (většinou pomocí kongruencí) dokázat, že žádné řešení neexistuje. Uvedeme příklad takové rovnice.

Příklad: Nalezněte všechna celá čísla x taková, že $2^x(4-x) = 2x+4$, a ukažte, že žádná jiná už nejsou.
Řešení: Předpokládejme, že x je větší než tři. Pak je levá strana rovnice nekladná, zatímco pravá je kladná. Tedy rovnost nemůže nastat a takové řešení neexistuje. Podobně předpokládejme, že x je menší než minus jedna. Levá strana je kladná, ale pravá nekladná. Proto rovnost ani v tomto případě nemůže nastat. Zbývají jen hodnoty $-1, 0, 1, 2, 3$, které snadno dosadíme do zadání. Rovnici vyhovují $x = 0$, $x = 1$ a $x = 2$, což jsou všechna řešení úlohy.

Příklady

1. Dokažte, že pokud a, b, c jsou celá čísla, potom číslo $(a-b)(b-c)(c-a)(a+b+c)$ je dělitelné třemi. (MKS, 32. ročník, 1. jarní série, úloha 2)

2. Urči paritu[1] čísla, pro jehož nějaké 2 přirozené dělitele d_x, d_y platí: $d_x + d_y = 2017$.

3. Pro která prvočísla p je $p^2 + 2$ také prvočíslo?

4. Najdi všechna přirozená čísla, která mají právě 4 dělitele, přičemž součet největšího a druhého nejmenšího dělitele je 10090.

5. Trojice čísel 14, 20, n má následující vlastnost: Součin každých dvou z nich je dělitelný tím třetím. Najděte všechna kladná celá čísla n, pro něž je tato podmínka splněna. (NÁBOJ 2016, úloha 16)

6. Dokažte, že pro každé přirozené číslo a existuje přirozené číslo $n > 1$ takové, že $n \mid a^n + 1$. (MKS, 34. ročník, 3. podzimní série, úloha 3)

7. Ve čtverci 4×4 je v každém poli vepsáno číslo 1. V našem tahu vybereme nějaká 3 pole, tvořící jakkoliv orientované L. V každém z těchto polí pak zvýšíme číslo o 1. Můžeme takto dosáhnout stavu, kdy bude ve všech polích číslo 33?

8. Řešte v oboru celých čísel rovnici $7x^2 + 5y^2 + 14 = 0$.

9. Nechť a, b jsou nesoudělná kladná celá čísla a a b taková, že $\frac{a+b}{a-b}$ je také celé číslo. Dokažte, že $ab + 1$, nebo $4ab + 1$ je čtverec. (TRiKS, 2016)

[1] Sudé nebo liché

10. Rozhodněte, zda pro každých šest po sobě jdoucích čísel existuje prvočíslo, které dělí právě jedno (MKS, 36. ročník, 2. podzimní série, úloha 4) z těchto čísel.

11. Najděte všechny trojice celých čísel (a, b, c) takové, že každý ze zlomků

$$\frac{a}{b+c}, \frac{b}{c+a}, \frac{c}{a+b}$$

má celočíselnou hodnotu. (MO 66. ročník, krajské kolo kategorie A, úloha 1)

12. Nechť n je celé kladné číslo. Označme všechny jeho kladné dělitele $d_1, d_2, ..., d_k$ tak, aby platilo $d_1 < d_2 < ... < d_k$ (je tedy $d_1 = 1$ a $d_k = n$). Zjistěte všechny takové hodnoty n, pro něž platí $d_5 - d_3 = 50$ a $11d_5 + 8d_7 = 3n$.
(MO 63. ročník, ústřední kolo kategorie A, úloha 1)

Řešení příkladů

1. Dokažte, že pokud a, b, c jsou celá čísla, potom číslo $(a-b)(b-c)(c-a)(a+b+c)$ je dělitelné třemi.
Řešení: Pokud by nějaká dvě z čísel a,b,c dávala po dělení třemi stejný zbytek (BÚNO[2] a,b), tak $3 \mid a-b$, *takže celý výraz je dělitelný třemi. V opačném případě dávají každá 2 čísla z čísel* a, b, c *po dělení třemi jiný zbytek, tedy v nějakém pořadí zbytky 0,1,2. Platí tedy* $a+b+c \equiv 0+1+2 \equiv 0 \pmod 3$. *Výraz je tedy vždy dělitelný třemi.*

2. Urči paritu čísla, pro jehož nějaké 2 přirozené dělitele d_x, d_y platí: $d_x + d_y = 2017$
Řešení: Vzhledem k tomu, že součet dělitelů je liché číslo, a to lze zapsat jako součet 2 čísel jen jako součet lichého a sudého čísla, tak má hledané číslo aspoň jednoho sudého dělitele, takže je sudé.

3. Pro která prvočísla p je $p^2 + 2$ také prvočíslo?
Řešení: Každé prvočíslo dává po dělení třemi buď zbytek 1, nebo zbytek 2, nebo se jedná o prvočíslo 3. Ať $p \equiv 1 \pmod 3$ *nebo* $p \equiv 2 \pmod 3$, *tak v obou případech* $p^2 \equiv 1 \pmod 3$. *Tedy* $p^2 + 2$ *je dělitelné třemi a zároveň větší nebo rovno* $2^2 + 2 = 6$, *takže to není prvočíslo. Zbývá rozebrat případ, kdy* $p = 3$. *Tedy* $p^2 + 2 = 11$, *což je prvočíslo.*
Úloha má tedy jediné řešení $p = 3$.
Poznámka: Úloha by samozřejmě šla vyřešit i bez kongruencí, stačilo by postupně dosadit
$p = 3k + 1$ *a* $p = 3k + 2$, $k \in \mathbb{Z}$. *S kongruencemi se ovšem pracuje pohodlněji, protože se vyhneme roznásobování výrazů.*

4. Najdi všechna přirozená čísla, která mají právě 4 dělitele, přičemž součet největšího a druhého nejmenšího dělitele je 10090.

[2] Bez újmy na obecnosti

Řešení: Protože číslo 4 umíme rozložit na přirozená čísla jen dvěma způsoby a to $4 = 4 \cdot 1 = 2 \cdot 2$*, tak mohou taková čísla n být jen ve tvaru* $n = p^3$ *nebo* $n = pq$*, kde* $p, q, p < q$ *jsou prvočísla.*
Pokud $n = p^3$*, tak má podle zadání platit* $p + p^3 = 10090$*, tedy* $p(p^2 + 1) = 10090 = 2 \cdot 5 \cdot 1009$*. Uvážíme-li ještě, že* $p < (p^2 + 1)$*, tak musí být* $p = 2$ *nebo* $p = 5$*, ale ani jedna z možností zřejmě nevyhovuje.*
Pokud $n = pq$*, tak si můžeme podmínku ze zadání přepsat jako* $p + pq = p(q + 1) = 10090 =$
$= 2 \cdot 5 \cdot 1009$*. Vzhledem k tomu, že* $p < q$ *a* p, q *jsou prvočísla, tak buď* $p = 2$ *nebo* $p = 5$*.Pro* $p = 2$ *ale vyjde* $q = 5044$*, což není prvočíslo. Pro* $p = 5$ *vyjde* $q = 2017$*, což je prvočíslo.*
Tedy $n = 5 \cdot 2017 = 10085$.

5. Trojice čísel 14, 20, n má následující vlastnost: Součin každých dvou z nich je dělitelný tím třetím. Najděte všechna kladná celá čísla n, pro něž je tato podmínka splněna.
Řešení: Číslo n je dělitelem $14 \cdot 20 = 2^3 \cdot 5 \cdot 7$*, takže se v jeho rozkladu mohou vyskytnout jedině prvočísla 2, 5 a 7, přičemž dvojka bude nanejvýš ve třetí mocnině a pětka se sedmičkou nanejvýš v první mocnině. Podmínka* $14 \mid 20n \Rightarrow 7 \mid 10n$ *znamená, že je n násobkem 7 (*$NSD(7, 10) = 1$*). Podobně z předpokladu* $20 \mid 14n \Rightarrow 10 \mid 7n$ *získáváme* $10 \mid n$*. Dohromady platí* $70 \mid n$*. Je snadné ověřit, že všechna čísla, která připadají v úvahu, tj. 70, 140 a 280, zadání vyhovují.*

6. Dokažte, že pro každé přirozené číslo a existuje přirozené číslo $n > 1$ takové, že $n \mid a^n + 1$.
Řešení: Pokud je a liché, potom je a^2 *liché a* $a^2 + 1$ *je sudé, číslo* $n = 2$ *tedy vyhovuje podmínce v zadání. Pokud je a sudé, položíme* $n = a + 1$*. Potom platí:* $a^n = (n-1)^n \equiv (-1)^n = -1 \pmod{n}$*, neboť n je liché. Pokud si tuto kongruenci přepíšeme podle definice, dostaneme* $n \mid a^n + 1$*, což jsme přesně chtěli.*

7. Ve čtverci 4×4 je v každém poli vepsáno číslo 1. V našem tahu vybereme nějaká 3 pole, tvořící jakkoliv orientované L. V každém z těchto polí pak zvýšíme číslo o 1. Můžeme takto dosáhnout stavu, kdy bude ve všech polích číslo 33?
Řešení: Označíme S jako součet všech čísel v tabulce (tedy na začátku $S = 16$*). V každém našem tahu se zbytek S po dělení třemi nezmění. A protože na začátku* $S \equiv 1 \pmod 3$*, tak S nikdy nebude dělitelné třemi, tedy do takového stavu se nemůžeme dostat. (Pokud by všechna čísla v tabulce byla 33, tak* $S = 33 \cdot 16$ *a tedy zřejmě* $3 \mid S$*)*

8. Řešte v oboru celých čísel rovnici $7x^2 + 5y^2 + 14 = 0$.
Řešení: Rovnici rozepíšeme: $7x^2 + 5y^2 + 14 = 5(x^2 + y^2 + 2) + 2x^2 + 4 = 0$ *Levá strana rovnice dává po dělení pěti stejný zbytek jako* $2x^2 + 4$*, ale jelikož* x^2 *dává pouze zbytky* $0, 1$ *a* 4 *(to vyzkoušíme postupným dosazováním* $x \equiv 0, 1, .., 4 \pmod 5$*), tak levá strana rovnice není nikdy dělitelná pěti a zadaná rovnice proto nemá žádné řešení.*

9. Nechť a, b jsou nesoudělná kladná celá čísla a a b taková, že $\frac{a+b}{a-b}$ je také celé číslo. Dokažte, že $ab+1$, nebo $4ab+1$ je čtverec.

   Řešení: Označíme $m = \frac{a+b}{a-b}$, pak $a+b = ma - mb$, odsud $\frac{a}{b} = \frac{m+1}{m-1}$. Vzhledem k nesoudělnosti a a b existuje k takové, že $m+1 = ka$ a $m-1 = kb$. Vynásobením těchto rovností: $m^2 - 1 = k^2ab$, takže $m^2 = k^2ab + 1$. k je dělitelem $m+1$ a $m-1$, takže dělí i jejich rozdíl 2. k tedy musí být 1, nebo 2. Dosazením do předchozí rovnice nám vychází, že $ab+1$, nebo $4ab+1$ je skutečně čtverec.

10. Rozhodněte, zda pro každých šest po sobě jdoucích čísel existuje prvočíslo, které dělí právě jedno z těchto čísel.

    Řešení: Je zřejmé, že z každých šesti po sobě jdoucích čísel jsou právě tři lichá. Dále dokážeme sporem, že z těchto tří lichých čísel je maximálně jedno dělitelné třemi. Předpokládejme, že jsou dvě z nich dělitelná třemi. Pak je jejich rozdíl také dělitelný třemi a jelikož jsou obě lichá, tak jejich rozdíl je sudý. Tento rozdíl je tedy dělitelný šesti a jelikož jde o různá čísla, tak se musí lišit alespoň o šest. Pak ale nemohou být obě v šestici po sobě jdoucích čísel. Analogicky dokážeme, že maximálně jedno z těchto tří lichých čísel je dělitelné pěti. Maximálně dvě z nich jsou proto dělitelná třemi nebo pěti, tedy v každých šesti po sobě jdoucích číslech existuje číslo, které není dělitelné dvěma, třemi ani pěti. Toto číslo je buďto rovno jedné, nebo má ve svém prvočíselném rozkladu prvočíslo větší nebo rovno sedmi (pro všechna čísla větší než jedna existuje prvočíselný rozklad). Nejprve vyřešíme první případ. Číslo jedna je obsaženo jen v šestici čísel 1, 2, 3, 4, 5, 6. Pro tuto šestici je číslo pět prvočíslem, které dělí právě jedno z čísel v ní. Ve druhém případě toto prvočíslo nemůže dělit žádné další číslo ze šestice, jelikož rozdíl každých dvou jeho násobků je větší nebo roven sedmi. Tedy pro každých šest po sobě jdoucích čísel existuje prvočíslo, které dělí právě jedno z nich.

11. Najděte všechny trojice celých čísel (a, b, c) takové, že každý ze zlomků

$$\frac{a}{b+c}, \frac{b}{c+a}, \frac{c}{a+b}$$

    má celočíselnou hodnotu.

    Řešení: Uvažovaná trojice zlomků je symetrická v tom smyslu, že nahradíme-li trojici celých čísel (a, b, c) jejich libovolnou permutací, dostaneme zase (až na pořadí) tutéž trojici zlomků. Stejně tak, nahradíme-li čísla a, b, c čísly opačnými. Tato skutečnost nám usnadní následující rozbor případů.

    Předpokládejme tedy, že čísla a, b, c jsou taková, že všechny tři uvažované zlomky mají celočíselnou hodnotu. Pokud se mezi nimi nachází nula, stačí bez újmy na obecnosti vyšetřit případ $a = 0$. Po dosazení do uvažovaných zlomků dostáváme, že zlomky $\frac{b}{c}$ a $\frac{c}{b}$ mají celočíselnou hodnotu. Odtud plyne, že b i c jsou nenulová a je $|b| \geq |c|$ a zároveň $|c| \geq |b|$, proto $c = \pm b$. Navíc číslo $b + c$ je jmenovatelem prvního zlomku, proto $b + c \neq 0$, takže musí být $b = c$. Celkově tak dostáváme (zjevně vyhovující) trojice

$(0, c, c)$ *a jejich permutace pro každé nenulové celé číslo* c.
Zbývá vyřešit případ, kdy $abc \neq 0$. *Vzhledem k pozorování z prvního odstavce budeme předpokládat, že alespoň dvě z čísel* a, b, c *jsou kladná. Pokud by byla kladná všechna tři, bude zlomek, který má v čitateli nejmenší z čísel* a, b, c *ležet mezi 0 a 1, takže nemůže mít celočíselnou hodnotu. Nechť tedy* a, b *jsou kladná čísla a* $c = -d$ *pro kladné* d. *Po dosazení do zadání dostaneme, že zlomky*

$$\frac{a}{d-b}, \frac{b}{d-a}, \frac{d}{a+b}$$

mají celočíselnou hodnotu. Z posledního z nich je jasné, že $d \geq a + b$. *Proto má první zlomek kladný jmenovatel, a protože jeho hodnota je celé číslo, musí platit* $a \geq d - b$ *neboli* $d \leq a+b$. *Je tudíž* $d = a+b$ *neboli* $c = -a-b$ *a dostáváme tak v souhrnu trojice* (a, b, c) *nenulových čísel, pro které platí* $a+b+c = 0$. *Všechny takové trojice vyhovují, neboť hodnota všech tří uvažovaných zlomků je pro ně rovna* -1.
Úloze vyhovují všechny trojice $(0, c, c)$, $(c, 0, c)$ *a* $(c, c, 0)$, *kde* c *je nenulové celé číslo, a všechny trojice* (a, b, c) *nenulových celých čísel, pro něž platí* $a + b + c = 0$.

Jiné řešení: Případ, kdy $abc \neq 0$ *vyřešíme ještě jiným způsobem. Pokud jsou zlomky celá čísla, tak jistě platí, že absolutní hodnota jmenovatele je menší nebo rovna absolutní hodnotě čitatele. Získáme tedy soustavu tří rovnic:*

$$|b + c| \leq a$$
$$|c + a| \leq b$$
$$|a + b| \leq c$$

Každou rovnici umocníme na druhou (zřejmě platí $|b + c|^2 = (b + c)^2$*).*

$$(b + c)^2 \leq a^2$$
$$(c + a)^2 \leq b^2$$
$$(a + b)^2 \leq c^2$$

Po sečtení těchto rovnic a vykrácení členů nám vyjde:

$$a^2 + b^2 + c^2 + 2ab + 2ac + 2bc \leq 0$$

Tedy $(a+b+c)^2 \leq 0$, *takže dostáváme stejně jako v 1. řešení trojice (a,b,c) nenulových celých čísel, pro něž platí* $a + b + c = 0$.

12. Nechť n je celé kladné číslo. Označme všechny jeho kladné dělitele $d_1, d_2, ..., d_k$ tak, aby platilo $d_1 < d_2 < ... < d_k$ (je tedy $d_1 = 1$ a $d_k = \mathrm{n}$). Zjistěte všechny takové hodnoty

n, pro něž platí $d_5 - d_3 = 50$ a $11d_5 + 8d_7 = 3n$.

Řešení: Rozlišíme, zda hledané n je liché či sudé.

(i) Nechť n je liché, pak i všechna d_i jsou lichá. Z rovnosti $11d_5 + 8d_7 = 3n$ plyne $d_7 \mid 11d_5$ a také $d_5 \mid 8d_7$ neboli $d_5 \mid d_7$. Z $d_5 \mid d_7 \mid 11d_5$ s ohledem na $d_7 > d_5$ máme $d_7 = 11d_5$ a po dosazení do rovnosti $11d_5 + 8d_7 = 3n$ dostaneme $99d_5 = 3n$ neboli $33d_5 = n$. Vidíme, že čtyři čísla 1, 3, 11 a 33 jsou dělitelé čísla n, a to dokonce jediní dělitelé menší než 50, neboť pro pátý dělitel d_5 už podle zadání platí $d_5 = d_3 + 50 > 50$. Máme tedy $d_1 = 1, d_2 = 3, d_3 = 11, d_4 = 33, d_5 = d_3 + 50 = 61$, a proto $n = 33d_5 = 33 \cdot 61 = 2013$. Toto číslo skutečně vyhovuje, neboť jeho nejmenší dělitelé jsou v předchozí větě vypsáni správně, navíc platí $d_6 = 61 \cdot 3$ a $d_7 = 61 \cdot 11$, takže je skutečně splněno $d_7 = 11d_5$, tedy i vše požadované.

(ii) Nechť n je sudé. Z rovnosti $11d_5 + 8d_7 = 3n$ pak plyne $2 \mid d_5$, takže rovněž $2 \mid d_5 - 50 = d_3$. Protože $d_1 = 1$ a $d_2 = 2$, nemůže být $d_3 = 3$, takže je buď $d_3 = 4$, nebo $d_3 = 2t$, kde $t > 2$. Poslední však možné není (číslo $t < d_3$ by chybělo ve výpisu nejmenších dělitelů čísla n), a proto je nutně $d_3 = 4$. Pak je ovšem $d_5 = d_3 + 50 = 54$, a tedy $3 \mid n$, přestože 3 není mezi nejmenšími děliteli čísla n. Žádné vyhovující sudé n proto neexistuje.

Úloha má jediné řešení $n = 2013$.

2.2 Prvočísla a rozklad na součin

Prvočíslo je číslo, které má právě 2 kladné dělitele, a to jedničku a samo sebe. Číslo 1 za prvočíslo nepovažujeme. Jak zjistíme, jestli je číslo n prvočíslo? Můžeme zkoušet jeho dělitelnost všemi čísly od 2 do n, nebo chytřeji do $\sqrt{n}$.
Pomocí tzv. Erastosthenova síta můžeme generovat všechna prvočísla od 2 do n. Tento jednoduchý algoritmus funguje „prosíváním“ seznamu čísel – na počátku seznam obsahuje všechna čísla v daném rozsahu $2, 3, 4, \ldots, n$. Poté se opakovaně první číslo ze seznamu označí, toto číslo je prvočíslem. Ze seznamu se pak odstraní všechny násobky tohoto čísla (což jsou čísla složená). Tak se pokračuje do doby, než je označeno nebo ze seznamu odstraněno poslední číslo.
V mnoha úlohách s prvočísly využijeme rozklad na součin. K čemu nám to je? Můžeme využít toho, že dělitelé prvočísla p jsou jen 1 a p. Takže pokud rozložíme prvočíslo $p = xy$, tak buď $x = p, y = 1$, nebo $y = p$, $x = 1$ (Pokud mohou být x, y záporná čísla, tak přibydou ještě možnosti $x = -p$, $y = -1$, resp. $y = -p$, $x = -1$).
Uvedeme zde několik základních rozkladů mnohočlenů:

$$(a+b)^2 = a^2 + 2ab + b^2$$

$$(a-b)^2 = a^2 - 2ab + b^2$$

$$a^2 - b^2 = (a-b)(a+b)$$

$$a^3 - b^3 = (a-b)(a^2 + ab + b^2)$$

$$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$$

Bohužel často v úlohách nejsou pěkné rozklady podle vzorce, v tom případě je vhodné povytýkat nebo přičíst k oběma stranám vhodnou hodnotu a následně se pokusit výraz rozložit. Dobře je to vidět na následujícím příkladu.

Příklad: Najděte všechny dvojice prvočísel p, q takové, že $2p + 4q = pq - 1$.
Řešení: Postupně upravujeme rovnici:

$$\begin{aligned} 2p + 4q &= pq - 1 \\ 2p + 4q - pq &= -1 \\ pq - 2p - 4q &= 1 \\ pq - 2p - 4q + 8 &= 9 \\ p(q-2) - 4(q-2) &= 9 \\ (p-4)(q-2) &= 9 \end{aligned}$$

Činitel $q-2$ je nezáporný, protože q je prvočíslo. Nezáporný tedy musí být i činitel $p-4$. Jsou právě tři možnosti, jak číslo 9 rozložit na součin dvou nezáporných čísel: $9 = 1\cdot 9 = 3\cdot 3 = 9\cdot 1$.
Z nich získáme celkem tři řešení $(p, q) \in \{(5; 11), (7; 5), (13; 3)\}$.

Příklady

1. Řešte v oboru přirozených čísel rovnici $p + 400 = a^2$, kde p je prvočíslo

2. Najděte všechna přirozená čísla a, b pro která platí $ab = a + b$.

3. Jaký největší obsah může mít obdélník s obvodem 20 cm?

4. Nalezněte všechna prvočísla, která nelze zapsat jako součet dvou složených čísel.
(MKS, 36. ročník, 2. podzimní série, úloha 4)

5. Najdi všechna přirozená čísla x, pro která platí, že $x^2 + x$ je druhou mocninou přirozeného čísla.

6. n je součin dvou po sobě jdoucích přirozených čísel. Dokažte, že je možné doplnit za n dvě číslice tak, aby vzniklé číslo bylo čtvercem. (TRiKS, 2016)

7. Najděte všechny neuspořádané trojice prvočísel p, q, r takové, že $pqr = 101(p + q + r)$ nebo $p + q + r = 101pqr$. (TRiKS, 2017)

8. Najděte všechna celá čísla n, pro něž je $n^4 - 3n^2 + 9$ prvočíslo.
(MO 61. ročník, ústřední kolo kategorie A, úloha 1)

9. Najděte všechna prvočísla p, pro něž existuje přirozené číslo n takové, že $p^n + 1$ je třetí mocninou některého přirozeného čísla.
(MO 66. ročník, domácí kolo kategorie A, úloha 1)

10. Dokažte, že pro žádné přirozené číslo n není číslo $27^n - n^{27}$ prvočíslo.
(Slovenská MO, 57. ročník, ústřední kolo kategorie A, úloha 4)

Řešené příklady

1. Řešte v oboru přirozených čísel rovnici $p + 400 = a^2$, kde p je prvočíslo
Řešení: Rovnici upravíme do tvaru $p = (a - 20)(a + 20)$. *Protože* p *je prvočíslo, tak musí nutně platit* $a - 20 = 1$ *a také* $a + 20 = p$. *Z toho plyne* $a = 21$ *a* $p = 41$, *což je skutečně jediným řešením této rovnice.*

2. Najděte všechna přirozená čísla a, b pro která platí $ab = a + b$.
Řešení: Rovnici upravíme do tvaru: $ab - a - b + 1 = 1$, *tedy* $(a - 1)(b - 1) = 1$. *Číslo 1 můžeme napsat jako součin dvou přirozených čísel jen jako* $1 \cdot 1$, *tedy* $a = b = 2$.

3. Jaký největší obsah může mít obdélník s obvodem 20 cm?
Řešení: Strany obdélníku označíme a,b. Podle zadání $a + b = 10$. *Teď hledáme nejvyšší hodnotu výrazu* $ab = b(10-b) = -b^2+10b = -(b-5)^2+25$. *Pro* $b = 5$ *je* $-(b-5)^2 = 0$, *jinak* $-(b-5)^2 < 0$. *Největší možný obsah je tedy* $25\,cm^2$.

Jiné řešení: Označíme strany obdélníka $a = 5 + x, b = 5 - x$ $(a + b = 10)$. Takže $ab = (5 + x)(5 - x) = 25 - x^2$. Největší možný obsah je tedy $25\,cm^2$ (pro $x = 0$, tedy: $a = b = 5$).

4. Nalezněte všechna prvočísla, která nelze zapsat jako součet dvou složených čísel.
   Řešení: Nejprve si uvědomme, že všechna sudá čísla větší než dva jsou složená, a tudíž i všechna prvočísla větší než dva jsou lichá. Číslo dva zjevně nelze zapsat jako součet dvou složených čísel (nejmenší složené číslo je čtyři). Dále tedy všechna prvočísla, která nám zbývá vyřešit, jsou lichá. Jelikož liché číslo lze zapsat pouze jako součet sudého a lichého čísla, všechna prvočísla menší než součet nejmenšího sudého složeného čísla a nejmenšího lichého složeného čísla (tj. čtyři a devět) takto zapsat nelze. Ovšem každé prvočíslo $p \geq 13$ lze zapsat jako $p = 9 + (p - 9)$, kde devět je složené číslo a $p - 9$ je sudé číslo větší než dva, tudíž rovněž složené. Proto žádné takové prvočíslo nebude hledaným řešením. Řešeními jsou tedy právě ta prvočísla, která jsou menší než 13, tedy 2, 3, 5, 7 a 11.

5. Najdi všechna přirozená čísla x, pro která platí, že $x^2 + x$ je druhou mocninou přirozeného čísla.
   Řešení: Pro všechna přirozená čísla x platí $x^2 < x^2 + x < x^2 + 2x + 1 = (x + 1)^2$, tedy $x^2 + x$ je čtverec mezi x^2 a $(x + 1)^2$. Mezi čtverci dvou po sobě jdoucích čísel ale žádný jiný čtverec není, takže žádné takové x neexistuje.

6. n je součin dvou po sobě jdoucích přirozených čísel. Dokažte, že je možné doplnit za n dvě číslice tak, aby vzniklé číslo bylo čtvercem.
   Řešení: Za n napíšeme dvojčíslí 25, vznikne tak číslo $100n+25$. Pak platí: $n = k(k+1)$, tedy $100n + 25 = 100k(k + 1) + 25 = 100k^2 + 100k + 25 = (10k + 5)^2$.

7. Najděte všechny neuspořádané trojice prvočísel p, q, r, takové, že $pqr = 101(p+q+r)$, nebo $p + q + r = 101pqr$.
   Řešení: Nejprve BÚNO uvažujme, že r je největší, tak $p + q + r \leq 3r$, ale $pqr \geq 4r$, takže $pqr > p + r + q$, proto $pqr = 101(p + r + q)$. Číslo 101 je prvočíslo, proto BÚNO $r = 101$, pak $pq = p + q + 101$ a $(p - 1)(q - 1) = 102 = 1 \cdot 102 = 2 \cdot 51 = 3 \cdot 34 = 6 \cdot 17$, takže p a q jsou 2 a 103, proto $\{p, q, r\} = \{2, 101, 103\}$.

8. Najděte všechna celá čísla n, pro něž je $n^4 - 3n^2 + 9$ prvočíslo
   Řešení: Zadaný výraz lze jednoduchou úpravou rozložit na součin:

$$n^4 - 3n^2 + 9 = n^4 + 6n^2 + 9 - 9n^2 = (n^2 + 3)^2 - (3n)^2 = (n^2 + 3n + 3)(n^2 - 3n + 3)$$

   Aby součin dvou celých čísel byl prvočíslem p, musí být jeden z činitelů roven 1 nebo -1 (a druhý p, resp. $-p$). Diskriminanty obou kvadratických trojčlenů jsou však $(\pm 3)^2 - 4 \cdot 3 = -3$, tedy záporné, takže oba trojčleny nabývají jen kladné hodnoty. Vzhledem k

tomu stačí uvažovat jen kvadratické rovnice:

$$n^2 + 3n + 3 = 1 \quad a \quad n^2 - 3n + 3 = 1$$

Řešením první z nich jsou čísla $n = -1$ a $n = -2$, pro něž druhý činitel nabývá hodnot 7 a 13, což jsou prvočísla. Řešením druhé rovnice jsou $n = 1$ a $n = 2$, pro něž první činitel opět nabývá prvočíselných hodnot 7 a 13.
Zadaný výraz je prvočíslem, právě když $n \in \{-2, -1, 1, 2\}$.

9. Najděte všechna prvočísla p, pro něž existuje přirozené číslo n takové, že $p^n + 1$ je třetí mocninou některého přirozeného čísla.
Řešení: Předpokládejme, že pro přirozené číslo a platí $p^n + 1 = a^3$ (zjevně $a \geq 2$). Tuto rovnost upravíme tak, aby bylo možné jednu stranu rozložit na součin:

$$p^n = a^3 - 1 = (a - 1)(a^2 + a + 1)$$

Z tohoto rozkladu plyne, že pokud $a > 2$, jsou čísla $a - 1$ i $a^2 + a + 1$ mocninami prvočísla p (s kladnými celočíselnými exponenty).
V případě $a > 2$ tak platí $a - 1 = p^k$, neboli $a = p^k + 1$ pro kladné celé číslo k, což po dosazení do trojčlenu $a^2 + a + 1$ dává hodnotu $p^{2k} + 3p^k + 3$. Jelikož $a - 1 = p^k < a^2 + a + 1$, je určená hodnota trojčlenu $a^2 + a + 1$ vyšší mocninou prvočísla p, zaručeně proto platí: $p^k \mid p^{2k} + 3p^k + 3$, tedy $p^k \mid 3$. Odtud plyne, že musí být $p = 3$ a $k = 1$, a tedy $a = p^k + 1 = 4$. Číslo $a^2 + a + 1 = 21$ však není mocninou tří, a tak v případě $a > 2$ žádné prvočíslo p rovnici $p^n + 1 = a^3$ nevyhovuje, ať je exponent n zvolen jakkoli.
Pro $a = 2$ dostáváme rovnici $p^n = 7$, proto je $p = 7$ jediné vyhovující prvočíslo.

Jiné řešení: Druhý čitatel je zřejmě větší než první a oba čitatele jsou přirozená čísla. p^n má všechny přirozené dělitele tvaru p^k $(0 \leq k \leq n)$, $k \in N$. Tedy platí, že pokud 2. čitatel vydělíme prvním, dostaneme přirozené číslo (zřejmě $a \neq 1$)

$$\frac{a^2 + a + 1}{a - 1} = \frac{a^2 - 2a + 1 + 3a}{a - 1} = \frac{(a-1)^2 + 3a}{a - 1} = a - 1 + \frac{3(a-1) + 3}{a - 1} =$$

$$= a + 2 + \frac{3}{a - 1} \in \mathbb{N}$$

$\Rightarrow a - 1 \mid 3$, *tedy buď $a = 2$, nebo $a = 4$. Tyto případy rozebereme stejně jako v 1. řešení a dojdeme k jedinému výsledku $p = 7$.*

10. Dokažte, že pro žádné přirozené číslo n není číslo $27^n - n^{27}$ prvočíslo.
Řešení:

$$27^n - n^{27} = (3^n)^3 - \left(n^9\right)^3 = \left(3^n - n^9\right)\left(9^n + 3^n \cdot n^9 + n^{18}\right)$$

Teď úlohu dokážeme sporem, budeme tedy předpokládat, že takové číslo n existuje, a tedy $27^n - n^{27}$ je prvočíslo. V tom případě se musí 1. závorka rovnat 1, protože druhá závorka je zřejmě větší než jedna. Tedy: $3^n - n^9 = 1 \Rightarrow 3^n = n^9 + 1 = (n^3)^3 + 1 =$

$(n^3+1)\,(n^6-n^3+1)$.

První závorka je větší jen pokud $2n^3 > n^6$*, tedy po úpravě* $n^3 < 2$*, což platí jen pro* $n = 1$*, které ale zřejmě úloze nevyhovuje.*

V ostatních případech je druhá závorka větší, tedy můžeme říct že $\frac{n^6-n^3+1}{n^3+1} \in \mathbb{N}$*, protože obě závorky jsou mocniny prvočísla 3.*

$$\frac{n^6-n^3+1}{n^3+1} = \frac{(n^3+1)^2-3n^3}{n^3+1} = n^3+1-\frac{3(n^3+1)-3}{n^3+1} = n^3-2+\frac{3}{n^3+1} \in \mathbb{N}$$

Tedy buď $n^3+1=1$*, nebo* $n^3+1=3$*. To je ale spor, protože žádná z těcto rovnic nemá v oboru přirozených čísel řešení, a proto takové číslo* n *neexistuje.*

2.3 Cifry

V této sekci se budeme zabývat ciframi a jejich vlastnostmi. Nejdříve si připomeneme jednoduchá kritéria dělitelnosti, ta se zakládají na ciferném součtu, nebo na posledních několika cifrách daného čísla.

Číslo je dělitelné dvěma právě tehdy, když má na místě jednotek sudou číslici.

Číslo je dělitelné třemi právě tehdy, když je jeho ciferný součet dělitelný třemi.

Číslo je dělitelné čtyřmi právě tehdy, když je poslední dvojčíslí dělitelné čtyřmi.

Číslo je dělitelné pěti právě tehdy, když je jeho poslední číslice 0 nebo 5.

Číslo je dělitelné osmi právě tehdy, když je jeho poslední trojčíslí dělitelné osmi.

Číslo je dělitelné devíti právě tehdy, když je jeho ciferný součet dělitelný devíti.

Číslo je dělitelné deseti právě tehdy, když je jeho poslední číslice 0.

Číslo je dělitelné 10^n právě tehdy, když jeho n posledních číslic jsou nuly.

Číslo je dělitelné jedenácti právě tehdy, když je rozdíl součtu číslic na sudém a lichém místě dělitelný jedenácti, tedy př. $11 \mid 5357$, protože $11 \mid +5-3+5-7=0$.

Kritéria dělitelnosti můžeme skládat, pro $n = pq$, kde p, q jsou nesoudělná čísla je libovolné číslo dělitelné číslem n, pokud jsou zároveň splněná kritéria dělitelnosti čísly p, q.
Př. Číslo je dělitelné 24 právě tehdy, když je zároveň dělitelné osmi i třemi.

Každé číslo n můžeme zapsat v desítkové soustavě $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0$.
Tedy číslo $\overline{xyz}$ můžeme zapsat jako $100x + 10y + z$.
Ciferný součet čísla n budeme značit $S(n)$. Platí:

$S(n) = S(10^x n)$. Jen vynásobíme n mocninou deseti, takže $S(n)$ se nezmění.

$9 \mid n - S(n)$. Toto platí, protože $n - S(n) = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 - (a_k + a_{k-1} +$
$+ \ldots + a_1 + a_0) = 9(a_k \cdot 11\ldots1 + a_{k-1} \cdot 1\ldots1 + \ldots + a_2 \cdot 11 + a_1)$.

$s(m+n) \leq s(m) + s(n)$. Podívejme se, jak se sčítají čísla m a n pod sebou. Na každém řádu je buď součet příslušných cifer z m a n, nebo dojde k přenosu jedničky. Pak se číslo na tomto řádu sníží o 10 a číslo řádu o jedna vyššího se zvýší o jedna, ciferný součet se tedy celkově sníží o 9. Proto platí dokazovaná nerovnost.

Příklady

1. Jaký je ciferný součet čísla $25^{64} \cdot 32^{25}$?

2. Kolik existuje kladných celých čísel, jejichž první číslice (tj. ta nejvíce vlevo) se rovná počtu jejich cifer? (NÁBOJ 2016, úloha 6)

3. Když si Kuba hrál se svým oblíbeným přirozeným číslem, zjistil zajímavou věc. Nejenže dané číslo bylo palindrom[3] a dávalo po dělení čtyřmi zbytek 1 a po dělení dvaceti pěti zbytek 22, ale dokonce bylo nejmenším číslem, které všechny předchozí body splňuje. Které číslo to bylo? (MKS, 34. ročník, 3. podzimní série, úloha 1)

4. Najděte nejmenší nezáporné celočíselné řešení rovnice $n - 2 \cdot S(n) = 2016$.
(NÁBOJ 2016, úloha 5)

5. Najděte všechny čtyřciferné druhé mocniny přirozených čísel ve tvaru $\overline{xxyy}$, kde x a y jsou ne nutně různé číslice. (NÁBOJ 2017, úloha 27)

6. Mějme číslo n zapsané v desítkové soustavě, přičemž jeho cifry zprava doleva klesají. Určete ciferný součet čísla $9n$ (v desítkové soustavě). (TRiKS 2016)

7. Na tabuli je napsáno v desítkové soustavě celé kladné číslo N. Není-li jednomístné, smažeme jeho poslední číslici c a číslo m, které na tabuli zůstane, nahradíme číslem $|m - 3c|$. (Například bylo-li na tabuli číslo $N = 1204$, po úpravě tam bude $120 - 3 \cdot 4 = 108$.) Najděte všechna přirozená čísla N, z nichž opakováním popsané úpravy nakonec dostaneme číslo 0. (MO 62. ročník, ústřední kolo kategorie A, úloha 4)

Řešení příkladů

1. Jaký je ciferný součet čísla $25^{64} \cdot 32^{25}$?
Řešení: $25^{64} \cdot 32^{25} = 5^{128} \cdot 2^{125} = 5^3 \cdot 10^{125}$ *Číslo* $5^3 \cdot 10^{125}$ *je tvořeno číslicemi 1, 2, 5 a sto dvaceti pěti 0. Proto je jeho ciferný součet roven 8.*

2. Kolik existuje kladných celých čísel, jejichž první číslice (tj. ta nejvíce vlevo) se rovná počtu jejich cifer?
Řešení: Pro každou nenulovou číslici n *existuje právě* 10^{n-1} *čísel začínajících* n *splňujících podmínku zadání – jsou to čísla mezi* $\overline{n0\ldots0}$ *a* $\overline{n9\ldots9}$. *Dohromady je tedy hledaných čísel*

$$1 + 10 + \ldots + 100\,000\,000 = 111\,111\,111$$

3. Když si Kuba hrál se svým oblíbeným přirozeným číslem, zjistil zajímavou věc. Nejenže dané číslo bylo palindrom a dávalo po dělení čtyřmi zbytek 1 a po dělení dvaceti pěti zbytek 22, ale dokonce bylo nejmenším číslem, které všechny předchozí body splňuje.

[3] Číslo, které se čte stejně zepředu i zezadu, př. 1526251

Které číslo to bylo?

Řešení: Kubovo oblíbené přirozené číslo dávalo zbytek 22 po dělení dvaceti pěti, tudíž jeho poslední dvojčíslí bylo 22, 47, 72 nebo 97. Protože zbytek po dělení čtyřmi závisí pouze na posledním dvojčíslí, hledané číslo musí končit na 97, jenž jediné z uvedených dvojčíslí dává zbytek 1 po dělení čtyřmi. Proto Kubovo oblíbené číslo bylo nejmenší palindrom končící na 97, což je 797.

4. Najděte nejmenší nezáporné celočíselné řešení rovnice $n - 2 \cdot S(n) = 2016$.

   Řešení: Číslo $n - S(n)$ je vždy dělitelné devítkou. Protože je devítkou dělitelné i 2016, musí jí být dělitelné rovněž $S(n)$, a tedy také n. Zjevně $n < 3000$, takže $S(n) \leq 2 + 9 + 9 + 9$, z čehož vyplývá nerovnost $n = 2016 + 2S(n) \leq 2074$. Nyní už jen zbývá dosadit $S(n) = 9$ a najdeme nejmenší řešení, kterým je 2034.

5. Najděte všechny čtyřciferné druhé mocniny přirozených čísel ve tvaru $\overline{xxyy}$, kde x a y jsou ne nutně různé číslice.

   Řešení: Označme hledané čtyřciferné číslo N. Potom $N = 1000x + 100x + 10y + y = 1100x + 11y =$
   $= 11 \cdot (100x + y)$, takže N je dělitelné jedenácti. Vzhledem k tomu, že N je čtverec, musí být dělitelné dokonce 11^2 a můžeme ho zapsat ve tvaru $N = 11^2k^2$, kde k je nějaké přirozené číslo. Při tomto značení platí, že $100x + y = 11k^2$. Levá strana rovnosti je určitě větší nebo rovna 100 a menší než 1010, tedy $4 \leq k \leq 9$. Vyzkoušením těchto možností zjistíme, že vyhovuje jen $k = 8$, tedy $N = 11^2 \cdot 8^2 = 88^2 = 7744$.

6. Mějme číslo n zapsané v desítkové soustavě, přičemž jeho cifry zprava doleva klesají. Určete ciferný součet čísla $9n$ (v desítkové soustavě).

   Mějme tedy číslo n zapsané v desítkové soustavě jako $a_i \ldots a_1 a_0$, kde ze zadání $a_i < \ldots < a_1 < a_0$. Všimněme si, že $9n = 10n - n$. Dále si tedy představíme tato dvě čísla a písemně je odečteme. Díky podmínce na velikosti cifer navíc víme, že přes desítku budeme odečítat pouze v prvním kroku (při odečítání jednotek).
   Po odečtení tedy dostáváme číslo s ciframi $a_i, (a_{i-1} - a_i), \ldots, (a_1 - a_2), (a_0 - a_1 - 1), (10 - a_0)$.
   Součet všech těchto cifer je tedy roven $a_i + (a_{i-1} - a_i) + \ldots + (a_1 - a_2) + (a_0 - a_1 - 1) + (10 - a_0) = 9$.

7. Na tabuli je napsáno v desítkové soustavě celé kladné číslo N. Není-li jednomístné, smažeme jeho poslední číslici c a číslo m, které na tabuli zůstane, nahradíme číslem $|m - 3c|$. (Například bylo-li na tabuli číslo $N = 1204$, po úpravě tam bude $120 - 3 \cdot 4 = 108$.) Najděte všechna přirozená čísla N, z nichž opakováním popsané úpravy nakonec dostaneme číslo 0.

   Řešení: Nejdříve zjistíme, pro která čísla N dostaneme rovnou nulu. Zřejmě $|m - 3c| = 0$, právě když $m = 3c$ neboli $N = 10m + c = 31c$. Všechny násobky $N = 31c$ pro $c \in$

$\{1, 2, \ldots, 9\}$ *tudíž úloze vyhovují. Dokážeme, že úloze vyhovují právě všechny přirozené násobky čísla 31. Protože* $c = N - 10m$, *je* $m - 3c = 31m - 3N$, *takže popsaná operace zachovává dělitelnost číslem 31. Stačí tedy ukázat, že z libovolného násobku* $N = 31k$, *kde* $k \geq 10$, *dostaneme popsanou úpravou vždy menší násobek čísla 31. Pro takové* N *je ovšem* $m = 31$, $m - 3c > 0$, *tudíž* $|m - 3c| = 31m - 3N < 4N - 3N = N$. *Znamená to, že po konečném počtu kroků dostaneme popsanou úpravou některý z devíti nejmenších násobků čísla 31 a následně nulu. Tím je úloha vyřešena.*

3. RSA Algoritmus

RSA algoritmus je v současnosti jedním z nejpoužívanějších šifrovacích algoritmů. V roce 1977 jej navrhli Ron Rivest, Adi Shamir a Leonard Adelman. Je založen na myšlence asymetrického šífrování, používá tedy 2 od sebe různé klíče. Jeden z klíčů je používán výhradně k šifrování a nelze jej použít k dešifrování. Druhý klíč je využíván výlučně pro dešifrování a naopak jej nelze použít k šifrování. V praxi je pouze jeden z dvojice klíčů veřejně dostupný, druhý je utajen. Aby byla asymetrická kryptografie skutečně robustní, musí být zaručena praktická nemožnost výpočtu jednoho klíče z druhého.

Algoritmus je založen na teoreticky jednoduché myšlence: Je snadné vynásobit dvě dlouhá (minimálně 100-místná) prvočísla, ale bez jejich znalosti je prakticky nemožné zpětně provést rozklad výsledku na původní prvočísla. Součin těchto čísel je tedy součástí veřejného klíče. Přitom obě prvočísla potřebujeme pro dešifrování. Vzhledem k tomu, že dosud není znám rychlý algoritmus na na prvočíselný rozklad velkého čísla, je algoritmus RSA považován za bezpečný

3.1 Popis fungování

1. Zvolíme 2 dostatečně velká prvočísla p, q. V praxi se používají prvočísla o velikosti 1024 až 4096 bitů, někdy i delší.

2. Vypočteme součin $n = p \cdot q$.

3. Spočítáme hodnotu Eulerovy funkce: $\varphi(n) = (p-1)(q-1)$. Eulerova funkce se značí $\varphi(n)$ a udává počet všech přirozených čísel k takových, že $1 \leq k \leq n$ a $NSD(k,n) = 1$, tedy počet všech menších čísel nesoudělných s n. Tedy např. $\varphi(5) = |\{1,2,3,4\}| = 4$.

4. Zvolíme celé číslo e menší než $\varphi(n)$, které je s $\varphi(n)$ nesoudělné. Číslo e se nazývá veřejný (šifrovací) exponent.

5. Zvolíme číslo d takové, že $e \cdot d \equiv 1 \pmod{\varphi(n)}$. Číslo d je tzv. soukromý (dešifrovací) exponent.

Dvojici (n, e) zveřejníme jako náš veřejný klíč a dvojici (n, d) si ponecháme jako soukromý klíč. Čísla p, q a $\varphi(n)$ musí také zůstat tajná, jelikož mohou být použita k vypočítání dešifrovacího exponentu d.

Pokud chceme poslat zprávu M, tak ji musíme nejdříve převést na celé číslo m, pro které platí, že $0 \leq m < n$. To se provádí pomocí předem dohodnutého reverzibilního protokolu.

Poté zašifrujeme zprávu pomocí rovnice $c \equiv m^e \pmod{n}$ a odešleme ji[1]. Příjemce získá zašifrovanou zprávu c. Tu poté odšifruje pomocí rovnice $m \equiv c^d \pmod{n}$. Nikdo kromě něj není schopen zprávu efektivně dešifrovat, protože hodnotu d zná jen příjemce.

Důkaz správnosti

Příjemce získá zašifrovaný text c. Původní zprávu m získá pomocí rovnice $m \equiv c^d \pmod{n}$. Nyní dokážeme, že takto opravdu získá původní zprávu.

$$c^d \equiv (m^e)^d \equiv m^{ed} \pmod{n}$$

Jelikož podle definice d platí $ed - 1 \equiv 0 \pmod{(p-1)(q-1)}$, tak $p-1$ i $q-1$ dělí $ed-1$. Tedy $ed - 1 = h(p-1) = k(q-1)$ pro nějaká celá čísla h, k.
Pokud jsou m, p nesoudělná, tak podle Malé Fermatovy věty[2]

$$m^{ed} = m^{ed-1}m = m^{h(p-1)}m = \left(m^{p-1}\right)^h m \equiv 1^h m \equiv m \pmod{p}$$

Naopak pokud jsou m, p soudělná, pak $p \mid m$, tedy $p \mid m^{ed}$. Z toho vyplývá, že $m^{ed} \equiv 0 \equiv m \pmod{p}$
Tedy $m^{ed} \equiv m \pmod{p}$. Podobně ukážeme, že $m^{ed} \equiv m \pmod{q}$.
Protože p, q jsou 2 různá prvočísla a $pq = n$, tak pomocí čínské věty o zbytcích:
$m^{ed} \equiv m \pmod{n}$, tedy $c^d \equiv m \pmod{n}$

3.2 Příklad

Uvedu příklad komunikace mezi Alicí a Bobem.
Alice si vytvoří soukromý a veřejný klíč, aby ho mohla využít pro zabezpečení komunikace. Nejdříve si musí zvolit dvě libovolná prvočísla p, q, tedy například $p = 101, q = 113$. Pak spočítá jejich součin $n = p \cdot q = 101 \cdot 113 = 11413$ a hodnotu Eulerovy funkce $\varphi(n) = (101-1)(113-1) = 11200$. Aby mohla určit veřejný exponent, musí zvolit takové číslo e pro které platí, že $1 < e < 11200$ a zároveň je s číslem 11200 nesoudělné. Alice si vybrala např. $e = 3533$. Nakonec musí Alice vypočítat d ze vztahu $3533 \cdot d \equiv 1 \pmod{11200}$, tedy $d = 6597$. Tuto hodnotu můžeme spočítat pomocí rozšířeného Euklidova algoritmu. Nyní může Alice veřejný klíč, tedy dvojici $(n = 11413, e = 3533)$ zveřejnit.

Nyní chce Bob Alici poslat zprávu $m = 9726$, musí tedy vypočítat $c \equiv m^e \pmod{n}$, tedy $c \equiv 8723^{3533} \pmod{11431} = 5761$. Zašifrovanou zprávu $c = 5761$ pošle Alici, která ji dešifruje pomocí svého soukromého klíče výpočtem $m \equiv c^d \pmod{n}$, tedy $m \equiv 5761^{6597} \pmod{11413} = 9723$.

[1] Jako d, e označujeme v tomto případě exponenty příjemce

[2] Malá Fermatova věta tvrdí, že pro každé prvočíslo p a každé celé číslo a takové, že $NSD(a, p) = 1$, platí $a^{p-1} \equiv 1 \pmod{p}$

Tento příklad by v praxi nebyl bezpečný, protože použitá prvočísla jsou příliš malá.

4. Závěr

Literatura

[1] Birge J. R., Wets R. J.-B. (1987): Computing bounds for stochastic programing problems by means of a generalized moment problem. *Mathematics of Operations Research*

[2] Lenka Slavíková *Teorie čísel.* Dostupné z: http://mks.mff.cuni.cz/library/TeorieCiselLS/TeorieCiselLS.pdf, 2009

[3] Vilém Vychodil: *Algoritmus RSA.* Dostupné z: http://vychodil.inf.upol.cz/publications/white-papers/rsa.pdf

[4] Matúš Drobuliak: *RSA šifra.* Dostupné z: http://www.karlin.mff.cuni.cz/ tuma/Aplikace15/Prace15/Drobuliak_RSA.pdf

[5] Stanislav Froula: *RSA algoritmus a jeho využití v elektronické komunikaci s orgány státní správy* . Dostupné z: https://theses.cz/id/tmrhys/BP-FROULA.pdf

[6] Matematický korespondenční seminář: *Archiv úloh z MKS.* Dostupné z: http://mks.mff.cuni.cz/archive/archive.php

[7] Mezinárodní korespondenční seminář: *Archiv úloh TRiKS.* Dostupné z: http://iksko.org/triks/past.php

[8] Matematický NÁBOJ: *Archiv úloh.* Dostupné z: https://math.naboj.org/archive.php

[9] Matematická olympiáda: *Archiv úloh z MO.* Dostupné z: http://www.matematickaolympiada.cz/cs/olympiada-pro-stredni-skoly

[10] Slovenská matematická olympiáda: *Archiv úloh.* Dostupné z: https://skmo.sk/dokumenty.php