# Úlohy o veľkých číslach

ŠKOLA MLADÝCH MATEMATIKŮ

# ÚLOHY O VEĽKÝCH ČÍSLACH

61

Vydal ÚV matematické olympiády v nakladatelství Mladá fronta

ŠKOLA MLADÝCH MATEMATIKŮ

IVAN KOREC

# Úlohy o veľkých číslach

PRAHA 1988
VYDAL ÚV MATEMATICKÉ OLYMPIÁDY
V NAKLADATELSTVÍ MLADÁ FRONTA

*Recenzovali RNDr. Tamara Marcisová, CSc., a RNDr. Jan Nekovář*

# 1. ÚVOD

V tejto knižke nájdete úlohy s konkrétnymi číslami. Keby tieto čísla neboli príliš veľké na to, aby sa s nimi dali priamo vykonávať aritmetické operácie, boli by mnohé z predložených úloh celkom triviálne. Takto sú však obťažnejšie, a na ich riešenie je potrebné použiť obraty obvyklé pri dokazovaní matematických viet alebo pri riešení dôkazových úloh. Medzi týmito dvoma činnosťami vlastne neexistuje presná hranica. V dôkazových úlohách však často možno z uvádzaných predpokladov usudzovať na postup, ktorý pravdepodobne privedie k cieľu. V tu predkladaných úlohách to bude niekedy obťažnejšie, pretože konkrétnu vlastnosť udaných čísel, ktorá je pri riešení potrebná, bude treba vybrať z mnohých vlastností týchto čísel, a formulácia úlohy vôbec nemusí na túto vlastnosť upozorňovať. Je celkom možné, že pri zdanlivo malej zmene číselných parametrov úlohy sa z relatívne ľahkej úlohy stane úloha prakticky neriešiteľná. Z tohto hľadiska sú tu obzvlášť nebezpečné tlačové chyby, ktorých možnosť sa nedá celkom vylúčiť. Aj predkladané úlohy sú veľmi rôznej náročnosti, od riešiteľných spamäti až po vyžadujúce umelé obraty, ktoré treba najprv nájsť. Autor ešte poznamenáva, že jeho zámerom bolo rozšíriť sortiment úloh z teórie čísel o ďalšie druhy, teda nie nahradiť svojimi úlohami doterajšie typy úloh.

Takmer všetky úlohy v tejto knihe sú vyriešené. Odporúčam však čitateľovi, aby sa vždy najprv pokúsil o samostatné riešenie úlohy, alebo aspoň dodatočne porozmýšľal nad postupom, ktorým by úlohu sám riešil. Tak mu kniha podstatne viac pomôže prineskoršom riešení iných úloh.

## 2. PREDPOKLADANÉ PROSTRIEDKY A METÓDY

Predpokladáme, že čitateľ má k dispozícii bežné matematické tabuľky, a prípadne kalkulačku. Nepredpokladáme však samočinný počítač alebo programovateľnú kalkulačku; k možnosti ich použitia sa vrátime ešte v tejto kapitole, pri analýze pojmu veľkého čísla. Ďalej predpokladáme dobré matematické znalosti na úrovni strednej školy, a o niečo hlbšie znalosti z teórie čísel. Tieto doplňujúce znalosti možno získať napríklad z [2], [3], [10], [13], ale sú zhrnuté aj v nasledujúcej kapitole tejto knižky.

Riešenie úlohy má byť podľa možnosti krátke, elegantné a elementárne. Tieto požiadavky si aspoň čiastočne vzájomne odporujú, a preto nie vždy možno určiť, ktoré z dvoch riešení je lepšie. (Stále máme na mysli len správne riešenia!) Ani krátkosť riešenia nie je celkom jednoduchý pojem. Napríklad jedno riešenie môže byť kratšie než iné jednoducho preto, že sa pri úpravách robí vždy viac krokov naraz, alebo preto, že sa niektorá časť prehlási za triviálnu, a jej dôkaz sa vynechá. To nemusí byť chybou, ale pri hodnotení krátkosti riešenia by sme mali brať do úvahy celú dĺžku myšlienkovej cesty, ktorou sa dospeje k žiadanému výsledku, a nie dĺžku jej zápisu. Aby sme teda dĺžku riešenia hodnotili celkom objektívne, musel by byť presne stanovený požadovaný stupeň podrobnosti zápisu. Nie je to síce principiálne nemožné, ale my sa tým rozhodne nebudeme zaoberať. Ťažkosti pri hodnotení elegantnosti riešenia by boli ešte väčšie, jednak preto, že ide o čiastočne subjektívny pojem, a za druhé preto, že niekedy sa namiesto pôvodnej úlohy rieši všeobecnejšia úloha. Aj elementárnosť riešenia je zložitý (a dokonca niekedy viacvýznamový) pojem, tu však máme pre riešiteľa aspoň takéto odporúčanie: Dávajte v riešeniach úloh prednosť takým vetám a postupom, ktoré sa bežne používajú pri riešení úloh MO. Neobmedzujte sa však násilne na tieto postupy, ak už viete viac, ale nepoužívajte silnejšie metódy a výsledky iba preto, aby ste ukázali, že ich ovládate.

Pokiaľ používate pri riešení matematické tabuľky, tak im „bezvýhradne dôverujte". Tlačové chyby sa síce v tabuľkách môžu vyskytnúť, sú však málo pravdepodobné; pravdepodobnosť chyby vo Vašom výpočte je asi väčšia. Nečítajte však z tabuliek viac, než sa v nich tvrdí. Ak napríklad v štvormiestnych logaritmických tabuľkách vyčítate $\log 2 = 0{,}3010$, tak to znamená len

$$0{,}30095 \leqq \log 2 \leqq 0{,}30105 .$$

Pravda, namiesto neostrých nerovností možno písať ostré, ale to už nevieme z tabuliek, ale z toho, že log 2 je iracionálne číslo. Pomocou štvormiestnych tabuliek však možno log 2 určiť aj presnejšie. Napríklad ak z tabuliek vyčítame

$$\log 2^9 = \log 512 = 2{,}7093, \text{ tak vieme, že}$$

$$2{,}70925 \leqq 9 \log 2 \leqq 2{,}70935 ,$$

a odtiaľ zistíme

$$0{,}301027 \leqq \log 2 \leqq 0{,}301039 .$$

(Všimnite si, že výsledok delenia deviatimi vľavo sme museli zaokrúhliť nadol, a výsledok delenia vpravo nahor, bez ohľadu na ďalšie číslice podielu. Inokedy už na to nebudeme zvlášť upozorňovať.)

Obdobne z $\log 2^8 = \log 256 = 2{,}4082$ vieme

$$2{,}40815 \leqq 8 \log 2 \leqq 2{,}40825$$

$$0{,}301018 \leqq \log 2 \leqq 0{,}301032 .$$

Spolu teda máme

$$0{,}301027 \leqq \log 2 \leqq 0{,}301032 ,$$

čo je presnejší výsledok, než dá bezprostredné použitie päťmiestnych logaritmických tabuliek. Samozrejme, údaje z päťmiestnych tabuliek by sme mohli spresňovať obdobne. Všeobecne však tento postup je len východiskom z núdze; ak máme k dispozícii presnejšie tabuľky, tak sa radšej pozrieme do nich. Pre hľadanie logaritmov prirodzených čísel do 200 je napríklad vhodná tabuľka logaritmov faktoriálov v [1] (ale hodnota log 200! je chybná).

Stupeň oprávnenej dôvery kalkulačke alebo počítaču predstavuje už zložitejší problém. (Nemáme pritom na mysli možnosť, že kalkulačka je pokazená, obdobne ako sme neuvažovali možnosť tlačovej chyby v matematických tabuľkách.) Tu už záleží na type kalkulačky, či počíta na viac miest než nakoniec ukáže na displeji alebo nie. V druhom prípade je aspoň posledné miesto výsledku nespoľahlivé, často je však nespoľahlivé aj v prvom prípade. Záleží aj na zložitosti počítaného výrazu. Napríklad súčin dvoch celých čísel bude spravidla presný, pokiaľ sa dá celý zobraziť na displeji. Výsledok umocňovania (aj v prípade, že základ i exponent sú prirodzené čísla, a presný výsledok by sa dal celý zobraziť) však už môže byť nepresný, pretože kalkulačka ho môže počítať cez logaritmus a exponenciálnu funkciu. Tu je ťažké dať konkrétnu a všeobecne platnú radu. Zistite si presnosť Vašej kalkulačky aspoň pomocou niekoľkých kontrolných príkladov, a potom ju využívajte ešte s istou rezervou voči tato zistenej presnosti. Na túto rezervu bude treba myslieť napríklad pri odčítavaní alebo porovnávaní dvoch skoro rovnakých čísel.

Vrátime sa teraz k pojmu veľkých čísel, o ktorých sme už hovorili v úvode ako o číslach príliš veľkých na to, aby sme s nimi bezprostredne vykonávali aritmetické operácie. Zrejme nejde o presne matematicky definovaný pojem. Dôležitejšie však je, že tento pojem závisí aj od metód a prostriedkov, ktoré máme k dispozícii (a aj od námahy, ktorú sme ochotní pri počítaní podstúpiť). Napríklad pre počítanie spamäti sú už trojciferné čísla veľké, ale pre počítanie na papieri alebo s kalkulačkou ich asi za veľké nebudeme pokladať. Na samočinných počítačoch (a to i na osobných, alebo i na výkonnejších programovateľných kalkulačkách) si možno naprogramovať viacnásobnú aritmetiku, a potom ani stociferné čísla nebudú pre nás príliš veľké. Úlohu o posledných čísliciach čísla $2^{300}$ bude potom najjednoduchšie riešiť tak, že dáme stroju vypočítať číslo $2^{300}$, a potrebný počet posledných číslic si pozrieme. Bude to správny postup, ale rozhodne nebude v intenciách autora tejto knižky; keby autor predpokladal, že čitatelia budú mať k dispozícii samočinné počítače, tak by zväčšil čísla v úlohách tak, aby sa obdobný spôsob nedal použiť.

V niektorých úlohách, napríklad s viacposchodovými mocninami, sú už zvolené čísla také veľké, že ich prakticky vôbec nie je možné obvyklým spôsobom dekadicky zapísať. Ak však abstrahujeme od praktických ohraničení (najmä časových a priestorových), ako je to v matematike bežné, možno hovoriť o ich dekadických zápisoch, a určovať niektoré ich cifry. Dekadické zápisy reálnych čísel (aspoň niektorých) sú nekonečné, a teda ich vlastne nemožno celé napísať ani v princípe. Napriek tomu však možno hovoriť napríklad o ich čísliciach, a (niekedy) niektoré z týchto číslic aj vypočítať. Úlohy o takýchto čísliciach by sme mohli ľahko preformulovať tak, aby sa v nich o nekonečných dekadických rozvojoch nehovorilo, nové formulácie by však boli menej názorné.

V niektorých riešeniach najprv „uhádneme“ výsledok, a potom dokážeme jeho správnosť. Niekedy „uhádneme“ vhodné prvočíslo a podobne. Samozrejme, že aj schopnosť „uhádnuť“, či aspoň odhadnúť výsledok, je výhodná pri riešení úlohy, spôsob „uhádnutia“ však nie je logicky nevyhnutnou časťou napísaného riešenia úlohy. Namiesto „uhádnutia“ môže v skutočnosti ísť o použitie počítača. Ak je napríklad potrebné uvážiť prvočíslo $p = 5501$, ťažko môže ísť o „uhádnutie“ alebo o ručné preskúšanie. K prvočíslu $p = 19$ by sme však takto dospieť mohli. Za riešením úlohy občas uvádzame ešte komentár, ktorý už nie je jeho súčasťou; môže napríklad obsahovať vysvetlenie k nejakému „uhádnutiu“, ale môže sa vzťahovať i k nasledujúcej úlohe. Koniec vlastného riešenia úlohy vyznačujeme značkou $\square$.

# 3. PREHĽAD VIET Z TEÓRIE ČÍSEL

## 1. ZÁKLADNÉ OZNAČENIA A ČÍSELNÉ SÚSTAVY

Množinu všetkých celých nezáporných čísel budeme označovať $\mathsf{N}$ a množinu všetkých celých kladných čísel budeme označovať $\mathsf{P}$. Pod *prirodzenými číslami* budeme (na rozdiel od klasickej terminológie) rozumieť celé nezáporné čísla, t. j. aj 0 bude prirodzené číslo. Množinu všetkých celých, resp. reálnych čísel budeme označovať $\mathsf{Z}$, resp. $\mathsf{R}$. Pokiaľ nebude hroziť nedorozumenie, budeme miesto „prirodzené číslo" alebo „celé číslo" písať len „číslo".

Kladieme $a^0 = 1$ aj pre $a = 0$. Prirodzený logaritmus označujeme ln, dekadický značíme log, ostatné základy vyznačujeme. Dolnú (teda obvyklú) celú časť čísla $x$ značíme $\lfloor x \rfloor$, hornú celú časť čísla $x$ značíme $\lceil x \rceil$, teda platí $\lceil x \rceil = -\lfloor -x \rfloor$. Pre $x \in \mathsf{R}$, $n \in \mathsf{P}$ platí

$$\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor, \quad \left\lceil \frac{x}{n} \right\rceil = \left\lceil \frac{\lceil x \rceil}{n} \right\rceil .$$

V tejto kapitole jednak zavedieme označenia, ktoré budeme používať v ďalšom, a za druhé zhrnieme niektoré známe fakty z elementárnej teórie čísel aj iných častí matematiky, ktoré môžu byť užitočné pri riešení úloh v nasledujúcich kapitolách. Zhrnutej látky je viac, než sa v ďalších kapitolách bezprostredne využíva. Je totiž možné, že pri iných postupoch riešenia úloh sa budú hodiť iné matematické vety než pri autorských riešeniach. Keby sa autor striktne obmedzil na vety fakticky ďalej použité, mohol by veľmi sťažiť situáciu tým riešiteľom, ktorí sa budú pokúšať o samostatné riešenie úloh. Čitateľ samozrejme nemusí pri riešení úloh používať výlučne iba prostriedky z tejto kapitoly. Podaný prehľad výsledkov má mu slúžiť iba ako pomôcka. Rozhodne nie je ani potrebné, aby čitateľ najprv podrobne preštudoval túto kapitolu a až potom začal riešiť úlohy. Doporučujeme mu však, aby si ju celú dopredu prezrel, aby neskôr vedel, čo a asi kde v nej môže nájsť.

Táto kapitola je iba prehľad, a nie učebnica. Vety sú vyslovované bez dôkazov, a väčšinou aj bez odkazov, najmä pokiaľ ide o látku bežne preberanú v elementárnych učebniciach teórie čísel. Ak čitateľ ešte nie je oboznámený s kongruenciami a ich použitím, doporučujeme mu, aby si zvlášť všimol piaty (a prípadne šiesty) odsek tejto kapitoly a potom kapitoly 5, 6. Aparát kongruencií mu bude užitočný nielen pri riešení úloh tejto zbierky, ale aj pri úlohách MO.

Znaky $\Sigma$, $\Pi$ používame pre opakovaný súčet, resp. súčin. Pritom pre $n = 0$ kladieme

$$\sum_{i=1}^{n} a_i = 0, \qquad \prod_{i=1}^{n} a_i = 1;$$

túto dohodu analogicky používame aj pri zápisoch

$$a_1 + a_2 + \ldots + a_n, \quad a_1 . a_2 . \ldots . a_n .$$

Znaky $\sum\limits_{p \leq K}$, $\prod\limits_{p \leq K}$ znamenajú súčet, resp. súčin cez všetky prvočísla nepresahujúce $K$.

Znak $\pm$ budeme používať vo dvoch rôznych významoch, ktoré treba rozlišovať podľa kontextu. $x_{1,2} = 2 \pm 1$ znamená $x_1 = 3$, $x_2 = 1$. Naproti tomu $x = 2 \pm 0{,}05$ znamená $1{,}95 \leq x \leq 2{,}05$.

Dekadické zápisy celých nezáporných čísel, ktoré obvykle používame, vyjadrujú číslo ako súčet násobkov mocnín čísla 10 (s koeficientmi 0 až 9). Napríklad

$$1987 = 1.10^3 + 9.10^2 + 8.10^1 + 7.10^0;$$

rádom nejakej číslice (presnejšie: rádom jej výskytu) v zápise nejakého čísla budeme nazývať príslušný exponent čísla 10.

S výnimkou dekadického zápisu čísla nula obvykle požadujeme, aby číslica najvyššieho rádu bola nenulová. Niekedy však niekoľko núl vpredu dopisujeme (alebo si ich aspoň predstavujeme dopísané); robíme to tak napríklad vtedy, keď chceme mať dekadické zápisy čísel až po istú hranicu rovnako dlhé.

Namiesto čísla 10 možno použiť ľubovoľné celé číslo $z > 1$ a každé $u \in \mathsf{P}$ vyjadriť v tvare

$$u = a_n.z^n + a_{n-1}.z^{n-1} + \ldots + a_1.z^1 + a_0.z^0,$$

pričom $0 \leqq a_i < z$ pre všetky $i = 0, \ldots, n$; ak ešte žiadame $a_n \neq 0$, je toto vyjadrenie jednoznačné. Ak by sme mali k dispozícii číslice pre čísla $0, 1, \ldots, z -$ $- 1$, mohli by sme písať $z$-adické zápisy čísel obdobne ako dekadické. Aj základné počtové výkony by sa robili v podstate rovnako. (Pravda, „malá násobilka" by bola iná.) Teoreticky a abstraktne však môžeme takéto zápisy uvažovať, aj keď sa na čísliciach konkrétne nedohodneme. Prakticky sa pre $z < 10$ obvykle používajú príslušné dekadické číslice, pre $z = 16$ sa pridávajú ako ďalšie číslice písmená A až F (základ 16 sa niekedy používa pri samočinných počítačoch). My budeme takmer výlučne pracovať s dekadickými zápismi čísel. Iný základ vždy výslovne uvedieme.

Podotknime ešte, že $z$-adické rozvoje reálnych čísel sú obdobným zovšeobecnením ich dekadických rozvojov, aké sme urobili vyššie pre zápisy prirodzených čísel.

Pre niektoré reálne čísla sú tieto (ako už aj dekadické) rozvoje nekonečné, nemožno ich teda celé napísať. Aj vtedy však možno hovoriť o ich jednotlivých čísliciach, a prípadne počítať konečné úseky týchto rozvojov.

V textoch úloh zásadne hovoríme o čísliciach čísla $x$ namiesto presnejšieho, no zdĺhavejšieho vyjadrovania sa o čísliciach dekadického zápisu (resp. rozvoja) čísla $x$.

## 2. DELITEĽNOSŤ A PRAVIDLÁ DELITEĽNOSTI

Pre každé dve celé čísla $a$, $b$ píšeme $a|b$ (a čítame „$a$ *delí* $b$“, „$b$ *je násobkom* $a$“ a pod.), ak existuje celé číslo $c$ také, že $a \cdot c = b$. Budeme pisať $a \nmid b$, ak neplatí $a|b$.

**Veta 2.1.** *Relácia deliteľnosti na* $\mathsf{Z}$ *je reflexívna a tranzitívna, t. j. pre každé* $a \in \mathsf{Z}$ *platí* $a|a$ *a pre všetky* $a$, $b$, $c \in \mathsf{Z}$ *platí ak* $a|b$, $b|c$, *tak aj* $a|c$. *Ďalej, pre všetky* $a$, $b$, $c$, $x$, $y \in \mathsf{Z}$ *platí*

(i) *ak* $a|b$, $a|c$, *tak aj* $a|bx + cy$;
(ii) *ak* $a|b$, *tak* $ax|bx$;
(iii) $1|a$, $a|-a$, $a|0$.

Pre teóriu deliteľnosti celých čísel je veľmi dôležitá nasledujúca

**Veta 2.2.** (Veta o delení so zvyškom.) *Pre každé* $a \in \mathsf{Z}$, $b \in \mathsf{P}$ *existujú* $q$, $r \in \mathsf{Z}$ *také, že*

$$a = b \cdot q + r \quad \text{a} \quad 0 \leqq r < b.$$

*Pritom čísla* $q$, $r$ *sú číslami* $a$, $b$ *jednoznačne určené.*

Čísla $q$, $r$ z tejto vety nazývame *celočíselným podielom* *a zvyškom pri (celočíselnom) delení* čísla $a$ číslom $b$. Budeme pre ne používať označenie

$$q = a \operatorname{DIV} b, \qquad r = a \operatorname{MOD} b,$$

(ktoré v podstate preberáme z programovacieho jazyka PASCAL). Symboly DIV a MOD sú symboly čiastočných operácií na množine $\mathsf{Z}$, a budeme ich písať medzi ich argumenty, obdobne ako $+$, $-$, . . Výraz $a.b \operatorname{MOD} m$ budeme vždy rozumieť ako $(a.b) \operatorname{MOD} m$; vo výraze $a.(b \operatorname{MOD} m)$ teda nesmieme vynechať zátvorku. Naproti tomu, $a + b \operatorname{MOD} m$ znamená $a + (b \operatorname{MOD} m)$. Obdobná dohoda platí pre DIV. (Teda, ako obvykle, multiplikatívne operátory majú vyššiu prioritu ako aditívne, a operátory s rovnakou prioritou sa aplikujú zľava doprava.)

**Veta 2.3.** *Pre všetky $a, b \in \mathsf{Z}$, $m, n \in \mathsf{P}$ platí*

$$(a + b) \operatorname{MOD} m = ((a \operatorname{MOD} m) + (b \operatorname{MOD} m)) \operatorname{MOD} m$$
$$(a.b) \operatorname{MOD} m = (a \operatorname{MOD} m).(b \operatorname{MOD} m) \operatorname{MOD} m$$
$$(a.n) \operatorname{MOD} (m.n) = (a \operatorname{MOD} m).n$$
$$(a \operatorname{MOD} (m.n)) \operatorname{MOD} m = a \operatorname{MOD} m$$

*Spoločným deliteľom* čísel $a$, $b$ nazveme každé číslo $d$ také, že $d|a$, $d|b$. *Najväčším spoločným deliteľom* čísel $a$, $b$ nazveme každý taký ich spoločný deliteľ, ktorý je násobkom každého ich spoločného deliteľa. Najväčšie spoločné delitele čísel $a$, $b$ sa môžu líšiť len znamienkom. Nezáporný najväčší spoločný deliteľ čísel $a$, $b$ (ten existuje, a je jednoznačne určený) budeme označovať $D(a, b)$.

**Veta 2.4.** *Pre každé $a, b, c \in \mathsf{Z}$ platí*

$$D(a, 0) = |a|,$$
$$D(a, b) = D(b, a)$$

$$D(a, b) = D(a - b.c, b),$$
$$D(c.a, c.b) = |c|.D(a, b),$$
$$D(a, b) = D(|a|, |b|).$$

Systematickým používaním prvých troch vzorcov (pričom tretí používame len pre $a \geqq b > 0$, $c = a$ DIV DIV $b$) možno určiť $D(a, b)$ pre každé $a, b \in \mathsf{N}$; pre $a < 0$ alebo $b < 0$ použijeme ešte najprv piaty vzorec. Takýto postup nazývame *Euklidovým algoritmom* pre výpočet $D(a, b)$. Pri vhodnej úprave nám tiež umožní určiť čísla $x$, $y$ z nasledujúcej vety.

**Veta 2.5.** *Ak $a, b \in \mathsf{Z}$, $a \neq 0$ alebo $b \neq 0$, tak $D(a, b)$ je najmenšie kladné celé číslo, ktoré sa dá vyjadriť v tvare $x.a + y.b$, $x, y \in \mathsf{Z}$. Ak $a = b = 0$, tak $D(a, b) = 0$.*

Na konkrétnom príklade $a = -162$, $b = 183$ ukážeme, ako možno vhodne zapisovať Euklidov algoritmus, ktorý určí $D(a, b)$ i čísla $x$, $y$ z vety 2.5. Zápis bude vyzerať takto

| —162 | 183 | | |
|---|---|---|---|
| 0 | 1 | 183 | |
| —1 | 0 | 162 | —1 |
| 1 | 1 | 21 | —7 |
| —8 | —7 | 15 | —1 |
| 9 | 8 | 6 | —2 |
| —26 | —23 | 3 | —2 |
| | | 0 | |

Vzniká teda číselná tabuľka zo štyroch stĺpcov. V záhlaví prvých dvoch stĺpcov uvedieme čísla $a$, $b$; nakoniec v týchto stĺpcoch vzniknú čísla $x$, $y$. Do tretieho stĺpca pod čiaru vpíšeme čísla $|a|$, $|b|$, a to najprv max $(|a|, |b|)$ (s výnimkou prípadu $ab = 0$; vtedy najprv napíšeme nulu). Pre prvé tri čísla $u$, $v$, $w$ v každom riadku okrem záhlavia má platiť $au + bv = w$;

v prvých dvoch riadkoch to možno dosiahnuť vhodnou voľbou $u, v \in \{-1, 0, 1\}$. Každý ďalší riadok vzniká pripočítaním vhodného násobku posledného hotového riadku k predposlednému. Príslušný koeficient, ktorý zapisujeme do štvrtého stĺpca, dostaneme až na znamienko celočíselným delením čísel v treťom stĺpci; zvyšok pri tomto delení môžeme hneď zapísať do tretieho stĺpca. Takto postupujeme, pokiaľ v treťom stĺpci nevznikne nula; riadok s nulou už nedopočítavame. Potom na prvých troch miestach posledného riadku máme po rade čísla $x$, $y$, $D(a, b)$. Teda v danom prípade je

$$D(-162, 183) = 3 = -26.(-162) - 23.183$$

*Najmenším spoločným násobkom* čísel $a$, $b$ nazveme také číslo $n$, ktoré je ich *spoločným násobkom* (t. j. $a|n$, $b|n$) a je deliteľom každého ich spoločného násobku. Najmenšie spoločné násobky čísel $a$, $b$ sa môžu líšiť iba znamienkom. Nezáporný najmenší spoločný násobok čísel $a$, $b$ budeme označovať $nsn(a, b)$. Možno ho určovať podľa nasledujúcej vety.

**Veta 2. 6.** *Pre všetky $a, b \in \mathbb{Z}$ platí*

$$nsn(a, b) . D(a, b) = |a| . |b| .$$

*Ďalej,* $nsn(0, 0) = 0$.

Uvedieme ešte niekoľko vzorcov pre najväčší spoločný deliteľ a najmenší spoločný násobok.

**Veta 2.7.** *Pre každé $a$, $b \in \mathbb{Z}$ sú nasledujúce tri podmienky ekvivalentné:*

(i) $a|b$;
(ii) $D(a, b) = |a|$;
(iii) $nsn(a, b) = |b|$.

**Veta 2.8.** *Pre všetky* $x, y, z \in \mathsf{Z}$ *platí*

$$D(x, x) = |x|$$
$$D(x, y) = D(y, x)$$
$$D(D(x, y), z) = D(x, D(y, z))$$
$$D(x, nsn(x, y)) = |x|$$
$$D(x, nsn(y, z)) = nsn(D(x, y), D(x, z))$$

$$nsn(x, x) = |x|$$
$$nsn(x, y) = nsn(y, x)$$
$$nsn(nsn(x, y), z) = nsn(x, nsn(y, z))$$
$$nsn(x, D(x, y)) = |x|$$
$$nsn(x, D(y, z)) = D(nsn(x, y), nsn(x, z)).$$

Operácie $D$, $nsn$ sú síce binárne, ale budeme tiež hovoriť o nezápornom najväčšom spoločnom deliteli, resp. najmenšom spoločnom násobku $n$ čísel, a budeme ho značiť $D(x_1, \ldots, x_n)$, resp. $nsn(x_1, \ldots, x_n)$. Na základe vety 2.8 vieme, že je jedno, ako budeme združovať argumenty (a medzivýsledky) do dvojíc, aby sme na ne mohli použiť pôvodnú binárnu operáciu.

Celé čísla $a$, $b$ nazveme *nesúdeliteľnými*, ak $D(a, b) = 1$.

**Veta 2.9.** *Nech* $a, b, c \in \mathsf{Z}$, *pričom čísla* $a, b$ *sú nesúdeliteľné. Potom*

(i) *ak* $a|c, b|c$, *tak* $a.b|c$;
(ii) *ak* $a|b.c$, *tak* $a|c$.

Na zisťovanie deliteľnosti pevným číslom sa niekedy namiesto vydelenia používajú pravidlá deliteľnosti. Aby sme niektoré z nich mohli sformulovať, zavedieme si dva pojmy. Nech $i, j, m \in \mathsf{P}$. Potom *j-ciferný súčet* čísla $m$ je číslo, ktoré dostaneme nasledovne. Najprv rozdelíme číslo $m$ (presnejšie, jeho dekadický zápis) od konca na skupiny po $j$ cifier. Potom tieto skupiny pokladáme za samostatné čísla, a všetky ich sčítame. (Prípadné nuly na začiatkoch skupín ignorujeme.) Výsledok je hľadaný $j$-ciferný súčet; pre $j = 1$ hovoríme jednoducho o *cifernom súčte*. *Posledné i-číslie* čísla $m$ je číslo tvorené jeho poslednými $i$ číslicami (alebo všetkými číslicami, ak ich $m$ má menej než $i$) v pôvodnom poradí; prípadné nuly na začiatku môžeme ignorovať. Ako príklad uveďme, že dvojciferný súčet čísla 1234567 je $1 + 23 + 45 + 67 = 136$ a posledné trojčíslie je 567. Pomocou operácie MOD možno posledné $i$-číslie čísla $m$ vyjadriť v tvare $m$ MOD $10^i$ a pre jeho $j$-ciferný súčet $c$ platí

$$c \operatorname{MOD}(10^j - 1) = m \operatorname{MOD}(10^j - 1).$$

**Veta 2.10.** *Nech $m, d, i \in \mathsf{P}$, $d \mid 10^i$. Potom zvyšky pri delení čísla m a jeho posledného i-čísla číslom d sú rovnaké. Špeciálne, m je násobkom čísla d práve vtedy, keď jeho posledné i-číslie je násobkom d.*

**Veta 2.11.** *Nech $m, d, j \in \mathsf{P}$, $d \mid (10^j - 1)$. Potom číslo m a jeho j-ciferný súčet dávajú rovnaký zvyšok pri delení číslom d. Špeciálne, m je násobkom d práve vtedy, keď jeho j-ciferný súčet je násobkom d.*

V šiestom odseku tejto kapitoly uvidíme, že ku každému $d \in \mathsf{P}$ nesúdeliteľnému s 10 existuje $j$ potrebné do predchádzajúcej vety. Pre tie $d$, pre ktoré nemožno použiť vetu 2.10 ani vetu 2.11, možno použiť nasledujúce tvrdenie:

**Veta 2.12.** *Nech $m, d, d_1, d_2, i, j \in \mathsf{P}$, $d = d_1 . d_2$, $d_1 \mid 10^i$, $d_2 \mid (10^j - 1)$. Potom číslo m je násobkom čísla d práve vtedy, keď jeho posledné i-číslie je násobkom čísla $d_1$ a jeho j-ciferný súčet je násobkom čísla $d_2$.*

Pre každé celé číslo $d > 1$ možno nájsť $d_1, d_2, i, j \in \mathsf{P}$, ktoré spĺňajú podmienky z vety 2.12; pritom $d_1$, $d_2$ sú jednoznačne určené. Vetu 2.12 použijeme len v prípade $d_1 > 1$, $d_2 > 1$; inak je výhodnejšie použiť niektorú z predchádzajúcich dvoch viest.

Vety 2.10 a 2.11 umožňujú vždy jednoducho určiť i zvyšok pri delení číslom $d$. Veta 2.12 to bezprostredne neumožňuje (okrem prípadu, keď je tento zvyšok nulový). Pritom však zvyšok pri delení čísla $m$ číslom $d$ je jednoznačne určený zvyškami pri delení $m$ číslami $d_1$, $d_2$. Spôsob, ako ho možno vypočítať, uvedieme v piatom odseku tejto kapitoly.

Vety 2.10, 2.11, 2.12 platia pre ľubovoľný základ číselnej sústavy; vtedy však pochopiteľne 10 znamená tento základ, a nie číslo desať.

Ako príklad použitia viet 2.10, 2.11, 2.12 uvedieme pravidlá deliteľnosti pre $d = 16$, 27 a $88 = 8.11$. Pre každé $m \in \mathsf{P}$ platí:

*Číslo m je deliteľné* 16-*mi práve vtedy, keď jeho posledné štvorčíslie je deliteľné* 16-*mi.*

*Číslo m je deliteľné* 27-*mi práve vtedy, keď jeho trojciferný súčet je deliteľný* 27-*mi.*

*Číslo m je deliteľné* 88-*mi práve vtedy, keď jeho posledné trojčíslie je deliteľné ôsmimi a jeho dvojciferný súčet je deliteľný jedenástimi.*

Pre $d = 7$ nedostávame „dobré" pravidlo deliteľnosti, lebo by sme museli tvoriť až šesťciferný súčet.

## 3. PRVOČÍSLA A ICH ROZLOŽENIE

*Prvočíslo* je také $n \in \mathsf{P}$, ktoré má práve dva kladné delitele. Existuje nekonečne mnoho prvočísel a možno ich zoradiť do rastúcej postupnosti

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

Ak chceme o nejakom čísle zistiť, či je prvočíslo alebo nie, môžeme použiť vetu:

**Veta 3.1.** *Celé číslo $a > 1$ je prvočíslo práve vtedy, keď nemá žiadny deliteľ $d$, $1 < d \leqq \sqrt{a}$.*

Namiesto všetkých $d$ z uvedeného intervalu stačí skúmať len prvočíselné hodnoty $d$, čo je vhodné, ak máme k dispozícii tabuľku prvočísel aspoň po $[\sqrt{a}]$. Ak nie, môžeme skúmať len deliteľnosť číslami $d = 2, 3$, a ďalej číslami $d$ tvaru $6k \pm 1$. Počet delení, ktoré urobíme, bude síce vyšší než pri použití tabuľky prvočísel, ale len približne tretinový v porovnaní s prípadom delenia všetkými $d$ z vety.

Ak chceme nájsť všetky prvočísla po istú hranicu (a nemáme po ruke alebo nechceme použiť hotové tabuľky), je vhodné tzv. *Eratostenovo sito*. Vypíšeme si za sebou všetky kladné celé čísla (až po hranicu $n_0$, pokiaľ chceme prvočísla zisťovať), a prečiarkneme číslo 1. Potom opakujeme nasledujúci postup: podčiarkneme najmenšie nepodčiarknuté a neprečiarknuté číslo, a prečiarkneme všetky jeho ďalšie násobky (až po hranicu $n_0$; na viacnásobnom prečiarknutí nezáleží). Takto postupne podčiarkujeme práve všetky prvočísla v poradí podľa veľkosti. Tento postup ukončíme, akonáhle podčiarkneme prvé číslo väčšie než $\sqrt{n_0}$. Potom prvočísla až po $n_0$ sú práve všetky neprečiarknuté čísla.

Označme $\pi(n)$ počet prvočísel neprevyšujúcich $n$. Platí

$$\lim_{n \to \infty} \left( \pi(n) : \frac{n}{\ln n} \right) = 1. \tag{3.1}$$

Je to hlboký číselnoteoretický výsledok, ale nemožno z neho urobiť žiaden odhad hodnoty $\pi(n)$ pre konkrétne

$n$. Možno ho však urobiť na základe nasledujúceho tvrdenia ([7], str. 406):

**Veta 3.2.** *Pre každé $n \geqq 55$ platí*

$$\frac{n}{\ln n + 2} < \pi(n) < \frac{n}{\ln n - 4}. \tag{3.2}$$

Zo vzorca (3.1) (ale aj z (3.2)) vyplýva, že rad prevrátených hodnôt prvočísel diverguje, a že existujú ľubovoľne dlhé konečné postupnosti zložených čísel. (Ale obe tvrdenia sa dajú dokázať omnoho elementárnejšie.) Nasledujúca veta hovorí o tom, že vzdialenosti medzi za sebou idúcimi prvočíslami nemôžu byť príliš veľké (v porovnaní s týmito prvočíslami).

**Veta 3.3** a) (Bertrandov postulát.) *Pre každé $n \geqq 2$ existuje prvočíslo $p$ medzi $n$ a $2n$ (t. j. $n < p < 2n$).*

b) *Pre každé $n \geqq 48$ existuje prvočíslo $p$ medzi $n$ a $\frac{9}{8} n$.*

c) *Pre každé $n \geqq 7$ leží medzi číslami $n$ a $2n$ aspoň jedno prvočíslo každého z tvarov $3k + 1$, $3k + 2$, $4k + 1$, $4k + 3$.*

d) *Existuje také $n_0$, že pre každé $n \geqq n_0$ existuje aspoň jedno prvočíslo medzi $n^3$ a $(n + 1)^3$.*

(Pre tvrdenie b), c) pozri [6], str. 14.)

Ešte uvedieme tri výsledky numerického charakteru; na ich formuláciu označíme $p_n$ $n$-té prvočíslo (t. j. $p_1 = 2$, $p_2 = 3$ atď.); toto označenie nebudeme používať v ďalších odsekoch.

**Veta 3.4.** a) *Najmenšie prvočíslo, pre ktoré platí $p_{n+1} - p_n > 100$ je $p_n = 370261$; pre toto prvočíslo platí $p_{n+1} - p_n = 112$.*

b) *Pre* $p_n < 10^7$ *platí* $p_{n+1} - p_n \leqq 154$, *a najmenšie prvočíslo, pre ktoré tu nastáva rovnosť, je* $p_n = 4652353$.
c) *Pre* $p_n > 2020000$ *platí* $p_{n+1} - p_n \leqq p_n/16597$.

Prvé dva výsledky sú uvedené v [7], str. 318, tretí je zo [14].

## 4. ROZKLAD NA PRVOČINITELE

**Veta 4.1.** *Každé číslo* $a \in \mathsf{P}$ *sa dá vyjadriť v tvare*

$$a = p_1^{e_1} . p_2^{e_2} . \ \ldots \ . p_n^{e_n}, \tag{4.1}$$

*kde* $p_1, \ldots, p_n$ *sú po dvoch rôzne prvočísla a* $e_1, \ldots, e_n \in \mathsf{P}$. (Pre $a = 1$ je $n = 0$, t. j. pravá strana (4.1) je prázdny súčin.) *Toto vyjadrenie je jednoznačné až na poradie činiteľov.*

Vyjadrenie (4.1) bude úplne jednoznačné, ak budeme žiadať $p_1 < p_2 < \ldots < p_n$. Ak uvažujeme rozklady viacerých čísel súčasne, býva vhodné, aby postupnosť $p_1, \ldots, p_n$ bola pre všetky tieto čísla rovnaká. To môžeme dosiahnuť, ak pripustíme aj nulové exponenty $e_1, \ldots, e_n$ v (4.1). Niekedy používame (4.1) aj s nulovými exponentmi vtedy, keď vieme síce odhadnúť zhora prvočísla, ktoré sa vyskytnú v rozklade nejakého čísla, nevieme však, či tam budú všetky až po túto hranicu.

**Veta 4.2.** *Nech* $a, b \in \mathsf{P}$, $p_1, \ldots, p_n$ *sú po dvoch rôzne prvočísla a nech platí* (4.1) *a*

$$b = p_1^{f_1} . p_2^{f_2} . \ \ldots \ . p_n^{f_n}, \tag{4.2}$$

*pričom* $e_1, \ldots, e_n, f_1, \ldots, f_n \in \mathsf{N}$. *Potom:*

(i) $a \mid b$ *práve vtedy, keď* $e_i \leqq f_i$ *pre všetky* $i = 1, \ldots, n$;

(ii) *a je k-tou mocninou prirodzeného čísla práve vtedy, keď* $k | e_i$, *pre všetky* $i = 1, \ldots, n$;
(iii) $D(a, b) = p_1^{\min(e_1, f_1)} . p_2^{\min(e_2, f_2)} . \ldots . p_n^{\min(e_n, f_n)}$;
(iv) $nsn(a, b) = p_1^{\max(e_1, f_1)} . p_2^{\max(e_2, f_2)} . \ldots . p_n^{\max(e_n, f_n)}$;
(v) $a . b = p_1^{e_1+f_1} . p_2^{e_2+f_2} . \ldots . p_n^{e_n+f_n}$.

Označme teraz pre $a \in \mathsf{P}$ $\varphi(a)$ počet čísel z množiny $\{0, 1, \ldots, a - 1\}$ nesúdeliteľných s $a$, $\tau(a)$ počet kladných deliteľov čísla $a$ a $S(a)$ súčet kladných deliteľov čísla $a$. Funkcia $\varphi$ sa nazýva *Eulerova funkcia*.

**Veta 4.3.** *Nech číslo* $a \in \mathsf{P}$ *má rozklad* (4.1), *pričom* $e_1, \ldots, e_n \in \mathsf{P}$.

*Potom platí*

$$\varphi(a) = a . \left(1 - \frac{1}{p_1}\right) . \left(1 - \frac{1}{p_2}\right) . \ldots . \left(1 - \frac{1}{p_n}\right);$$

$$\tau(a) = (e_1 + 1) . (e_2 + 1) . \ldots . (e_n + 1);$$

$$S(a) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} . \frac{p_2^{e_2+1} - 1}{p_2 - 1} . \ldots . \frac{p_n^{e_n+1} - 1}{p - 1}.$$

Ľahko zistíme, že predpoklad $e_1, \ldots, e_n \in \mathsf{P}$ bol potrebný iba pre Eulerovu funkciu $\varphi$.V ďalších dvoch vzorcoch zodpovedajú nulové exponenty činiteľom 1, ktoré neovplyvňujú výsledok.

**Veta 4.4.** *Pre každé dve nesúdeliteľné čísla* $a, b \in \mathsf{P}$ *platí*

$$\varphi(a . b) = \varphi(a) . \varphi(b), \quad \tau(a . b) = \tau(a) . \tau(b),$$
$$S(a . b) = S(a) . S(b).$$

Vlastnosť funkcií $\varphi$, $\tau$, $S$ vyjadrenú vo vete 4.4 nazývame *multiplikatívnosť*.

## 5. KONGRUENCIE A ZVYŠKOVÉ TRIEDY

Pre $a, b \in \mathsf{Z}$, $m \in \mathsf{P}$ hovoríme, že *a je kongruentné s b podľa modulu m* (alebo „*modulo m*"), a píšeme

$$a \equiv b(\mathrm{mod}\, m), \tag{5.1}$$

ak $m|(b - a)$. Vzťah (5.1) je ekvivalentný s rovnosťou

$$a \,\mathrm{MOD}\, m = b \,\mathrm{MOD}\, m.$$

**Veta 5.1.** *Pre pevne zvolené $m \in \mathsf{P}$ je kongruentnosť modulo $m$ reláciou ekvivalencie, t. j. pre každé, $a, b, c \in \mathsf{Z}$ platí*

(i) $a \equiv a(\mathrm{mod}\, m)$;
(ii) *ak* $a \equiv b(\mathrm{mod}\, m)$, *tak* $b \equiv a(\mathrm{mod}\, m)$;
(iii) *ak* $a \equiv b(\mathrm{mod}\, m)$, $b \equiv c(\mathrm{mod}\, m)$. *tak* $a \equiv c(\mathrm{mod}\, m)$.

Keďže kongruentnosť modulo $m$ (formálne je to množina $\{(a, b) \in \mathsf{Z} \times \mathsf{Z};\ a \equiv b(\mathrm{mod}\, m)\}$) je reláciou ekvivalencie na $\mathsf{Z}$, zodpovedá jej istý rozklad množiny $\mathsf{Z}$. Prvky tohto rozkladu nazývame *zvyškové triedy modulo m*. Zvyškovú triedu modulo $m$ môžeme určiť pomocou ktoréhohokoľvek jej prvku, spravidla ju však určujeme pomocou toho jej prvku $a$, pre ktorý platí $0 \leqq a < m$. Pri úvahách o kongruenciách modulo $m$ väčšinou záleží iba na zvyškových triedach, a nie na ich konkrétnych reprezentantoch.

**Veta 5.2.** *Ak $a, b, c, d \in \mathsf{Z}$, $m \in \mathsf{P}$ a platí*

$$a \equiv b(\mathrm{mod}\, m), \qquad c \equiv d(\mathrm{mod}\, m),$$

*tak platí aj*

$$a + c \equiv b + d(\mathrm{mod}\, m),\ \ a - c \equiv b - d(\mathrm{mod}\, m),$$

$$a . c \equiv b . d(\mathrm{mod}\, m).$$

Špeciálne, pre $c = d$ takto zistíme, že kongruenciu možno násobiť číslom. O možnosti deliť kongruenciu a o druhom možnom spôsobe násobenia, resp. delenia kongruencií hovorí nasledujúca veta.

**Veta 5. 3.** *Nech* $a, b, c \in \mathsf{Z}$. $m \in \mathsf{P}$. *Potom*

a) *Ak* $a.c \equiv b.c (\mathrm{mod}\ m)$ *a čísla* $c$, $m$ *sú nesúdeliteľné, tak platí* $a \equiv b (\mathrm{mod}\ m)$.
b) *Ak* $c \neq 0$, *tak vzťahy* $a \equiv b (\mathrm{mod}\ m)$ a

$$a.c \equiv b.c (\mathrm{mod}\ m.|c|)$$

*sú ekvivalentné.*

Kongruencie s neznámymi riešime podobne ako rovnice (tu nie je zaužívaný žiadny pár termínov zodpovedajúci páru rovnosť — rovnica): snažíme sa ich upraviť na taký tvar, že naľavo je neznáma, a na pravej strane už známa hodnota. Pritom používame najmä úpravy, uvedené v predchádzajúcich vetách. (Samozrejme, tento postup nevedie vždy k cieľu a existujú aj iné spôsoby, obdobne ako pri rovniciach.)

Niekedy môžeme kongruenciu modulo $m$ vyriešiť preskúmaním všetkých $m$ zvyškových tried modulo $m$ pomocou ich reprezentantov. Riešením kongruencií sa nebudeme systematicky zaoberať. Uvedieme len vety o systémoch kongruencií s jednou neznámou, v ktorých jednotlivé kongruencie sú už „vo vyriešenom tvare".

**Veta 5.4.** *Nech* $m_1$, $m_2 \in \mathsf{P}$, $a_1$, $a_2 \in \mathsf{Z}$. *Potom sústava dvoch kongruencií*

$$x \equiv a_1 (\mathrm{mod}\ m_1), \quad x \equiv a_2 (\mathrm{mod}\ m_2) \tag{5.2}$$

*má riešenie práve vtedy, keď*

$$a_1 \equiv a_2 (\mathrm{mod}\ D(m_1, m_2)). \tag{5.3}$$

*Ak je podmienka* (5.3) *splnená, tak existuje práve jedno* $b \in \{0, 1, \ldots, nsn(m_1, m_2) - 1\}$ *také, že sústava* (5.2) *je ekvivalentná s kongruenciou*

$$x \equiv b(\text{mod } nsn(m_1, m_2)). \tag{5.4}$$

Číslo $b$ do vzťahu (5.4) môžeme určiť napríklad tak, že Euklidovým algoritmom nájdeme $d = D(m_1, m_2)$ a celé čísla $u$, $v$ také, že $d = um_1 + vm_2$ a položíme

$$b = \left(a_2 u . \frac{m_1}{d} + a_1 v . \frac{m_2}{d}\right) \text{MOD } nsn(m_1, m_2). \tag{5.5}$$

**Veta 5.5.** *Sústava kongruencií*

$$x \equiv a_i(\text{mod } m_i), \quad i = 1, \ldots, n \tag{5.6}$$

*má riešenie práve vtedy, keď*

$$a_i \equiv a_j(\text{mod } D(m_i, m_j)) \text{ pre všetky } i, j,\ 1 \leqq i < j \leqq n. \tag{5.7}$$

*Ak je podmienka* (5.7) *splnená, tak existuje celé číslo* $b$ *také, že sústava* (5.6) *je ekvivalentná s kongruenciou*

$$x \equiv b(\text{mod } nsn(m_1, \ldots, m_n)). \tag{5.8}$$

Špeciálne, sústava (5.6) je riešiteľná vždy vtedy, keď sú čísla $m_1, \ldots, m_n$ po dvoch nesúdeliteľné. Vzorec (5.5) by bolo možné zovšeobecniť aj na sústavu (5.6), výhodnejšie je však riešiť ju tak, že postupne znižujeme počet kongruencií v nej podľa vety 5.4 a vzorca (5.5).

Ešte sa zmienime o jednej veľmi jednoduchej diofantickej rovnici. (Prídavné meno „diofantický" pri rovnici alebo systéme rovníc znamená, že sa zaoberáme len celočíselnými, prípadne len prirodzenými riešeniami.)

**Veta 5.6.** *Rovnica*

$$(5.9) \qquad ax + by = c,$$

*kde $a$, $b$, $c$ sú celé čísla, má celočíselné riešenie práve vtedy, keď $D(a, b) \mid c$. Ďalej, ak $(a, b) \neq (0, 0)$ a $(x_0, y_0)$ je jedno celočíselné riešenie rovnice* (5.9), *tak všetky jej celočíselné riešenia možno dostať podľa vzorcov*

$$(5.10) \quad x = x_0 + \frac{b}{D(a, b)}.t, \quad y = y_0 - \frac{a}{D(a. b)}.t, \quad t \in \mathrm{Z}.$$

Podľa tejto vety môžeme zisťovať tiež riešiteľnosť každej kongruencie tvaru $ax \equiv b(\mathrm{mod}\ m)$ tým, že miesto nej vyšetrujeme diofantickú rovnicu $ax + my = b$. Táto kongruencia je riešiteľná práve vtedy, keď je riešiteľná uvedená rovnica, t. j. keď $D(a, m)|b$.

## 6. UMOCŇOVANIE ZVYŠKOVÝCH TRIED

Ak je $a \equiv b(\mathrm{mod}\ m)$, tak pre každé $n \in \mathrm{N}$ je tiež $a^n \equiv b^n(\mathrm{mod}\ m)$. Teda takto možno kongruencie umocňovať, obdobne ako ich možno sčítavať a násobiť. Avšak zo vzťahov

$$a \equiv b(\mathrm{mod}\ m), \qquad r \equiv s(\mathrm{mod}\ m)$$

nevyplýva (a to ani pre $r$, $s \in \mathrm{P}$) vzťah $a^r \equiv b^s(\mathrm{mod}\ m)$. Teda týmto spôsobom kongruencie umocňovať nemožno. Uvedieme niekoľko výsledkov o tom, čím možno podmienku $r \equiv s(\mathrm{mod}\ m)$ vhodne nahradiť.

**Veta 6.1.** (Malá Fermatova veta.) *Ak $p$ je prvočíslo, tak pre každé $a \in \mathrm{Z}$ platí*

$$a^p \equiv a \pmod{p}. \tag{6.1}$$

Pokiaľ sú $a$, $p$ nesúdeliteľné (t. j. $p \nmid a$), možno zo (6.1) dostať

$$a^{p-1} \equiv 1 \pmod{p}; \tag{6.2}$$

zrejme aj (6.1) možno dostať zo (6.2).

Zovšeobecnenie vzorca (6.2) na prípad zloženého modulu dáva nasledujúca veta; $\varphi$ v nej znamená Eulerovu funkciu: pre $n \in \mathsf{P}$ je $\varphi(n)$ počet čísel z množiny $\{0, 1, \ldots, n - 1\}$ nesúdeliteľných s $n$. (Vzorec na výpočet $\varphi(n)$ je vo vete 4.3.)

**Veta 6.2.** (Eulerova veta.) *Ak $a \in \mathsf{N}$, $m \in \mathsf{P}$ a čísla $a$, $m$ sú nesúdeliteľné, tak*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{6.3}$$

Vzorec (6.3) je zrejme zovšeobecnením vzorca (6.2); nájsť zovšeobecnenie vzorca (6.1) by bolo o niečo komplikovanejšie.

Pokiaľ sú $a$, $m$ nesúdeliteľné, existuje *inverzný prvok k $a$ podľa modulu $m$* (t. j. taký prvok $b$, že platí $a . b \equiv 1 \pmod{m}$). Vtedy možno zaviesť mocniny $a$ modulo $m$ s ľubovoľným celočíselným exponentom; špeciálne, $a^{-1}$ bude inverzný prvok k $a$. Nesmieme však zabudnúť, že takéto mocniny sú vždy robené pre pevne zvolený modul $m$.

***Rádom prvku a podľa modulu m*** nazveme najmenšie $r \in \mathsf{P}$ také, že $a^r \equiv 1 \pmod{m}$. (Tento rád je definovaný vtedy a len vtedy, keď sú $a$, $m$ nesúdeliteľné.) Ak je $r$ rád prvku a podľa modulu $m$, a $n \in \mathsf{N}$, tak platí

$$a^n \equiv 1 \pmod{m} \text{ práve vtedy, keď } r \mid n.$$

Špeciálne odtiaľ dostávame $r \mid \varphi(m)$.

**Definícia 6.3.** Hovoríme, že číslo $a$, $0 < a < m$ je *primitívny koreň podľa modulu* $m$, ak je rád prvku $a$ podľa modulu $m$ rovný $\varphi(m)$.

**Veta 6.4.** *Nech $m \in \mathsf{P}$, $m > 1$. Potom primitívny koreň podľa modulu $m$ existuje práve vtedy, keď $m = 2$, $m = 4$, $m = p^e$ alebo $m = 2p^e$, kde $e \in \mathsf{P}$ a $p$ je nepárne prvočíslo.*

Zvoľme teraz pevne nejaké $m$ vyhovujúce podmienke z vety 6.4 a nejaký jeho primitívny koreň $g$. Najmenšie $i \in \mathsf{N}$ také, že

$$a \equiv g^i (\mathrm{mod}\ m)$$

nazveme *index čísla* $a$ a označíme ho ind $(a)$. (Striktne vzaté, mali by sme v označení ind, ako aj v termíne „index čísla" uvádzať aj príslušné $m$ a $g$; nerobíme to, pretože sme ich pevne zvolili.) Potom ind $(a)$ je definované práve vtedy, keď sú čísla $a$, $m$ nesúdeliteľné. Ďalšie vlastnosti uvádza nasledujúca veta.

**Veta 6.5.** *Nech $m$ spĺňa podmienku z vety 6.4 a $g$ je jeho (zvolený) primitívny koreň. Potom pre každé $a$, $b$ nesúdeliteľné s $m$ platí:*

$$0 \leqq \mathrm{ind}\,(a) < \varphi(m) \tag{6.4}$$

$$a \equiv b (\mathrm{mod}\ m) \text{ práve vtedy, keď } \mathrm{ind}\,(a) = \mathrm{ind}\,(b) \tag{6.5}$$

$$\mathrm{ind}\,(a.b) \equiv \mathrm{ind}\,(a) + \mathrm{ind}\,(b)\ (\mathrm{mod}\ \varphi(m)) \tag{6.6}$$

$$\mathrm{ind}\,(a^n) \equiv n.\mathrm{ind}\,(a)\ (\mathrm{mod}\ \varphi(m))\,. \tag{6.7}$$

Tieto vzorce ukazujú, že funkcia ind má podobné vlastnosti ako logaritmus. Ak máme k dispozícii jej hodnoty (vo vhodných tabuľkách), tak ju môžeme aj podobne použiť. Pre prvočíselné $m < 100$ sú takéto tabuľky uvedené v [10]. Na ukážku pomocou týchto tabuliek vyriešime kubickú kongruenciu

$$x^3 \equiv 13\ (\mathrm{mod}\ 61)\,.$$

Zvolíme $m = 61$ (a $g = 2$, pretože tomu zodpovedajú tabuľky). Postupne dostávame

$$\operatorname{ind}(x^3) = \operatorname{ind}(23),$$

$$3 \operatorname{ind}(x) \equiv 57 \pmod{60},$$

$$\operatorname{ind}(x) \equiv 19 \pmod{20}.$$

Teda $\operatorname{ind}(x) \in \{19, 39, 59\}$, čomu zodpovedá

$$x \equiv 54, 37, 31 \pmod{61}.$$

Posledný zápis treba rozumieť tak, že mu vyhovujú všetky $x$, ktoré sú kongruentné modulo 61 s niektorým číslom na pravej strane.
Ešte uvážme kongruenciu

$$x^3 \equiv 20 \pmod{43}.$$

Zvolíme $m = 43$ (a $g = 3$). Postupne dostávame

$$\operatorname{ind}(x^3) = \operatorname{ind}(20),$$

$$3 \operatorname{ind}(x) \equiv 37 \pmod{42}.$$

Pretože však kongruencia

$$3y \equiv 37 \pmod{42}$$

nemá riešenie, nemá riešenie ani pôvodná kubická kongruencia.

Hovoríme, že $a$ je *kvadratický zvyšok podľa modulu $m$*, ak kongruencia

$$x^2 \equiv a \pmod{m}$$

má riešenie. V opačnom prípade hovoríme, že $a$ je *kvadratický nezvyšok modulo $m$*. Pokiaľ existuje $\operatorname{ind}(a)$ (pre modul $m$), $a$ je kvadratický zvyšok podľa modulu $m$ práve vtedy, keď $\operatorname{ind}(a)$ je párne číslo.

**Veta 6.6.** *Nech* $m = 4$, $m = p^e$ *alebo* $m = 2p^e$, *kde* $d \in \mathsf{P}$ *a* $p$ *je nepárne prvočíslo a nech* $D(a, m) = 1$. *Potom* $a$ *je kvadratický zvyšok podľa modulu* $m$ *práve vtedy, keď*

$$a^{\varphi(m)/2} \equiv 1(\mathrm{mod}\, m).$$

V porovnaní s podmienkou z vety 6.4 sme vynechali prípad $m = 2$, kedy je $\varphi(m) = 1$, teda $\frac{\varphi(m)}{2}$ nie je celé číslo. V ostatných prípadoch je $\varphi(m)$ zrejme párne.

Hovoríme, že $a$ je *kubický zvyšok podľa modulu* $m$, ak kongruencia

$$x^3 \equiv a(\mathrm{mod}\, m)$$

má riešenie. V opačnom prípade hovoríme, že $a$ je *kubický nezvyšok podľa modulu* $m$. Ak existuje ind $(a)$ pre modul $m$ a $3|\varphi(m)$, tak $a$ je kubický zvyšok podľa modulu $m$ práve vtedy, keď $3|$ind $(a)$. Ak $m$ spĺňa podmienku z vety 6.4 a $3 \nmid \varphi(m)$, tak každé celé číslo $a$ nesúdeliteľné s $m$ je kubický zvyšok modulo $m$.

**Veta 6.7** *Nech* $m$ *spĺňa podmienku z vety* 6.4, $3|\varphi(m)$ *a číslo* $a$ *je nesúdeliteľné s* $m$. *Potom* $a$ *je kubický zvyšok podľa modulu* $m$ *práve vtedy, keď*

$$a^{\varphi(m)/3} \equiv 1(\mathrm{mod}\, m).$$

Preskúmajme teraz, či je možné znížiť exponent $\varphi(m)$ vo vzorci (6.3) v Eulerovej vete. Pokiaľ existuje primitívny koreň modulo $m$, tak exponent $\varphi(m)$ nemožno znížiť. V ostatných prípadoch ho však znížiť možno. Označme pre každé $m \in \mathsf{P}$ symbolom $\lambda(m)$ najmenší spoločný násobok rádov podľa modulu $m$ všetkých čísel nesúdeliteľných s $m$ (stačí ich brať len spomedzi čísel $0, 1, \ldots, m - 1$). Platí $\lambda(m)|\varphi(m)$, a $\lambda(m)$ je najmenší exponent, ktorým možno $\varphi(m)$ v Eulerovej vete nahradiť. Číslo $\lambda(m)$ nazývame *univerzálny exponent modulo* $m$.

**Veta 6.8.** (i) *Ak $m$ je mocnina nepárneho prvočísla lebo $m = 2$ alebo $m = 4$, tak $\lambda(m) = \varphi(m)$;*

(ii) *Ak $m$ je mocnina dvoch, $m > 4$, tak*

$$\lambda(m) = \frac{1}{2}\varphi(m)\left(= \frac{1}{4}m\right);$$

(iii) *Ak sú $m_1$, $m_2$ nesúdeliteľné čísla, tak*
$$\lambda(m_1 . m_2) = nsn(\lambda(m_1), \lambda(m_2)).$$

Teda ak pre číslo $a$ platí (4.1), tak

$$\lambda(a) = nsn(\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \ldots, \lambda(p_n^{e_n})).$$

Napríklad pre $a = 1000$ platí

$$\lambda(1000) = nsn(\lambda(8), \lambda(125)) = nsn(2,100) = 100.$$

Vo vetách 2.11, 2.12 o pravidlách deliteľnosti sa vyskytovalo číslo $j$, nebolo však jasné, ako ho nájsť (a či vôbec existuje). Vždy možno položiť $j = \lambda(d)$, resp. $j = \lambda(d_2)$, ale nedostaneme tak vo všeobecnosti najmenšie vhodné $j$. Avšak najmenšie vhodné $j$ je vždy deliteľom čísla $\lambda(d)$.

## 7. SÚČTY ŠTVORCOV

Niektoré, no nie všetky, prirodzené čísla sa dajú vyjadriť v tvare súčtu dvoch štvorcov celých čísel (ďalej len „štvorcov").
Napríklad

$$2 = 1^2 + 1^2, \quad 5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2,$$

avšak čísla 3, 6, 7 už obdobne vyjadriť nemožno. O možnosti tohoto vyjadrenia hovorí nasledujúca veta.

**Veta 7.1.** a) *Prvočíslo $p$ sa dá vyjadriť v tvare súčtu dvoch štvorcov práve vtedy, keď $p \not\equiv 3 \pmod 4$. Jeho vyjadrenie v tomto tvare je jednoznačné až na poradie sčítancov.*

b) *Číslo $a \in \mathsf{P}$ sa dá vyjadriť v tvare súčtu dvoch štvorcov práve vtedy, keď v jeho rozklade na prvočinitele* (4.1) *nevystupuje žiadne prvočíslo tvaru $4k + 3$ s nepárnym exponentom.*

c) *Číslo $a \in \mathsf{P}$ sa dá vyjadriť v tvare súčtu dvoch nesúdeliteľných štvorcov práve vtedy, keď nie je deliteľné žiadnym prvočíslom tvaru $4k + 3$.*

Ak chceme nájsť vyjadrenie nejakého čísla $a \in \mathsf{P}$ v tvare súčtu dvoch štvorcov, stačí nájsť takéto vyjadrenie pre jeho prvočinitele s nepárnymi exponentmi v rozklade (4.1), a ďalej použiť vzorec

$$(7.1) \quad (a^2 + b^2).(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Vyjadrovanie v tvare súčtu dvoch štvorcov súvisí tiež s rozkladom na gaussovské prvočísla; pozri 8. odsek tejto kapitoly.

Pre vyjadrovanie celých čísel v tvare súčtu štyroch štvorcov platí nasledujúca

**Veta 7.2.** (Lagrangeova veta.) *Každé celé nezáporné číslo možno vyjadriť v tvare súčtu štyroch štvorcov.*

Jednoznačnosť už neplatí ani pre prvočísla tvaru $4k + 3$; napríklad

$$19 = 4^2 + 1^2 + 1^2 + 1^2 = 3^2 + 3^2 + 1^1 + 0^2.$$

Ak hľadáme (aspoň jedno) vyjadrenie čísla $a \in \mathsf{P}$ v tvare súčtu štyroch štvorcov, stačí nájsť takéto vyjadrenia pre jeho prvočíselné delitele, a ďalej používať vzorec

$$(7.2)\ (a^2 + b^2 + c^2 + d^2).(A^2 + B^2 + C^2 + D^2) = \\ = (aA - bB - cC - dD)^2 + (aB + bA + \\ + cD - dC)^2 + (aC - bD + cA + dB)^2 + \\ + (aD + bC - cB + dA)^2.$$

Nie každé prirodzené číslo možno písať ako súčet troch štvorcov; takto nemožno napísať napríklad číslo 15. Pritom však $15 = 3.5$, a čísla 3, 5 možno písať ako súčty troch štvorcov. Teda analógia vzorcov (7.1), (7.2) pre súčty troch štvorcov neexistuje.

## 8. GAUSSOVSKÉ CELÉ ČÍSLA

Komplexné čísla tvaru $a + bi$, kde $a, b \in \mathsf{Z}$, nazývame *gaussovské celé čísla*. Pri obvyklom znázornení komplexných čísel v rovine zodpovedajú tzv. *mrežovým bodom*, t. j. bodom s celočíselnými súradnicami. Množinu všetkých gaussovských celých čísel budeme označovať G.

**Veta 8.1.** *Pre každé $a, b \in \mathsf{G}$, $b \neq 0$ existujú $q, r \in \mathsf{G}$ také, že*

$$a = b.q + r \quad \text{a} \quad |r| < |b|.$$

Čísla $q$, $r$ vo všeobecnosti nie sú jednoznačne určené. (V závislosti od $a$, $b$ možno $q$ zvoliť jedným až štyrmi spôsobmi; potom je už $r$ určené jednoznačne.) Pre $r \in G$ nemusí byť $|r|$ celé číslo, ale $||r|| = |r|^2$ (tzv. norma čísla $r$) už je celé nezáporné číslo. Vo vete 8.1 zrejme možno nahradiť absolútne hodnoty normami, čo je pri niektorých úvahách výhodné.

Pre $a, b \in \mathsf{G}$ budeme písať $a|b$, ak existuje $c \in \mathsf{G}$ také, že $a.c = b$. (Pokiaľ je $a, b \in \mathsf{Z}$, tak $a|b$ v tomto novom zmysle je ekvivalentné s $a|b$ v pôvodnom zmysle pre celé čísla; preto nevadí, že používame rovnaký symbol.) Relácia deliteľnosti na G má obdobné vlastnosti ako relácia deliteľnosti na Z. Napríklad veta 2.1 bude platiť, ak v nej všade nahradíme písmeno Z písmenom G. V (iii) by sme však mohli doplniť $i|a$. Ktorékoľvek dve z čísel

$$a, \mathrm{i}.a, -a = \mathrm{i}^2.a, -\mathrm{i}.a = \mathrm{i}^3.a$$

sú z hľadiska deliteľnosti úplne rovnocenné; hovoríme tiež, že sú *asociované*. Niekedy si zo štyroch navzájom asociovaných čísel pevne vyberáme jedno. Urobíme to aj my v nasledujúcej definícii, aby sme potom mohli ľahšie vysloviť vetu o rozklade na prvočinitele pre gaussovské celé čísla.

**Definícia 8.2.** *Gaussovské prvočísla* sú

a) číslo $1 + \mathrm{i}$;
b) každé (obyčajné) prvočíslo tvaru $p = 4k + 3$, kde $k \in \mathsf{N}$;
c) každé číslo $a + b\mathrm{i}$, kde $a \in \mathsf{P}$, $b \in \mathsf{Z}$, $a^2 + b^2$ je (obyčajné) prvočíslo a $|b| < a$.

Teda gaussovskými prvočíslami sú napríklad

$$1 + \mathrm{i}, 3, 2 + \mathrm{i}, 2 - \mathrm{i}, 7, 11, 3 + 2\mathrm{i}, 3 - 2\mathrm{i}, \ldots$$

ale nie sú nimi napríklad

$$1, 1 - \mathrm{i}, -3, 1 + 2\mathrm{i}, 5, 17, \ldots$$

(aj keď niektoré z týchto čísel sú asociované s gaussovskými prvočíslami).

Postupnosť všetkých gaussovských prvočísel možno dostať z postupnosti všetkých (obyčajných) prvočísel tak, že v nej

a) prvočíslo 2 nahradíme číslom $1 + \mathrm{i}$;

b) prvočísla tvaru $4k + 3$ ponecháme;

c) každé prvočíslo $p$ tvaru $4k + 1$ nahradíme dvojicou čísel

$$a + bi,\ a - bi \text{ takou, že } a^2 + b^2 = p \text{ a } 0 < b < a .$$

Jednotlivé body tohoto predpisu zodpovedajú rovnako označeným bodom definície 8.2. Čísla $a \pm bi$, ktoré v bode c zodpovedajú prvočíslu $p$ (tvaru $4k + 1$), sú týmto $p$ jednoznačne určené a platí $p = (a + bi).(a - bi)$. Prvočíslo 2 možno síce písať ako $(1 + i).(1 - i)$, ale napriek tomu sme mu (v bode a) priradili jediné gaussovské prvočíslo, a to $1 + i$. Číslo $1 - i$ je totiž už s ním asociované, pretože $1 - i = i^3.(1 + i)$, a preto sme ho nezaradili medzi gaussovské prvočísla. (Voľbu medzi $1 + i$, $1 - i$ sme však mohli urobiť ľubovoľne.)

**Veta 8.3.** *Každé $a \in \mathsf{G} - \{0\}$ sa dá vyjadriť v tvare*

$$a = i^e . q_1^{e_1} . q_2^{e_2} . \ldots . q_k^{e_k} , \tag{8.1}$$

*kde $e \in \{0, 1, 2, 3\}$, $q_1, \ldots, q_k$ sú po dvoch rôzne gaussovské prvočísla a $e_1, \ldots, e_k \in \mathsf{P}$. Rozklad* (8.1) *je jednoznačný až na poradie činiteľov.*

Napríklad

$$\begin{aligned} 1 &= i^0 \text{ (tu je } k = 0), \\ 7 - 4i &= i^3.(2 + i).(3 + 2i), \\ 65 &= (2 + i).(2 - i).(3 + 2i).(3 - 2i), \\ 8 &= i.(1 + i)^6. \end{aligned}$$

Rozklad celého čísla $a \neq 0$ na súčin gaussovských prvočísel (a mocniny i) podľa vety 8.3 možno urobiť tak, že najprv $a$ rozložíme na súčin prvočísel v tvare (4.1) a potom ešte rozložíme prvočíslo 2 a prvočísla tvaru $4k + 1$, ktoré sa nachádzajú v tomto rozklade.

## 9. FAKTORIÁLY A KOMBINAČNÉ ČÍSLA

*Faktoriály* $n!$ čísel $n \in \mathsf{N}$ môžeme definovať napríklad rekurentne vzorcami

$$(9.1) \qquad 0! = 1, \quad (n+1)! = n!.(n+1)$$

pre všetky $n \in \mathsf{N}$. *Kombinačné čísla* $\binom{m}{n}$ môžeme potom pre $m, n \in \mathsf{N}$, $n \leqq m$ definovať vzorcom

$$(9.2) \qquad \binom{m}{n} = \frac{m!}{n!.(m-n)!}$$

Možno ich však dostať i z Pascalovho trojuholníka. Niekedy sa definuje $\binom{m}{n}$ pre každé $m \in \mathsf{N}$, $n \in \mathsf{Z}$; vtedy pre $n < 0$ alebo $n > m$ kladieme $\binom{m}{n} = 0$.

**Veta 9.1.** (Wilsonova). *Číslo $n > 1$ je prvočíslo práve vtedy, keď $(n-1)! + 1 \equiv 0 \pmod{n}$.*

**Veta 9.2.** *Pre každé $n \in \mathsf{P}$ je číslo $\binom{2n}{n}$ deliteľné všetkými prvočíslami $p$, $n < p \leqq 2n$.*

Rozklad faktoriálov na prvočinitele možno tvoriť podľa nasledujúcej vety.

**Veta 9. 3.** *Pre každé $n \in \mathsf{N}$ platí*

$$(9.3) \qquad n! = \prod_{p \leqq n} p^{e_p} \text{ kde } e_p = \sum_{k=1}^{[\log_p n]} \left[\frac{n}{p^k}\right]$$

*pre všetky $p$ ($p$ prebieha prvočísla nepresahujúce $n$).*

Prakticky nemusíme počítať $\lfloor \log_p n \rfloor$, ale stačí tvoriť príslušné členy radu pre $e_p$, pokiaľ sú nenulové. Napríklad pre $n = 10$ bude

$$e_2 = \left\lfloor \frac{10}{2} \right\rfloor + \left\lfloor \frac{10}{4} \right\rfloor + \left\lfloor \frac{10}{8} \right\rfloor = 5 + 2 + 1 = 8,$$

$$e_3 = \left\lfloor \frac{10}{3} \right\rfloor + \left\lfloor \frac{10}{9} \right\rfloor = 3 + 1 = 4,$$

$$e_5 = \left\lfloor \frac{10}{5} \right\rfloor = 2, \quad e_7 = \left\lfloor \frac{10}{7} \right\rfloor = 1,$$

a preto $10! = 2^8 . 3^4 . 5^2 . 7$.

Ako dôsledok predchádzajúcej vety dostávame:

**Veta 9.4.** *Pre každé $m, n \in \mathbb{N}, m \leqq n$ platí*

$$\binom{n}{m} = \prod_{p \leqq n} p^{f_p}, \tag{9,4}$$

$$kde\ f_p = \sum_{k=1}^{\lfloor \log_p n \rfloor} \left( \left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor - \left\lfloor \frac{n-m}{p^k} \right\rfloor \right)$$

*pre všetky $p$ ($p$ prebieha prvočísla nepresahujúce $n$).*

Výraz $\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor - \left\lfloor \frac{n-m}{p^k} \right\rfloor$ môže nadobúdať len hodnotu 0 alebo 1, pričom hodnotu 1 nadobúda práve vtedy, keď pri sčítaní čísel $m$, $n - m$ v sústave o základe $p$ nastáva prenos z $(k - 1)$-ého do $k$-tého rádu. Teda $f_p$ je počet prenosov pri sčítaní čísel $m$, $n - m$ v sústave o základe $p$.

Faktoriály rastú veľmi rýchle, a ich výpočet násobením je namáhavý. Približne môžeme ich hodnoty počítať podľa Stirlingovho vzorca

$$(9.5)\qquad n! \doteq \sqrt{2\pi n}\,.\left(\frac{n}{e}\right)^n$$

kde $\doteq$ znamená asymptotickú rovnosť: V limite pre $n \to \infty$ sa podiel ľavej a pravej strany blíži k jednej. Pravda, z tohoto faktu samotného nemožno robiť žiadne závery o presnosti vzorca (9.5). Platí však, že pre $n \geqq 10$ relatívna chyba výsledku nepresiahne $\frac{10}{n}$ % (teda napríklad 1 % pre $n = 10$, ale len 0,1 % pre $n = 100$). Presnejšie vzorce sú napríklad: pre všetky $n \geqq 2$

$$(9.6)\qquad \sqrt{2\pi n}\,.\left(\frac{n}{e}\right)^n\left(1 + \frac{1}{12n}\right) < n! < \sqrt{2\pi n}\left(\frac{n}{e}\right)^n\cdot\left(1 + \frac{1}{11n}\right)$$

a pre všetky $n \geqq 8$

$$(9.7)\qquad \sqrt{2\pi n}\,.\left(\frac{n}{e}\right)^n\cdot\left(1 + \frac{1}{12n} + \frac{0{,}9}{288n^2}\right) < n! < \sqrt{2\pi n}\cdot\left(\frac{n}{e}\right)^n\cdot\left(1 + \frac{1}{12n} + \frac{1}{288n^2}\right).$$

Pokiaľ je výhodné použiť logaritmus faktoriálu, môžeme ho približne počítať podľa vzorca

$$(9.8)\qquad \ln(n!) = n.(\ln n - 1) + \frac{1}{2}\ln(2\pi n) + \frac{1}{12n} - \frac{1}{360n^3} + \frac{1}{1260n^5} - \frac{1}{1680n^7} + \frac{1}{1188n^9} - \dots$$

pre každé $n \geqq 2$. Možno v ňom vziať ľubovoľný počet členov (ale aspoň 2). Absolútna chyba nepresiahne prvý vynechaný člen, a bude mať rovnaké znamienko.

Výsledky tohto odseku platia všeobecne pre postupnosti komplexných čísel. Číselnú postupnosť $(a_0, a_1, a_2, \ldots)$ nazveme *rekurentnou postupnosťou druhého stupňa*, ak existujú (komplexné) čísla $p$, $q$ také, že pre všetky prirodzené čísla $n$ platí

(10.1) $$a_{n+2} = p.a_{n+1} + q.a_n.$$

Na určenie tejto postupnosti potrebujeme okrem vzorca (10.1) poznať jej prvé dva členy $a_0$, $a_1$. Ak má kvadratická rovnica

(10.2) $$x^2 = p.x + q$$

dva rôzne korene $x_1$, $x_2$, tak pre každú postupnosť vyhovujúcu vzorcu (10.1) existujú čísla $u$, $v$ také, že pre každé prirodzené číslo $n$ platí

(10.3) $$a_n = u.x_1^n + v.x_2^n.$$

Hovoríme, že $(a_0, a_1, a_2, \ldots)$ je *lineárna kombinácia* geometrických postupností

$$(1, x_1, x_1^2, \ldots), \qquad (1, x_2, x_2^2, \ldots)$$

s koeficientmi $u$, $v$. K daným $a_0$, $a_1$ vypočítame príslušné $u$, $v$ zo vzťahu (10.3) pre $n = 0, 1$. Ak má rovnica (20.2) dvojnásobný koreň $x_1$, tak namiesto vzorca (10.3) platí vzorec

(10.4) $$a_n = u.x_1^n + v.nx_1^n,$$

t. j. $(a_0, a_1, a_2, \ldots)$ je lineárna kombinácia postupností.

$$(1, x_1, x_1^2, \ldots), \qquad (0, x_1, 2x_1^2, \ldots).$$

Koeficienty $u$, $v$ sa dajú vypočítať obdobne. Ak vyšetrujeme reálnu postupnosť $(a_0, a_1, a_2, \ldots)$ a rovnica (10.2) má imaginárne korene $x_{1,2} = r.(\cos\alpha \pm \mathrm{i}\sin\alpha)$, tak namiesto vzorca (10.3) možno použiť vzorec

(10.5) $$a_n = u_1.r^n \cos n\alpha + v_1.r^n \sin n\alpha.$$

Teda $(a_0, a_1, a_2, \ldots)$ je lineárna kombinácia postupností

$$(1, r\cos\alpha, r^2\cos 2\alpha, \ldots), 0, r\sin\alpha, r^2\sin 2\alpha, \ldots).$$

Koeficienty $u_1$, $v_1$ budú reálne čísla zatiaľ čo $u$, $v$ vo vzorci (10.3) mohli vyjsť imaginárne.

Postupnosť $(a_0, a_1, a_2, \ldots)$ nazveme *rekurentnou postupnosťou stupňa k*, ak existujú čísla $p_0, p_1, \ldots, p_{k-1}$ také, že pre každé prirodzené $n$ platí

(10.6) $$a_{n+k} = p_{k-1}a_{n+k-1} + p_{k-2}a_{n+k-2} + \ldots + p_0a_n$$

Na jej jednoznačné určenie potrebujeme poznať ešte jej prvých $k$ členov $a_0, a_1, \ldots, a_{k-1}$. Ak má rovnica

(10.7) $$x^k = p_{k-1}x^{k-1} + p_{k-2}x^{k-2} + \ldots + p_0$$

$k$ po dvoch rôznych koreňov $x_1, x_2, \ldots, x_k$, tak každá postupnosť spĺňajúca (10.6) je lineárnou kombináciou geometrických postupností

$$(1, x_j, x_j^2, \ldots), \quad j = 1, 2, \ldots, k.$$

Aj v prípade, že rovnica (10.7) má viacnásobné korene, je každá postupnosť spĺňajúca (10.6) lineárnou kombináciou vhodných $k$ postupností. Dostaneme ich tak, že k $s$-násobnému koreňu $q$ rovnice (10.7) priradíme vždy $s$ postupností

$$(0^j q^0, 1^j q^1, 2^j q^2, 3^j q^3. \ldots), j = 0, 1, \ldots, s - 1.$$

(Všimnime si, že pre $j = 0$ priraďujeme geometrickú postupnosť s kvocientom $q$; teda prípad jednoduchých koreňov je tu tiež zahrnutý.) Ak sú (niektoré) korene rovnice (10.7) imaginárne, a chceme uvažovať len reálne postupnosti, použijeme postup obdobný prechodu od (10.3) k (10.5). Podrobnosti nechávame na rozmyslenie čitateľovi, rovnako ako sme mu ponechali zovšeobecnenie pojmu lineárnej kombinácie z dvoch na $k$ postupností.

## 11. NIEKTORÉ NEROVNOSTI

Z mnohých nerovností v [4] pripomeňme aspoň nerovnosť medzi aritmetickým a geometrickým priemerom.

**Veta 11.1.** *Pre všetky kladné reálne čísla* $a_1, a_2, \ldots, \ldots, a_n (n \neq 0)$ *platí*

$$\sqrt[n]{a_1 . a_2 . \ldots . a_n} \leqq \frac{a_1 + a_2 + \ldots + a_n}{n}.$$

Nerovnosti pre kombinačné čísla možno odvodzovať okrem iného zo Stirlingovho vzorca pre faktoriály. Často však možno postupovať oveľa elementárnejšie, napríklad nerovnosť

$$\binom{n}{k} < 2^n$$

pre $0 \leqq k < n$ snáď najľahšie dostaneme pomocou rozvoja výrazu $(1 + 1)^n$ podľa binomickej vety.

Nerovnosti v nasledujúcej vete spresňujú niektoré tzv. približné vzorce, ktoré sa často nájdu v príručkách („spravočnikoch"), prípadne i v tabuľkách, ale nie vždy s uvedením oboru platnosti (ktorý závisí aj od požadovanej presnosti). Ak je čitateľ oboznámený so základmi diferenciálneho počtu, zaiste zbadá, že väčšina koeficientov pri mocninách $x$ v uvedených nerovnostiach vzniká z Taylorových radov pre odhadované funkcie. Ostatné koeficienty (napríklad $-\frac{1}{7}$ v odhade pre $\sin x$) sú zvolené v tvare zlomkov s malými menovateľmi, aj za cenu istého oslabenia odhadov. Odhady sú tým presnejšie, t. j. dolný a horný odhad sú k sebe tým bližšie, čím menšie je $x$. (Okrem toho by sme ich mohli spresniť, keby sme uvažovali menší interval pre $x$.)

**Veta 11.2.** *Pre každé reálne číslo* $x$, $0 < x < 1$, *platí*

$$1 - x + \frac{1}{2}x^2 < \frac{1}{1+x} < 1 - x + x^2,$$

$$1 + \frac{1}{2}x - \frac{1}{8}x^2 < \sqrt{1+x} < 1 + \frac{1}{2}x - \frac{1}{12}x^2,$$

$$1 - \frac{1}{2}x - \frac{1}{2}x^2 < \sqrt{1-x} < 1 - \frac{1}{2}x - \frac{1}{8}x^2,$$

$$x - \frac{1}{2}x^2 < \ln(1+x) < x - \frac{3}{10}x^2,$$

$$-x - \frac{x^2}{2(1-x)} < \ln(1-x) < -x - \frac{x^2}{2},$$

$$1 + x + \frac{1}{2}x^2 < \mathrm{e}^x < 1 + x + \frac{3}{4}x^2,$$

$$1 - x + \frac{1}{3}x^2 < \mathrm{e}^{-x} < 1 - x + \frac{1}{2}x^2,$$

$$x - \frac{1}{6}x^3 < \sin x < x - \frac{1}{7}x^3,$$

$$1 - \frac{1}{2}x^2 < \cos x < 1 - \frac{4}{9}x^2,$$

$$x + \frac{1}{3}x^3 < \operatorname{tg} x < x + \frac{4}{7}x^3.$$

Uvedieme ešte obdobné vzorce pre dekadický logaritmus a funkciu $10^x$, avšak už s koeficientmi v dekadickom zápise a zaokrúhlenými vhodným smerom.

**Veta 11.3.** *Pre každé reálne číslo* $x$, $0 < x < 1$, *platí*

$$0{,}43429x - 0{,}22x^2 < \log(1 + x) < 0{,}4343x$$

$$-0{,}4343x - 0{,}22 \, . \frac{x^2}{1 - x} < \log(1 - x) < -0{,}43429x$$

$$1 + 2{,}30258x < 10^x < 1 + 2{,}30259x + 6{,}7x^2$$

$$1 - 2{,}30259x < 10^{-x} < 1 - 2{,}30258x + 2{,}7x^2 .$$

**Veta 11.4.** *Ak pre reálne čísla* $y, z, x, a, b$ *platia nerovnosti* $0 < |y| < 0{,}02$, $0 < |z| < 2 \, . \, 10^{-5}$, $0 < x < 1$, $0 <$ $< a < b$, *tak*

$$0{,}43 \, . \, |y| < |\log(1 + y)| < 0{,}44 \, . \, |y| ,$$

$$0{,}43429 \, . \, |z| < |\log(1 + z)| < 0{,}4343 \, . \, |z| ,$$

$$(1 - x) \, . \log a + x \, . \log b < \log((1 - x) \, . \, a + x \, . \, b) <$$

$$< (1 - x) \, . \log a + x \, . \log b + 0{,}0543 \, . \left(\frac{b - a}{a}\right)^2 .$$

Posledný vzorec sa dá použiť pri interpolácii hodnôt z logaritmických tabuliek. Napríklad pri bežnom použití logaritmických tabuliek [1] je $\frac{b - a}{a} < 0{,}00091$, teda interpolovanú hodnotu určíme s chybou najviac $5 \, . \, 10^{-6} +$ $+ 0{,}0543 \, . \, 0{,}00091^2 < 5{,}05 \, . \, 10^{-6}$.

V nasledujúcej vete pôjde o odhady súčinov mnohých činiteľov blízkych k 1. Ako návod pre čitateľa, ktorý by si chcel vetu dokázať, uvádzame: Pri pevne zvolenom čísle $x$ (a pevnom $n$) sú uvedené súčiny minimálne, ak

$n - 1$ činiteľov je rovných jednej a maximálne, ak sú všetky činitele navzájom rovné. Dolné odhady už vyjdú triviálne, pre horné treba ešte použiť binomickú vetu a ďalej odhadovať členy, ktoré vzniknú.

**Veta 11.5.** *Ak sú $a_1, a_2, \ldots, a_n$ nezáporné reálne čísla a pre ich súčet $x = a_1 + a_2 + \ldots + a_n$ platí* $0 < x < 1$, tak

$$1 + x \leqq (1 + a_1).(1 + a_2). \ldots .(1 + a_n) < 1 + x + \frac{3}{4} x^2 ,$$

$$1 - x \leqq (1 - a_1).(1 - a_2). \ldots .(1 - a_n) < 1 - x + \frac{1}{2} x^2 .$$

# 4. NEROVNOSTI S MOCNINAMI

**Úloha 4.1.** Usporiadajte podľa veľkosti čísla

$$A = 5^{6^{6^6}},\ B = 8^{8^{8^5}},\ C = 6^{3^{6^7}},\ D = 9^{9^{9^4}}.$$

*Riešenie I* (s kalkulačkou alebo tabuľkami). Platí $\log\log A = \log(6^{6^6}\log 5) = 6^6 \log 6 + \log\log 5 \doteq$ $\doteq 36305{,}27$ a obdobne $\log\log B \doteq 29592{,}41$, $\log\log C \doteq$ $\doteq 133563{,}3$, $\log\log D \doteq 6260{,}76$.
Rozdiely medzi vypočítanými číslami sú dostatočné na to, aby sme mohli usúdiť

$$\log\log D < \log\log B < \log\log A < \log\log C,$$

a teda $D < B < A < C$. □

Pre výpočet s tabuľkami by bolo výhodné logaritmovať ešte raz (t. j. počítať $\log\log\log A$ atď.), pričom by sme uvážili, že $|\log\log 5| < 1$, teda vplyv tohto sčítanca na výsledný logaritmus je malý; skutočne, podľa vzorca

$$\log(x + y) = \log x + \log\left(1 + \frac{y}{x}\right),$$

máme

$$\log\log\log A = 6\log 6 + \log\log 6 + \\ + \log\left(1 + \frac{\log\log 5}{6^6 \log 6}\right).$$

Posledný sčítanec je (záporný a) v absolútnej hodnote menší než

$$0{,}44\,.\,\frac{|\log\log 5|}{6^6\,.\log 6} < 3\,.\,10^{-6}.$$

Odhady pre $B$, $C$, $D$ (s číslami 8, 6, 9 namiesto 5) by vyšli podobne.

*Riešenie II* (bez použitia kalkulačky a tabuliek). Platí

$$9^{9^{9^4}} < 64^{9^{9^4}} = 8^{2\cdot 9^{9^4}} < 8^{9^{9^4+1}} < 8^{9^{10000}} < 8^{16^{10000}} =$$

$$= 8^{2^{40000}} < 8^{6^{13334}} < 8^{8^{2^{14}}} < 8^{8^{8^5}}, \text{ a teda } D < B.$$

$$8^{8^{8^5}} < 25^{8^{8^5}} = 5^{2\cdot 2^{3\cdot 8^5}} = 5^{2^{3\cdot 2^{15}+1}} < 5^{2^{100000}} =$$

$$= 5^{32^{20000}} < 5^{6^{40000}} < 5^{6^{216^2}} = 5^{6^{(6^3)^2}} =$$

$$= 5^{6^{6^6}}, \text{ a teda } B < A.$$

Najťažší odhad, ktorý sme potrebovali, bol $2^{15} = 32768 <$ $< 33333$. Všetky ostatné sa dajú overiť spamäti. Nakoniec

$$5^{6^{6^6}} < 6^{6^{6^6}} < 6^{9^{6^6}} = 6^{3^{2\cdot 6^6}} < 6^{3^{6^7}}, \text{ a teda } A < C.$$

Spolu teda máme $D < B < A < C$. □

Pri druhom riešení sme potrebovali „uhádnuť“ poradie čísel podľa veľkosti. Inak by sme sa mohli napríklad pokúšať o dôkaz nerovnosti $B < D$ (čo by sa nám, samozrejme, nevydarilo) alebo o dôkaz nerovnosti $D < C$ (čo by sa nám asi podarilo, ale nakoniec by bolo zbytočné). Namiesto hádania sme však mohli („tajne“) použiť prvé riešenie; z neho sme tiež mohli usudzovať, aké jemné odhady asi budú potrebné.

**Úloha 4.2.** Určite, ktoré z čísel

$$A = 7^{2^{8^9}}, B = 6^{9^{9^8}}$$

je väčšie.

*Riešenie I* (s kalkulačkou). Platí

$$\log\log A \doteq 40403562, \quad \log\log B \doteq 41077010{,}96,$$

a preto $A < B$. □

*Riešenie II*. Platí

$$9^6 = 3^{12} = 531441 > 524288 = 2^{19}$$

(môžeme to zistiť priamym výpočtom alebo z tabuliek), a preto

$$7^{2^{8^9}} < 6^{2\cdot 2^{2^{27}}} = 6^{2^{2^{27}+1}} < 6^{9^{6(2^{27}+1)/19}} = 6^{9^{6(2^8\cdot 2^{19}-1)/19}} <$$

$$< 6^{9^{6\cdot 256\cdot 9^6/19}} = 6^{9^{1536\cdot 9^6/19}} < 6^{9^{81\cdot 9^6}} = 6^{9^{9^8}},$$

teda $A < B$. □

Rozdiel medzi $\log\log A$, $\log\log B$ síce stačil na prvé riešenie, je však príliš malý na to, aby sme zistili $A < B$ využitím odhadu $3^2 > 2^3$. (Keby sme v $B$ nahradili nižšiu deviatku osmičkou, dostali by sme už číslo menšie než $A$.)

**Úloha 4.3.** Zistite, ktoré z čísel

$$A = 2^{2^{2^{125743}}}, \quad B = 3^{2^{3^{79335}}}$$

je väčšie.

*Riešenie*. Označme $C = 2^{125743}$, $D = 3^{79335}$. Zrejme $A \neq B$, $C \neq D$. Ukážeme, že $A < B$ práve vtedy, keď $C < D$. Skutočne, ak $C < D$, tak zrejme

$$A = 2^{2^C} < 2^{2^D} < 3^{2^D} = B.$$

Obrátene, ak $C > D$, tak $C \geqq D + 1$, a potom

$$B = 3^{2^D} < 4^{2^D} = 2^{2^{D+1}} \leqq 2^{2^C} = A,$$

teda $A > B$. Preto stačí len zistiť, ktoré z čísel $C, D$ je väčšie. Z tabuľky 37-miestnych logaritmov zaokrúhlením dostaneme

$$\log 2 = 0{,}301029995664 \pm 5.10^{-13},$$

$$\log 3 = 0{,}477121254720 \pm 5.10^{-13}.$$

Preto platí

$$\log C = 125743 \log 2 = 37852{,}414744778 \pm 7.10^{-8},$$

$$\log D = 79335 \log 3 = 37852{,}414743211 \pm 5.10^{-8}$$

a odtiaľ už vidno $\log C > \log D$, teda $C > D$, a teda aj $A > B$. □

Keby sme počítali na kalkulačke (konkrétne SHARP PC 1211, ale bez použitia programovania), dostali by sme

$$\log C = 125743 \log 2 = 37852{,}41474$$

$$\log D = 79335 \log 3 = 37852{,}41474,$$

teda čísla $C$, $D$ by sme nevedeli porovnať. Využitím „skrytých miest" by sme dostali

$$125743 \log 2 - 79335 \log 3 \doteq 16.10^{-7}$$

a teda $C > D$, „skryté miesta" však vo všeobecnosti nemusia byť spoľahlivé, a teda ani určenie znamienka čísla $\log C - \log D$ týmto spôsobom nie je spoľahlivé.

Všimnime si tiež, že z nášho riešenia dostávame $\log C - \log D = 157.10^{-8} \pm 13.10^{-8}$, teda relatívna chyba, s ktorou je určené číslo $\log C - \log D$, je značná (presahuje 8 %). Zobrať hodnoty $\log 2$, $\log 3$ napríklad s presnosťou na 10 desatinných miest by už zrejme nestačilo.

**Úloha 4.4.** Nájdite najväčšie celé číslo $x$, pre ktoré platí

$$x^{x^x} < 100^{100}.$$

*Riešenie.* Platí $x \geqq 4$, pretože

$$4^{5^5} = 4^{256} < 4^{300} = 64^{100} < 100^{100}.$$

Na druhej strane, $x < 5$, pretože

$$5^{5^5} > 5^{3 \cdot 5^3} = (5^3)^{5^3} = 125^{125} > 100^{100}.$$

Preto hľadané číslo je $x = 4$. □

**Úloha 4.5.** Nájdite najväčšie celé čísla $x$, $y$, $z$, pre ktoré platí

$$x^{4^4} < 100^{100},\ 4^{y^4} < 100^{100},\ 4^{4^z} < 100^{100}.$$

*Riešenie.* Podľa predchádzajúcej úlohy vieme $x \geqq 4$, $y \geqq 4$, $z \geqq 4$. Z odhadov

$$4^{4^5} > 4^{5^4} > 4^{600} = (4^4)^{150} = 256^{150} > 100^{100}$$

potom vidíme $y = 4$, $z = 4$. Ostáva určiť $x$, Platí $x \geqq 6$, pretože

$$6^{4^4} = 6^{4.64} = (6^4)^{64} < 1300^{64} = 10^{192}.1{,}3^{64} <$$
$$< 10^{192}.1{,}7^{32} < 10^{192}.3^{16} < 10^{192}.10^8 = 100^{100}.$$

Na druhej strane, $x < 7$, pretože

$$7^{4^4} = 7^{4.64} = (7^4)^{64} > 2000^{64} = 10^{192}.2^{64} > 10^{192}.$$
$$.(2^{10})^6 > 10^{192}.(10^3)^6 = 10^{210} > 100^{100}.$$

Preto $x = 6$. □

Číslo $x$ sme mohli nájsť aj tak, že by sme najprv vyriešili rovnicu $u^{4^4} = 100^{100}$, odkiaľ ľahko dostaneme $\log u = \dfrac{200}{256} = 0{,}78125$. Pretože $u \notin \mathsf{N}$ je výsledkom $x = \lfloor u \rfloor$. Z tabuliek zistíme

$$\log 6 \doteq 0{,}77815, \qquad \log 7 \doteq 0{,}84510$$

teda $x = 6$. Pretože $\log u$ je podstatne bližšie k $\log 6$ než k $\log 7$, boli v pôvodnom riešení pre dôkaz $x \geqq 6$ potrebné presnejšie odhady než pre dôkaz $x < 7$.

**Úloha 4.6.** Nájdite najväčšie celé číslo $x$, pre ktoré platí

$$x^{x^{x^x}} < 1000^{1000^{1000}}.$$

*Riešenie.* Platí $x \geqq 5$, pretože

$$5^{5^{5^5}} = 5^{5^{3125}} < 5^{5^{4\cdot 800}} = 5^{625^{800}} < 1000^{1000^{1000}}.$$

Na druhej strane, $x < 6$, pretože

$$6^{6^{6^6}} = 6^{6^{36\cdot 36^2}} > 6^{6\cdot 6^{36000}} = (6^6)^{(6^{36})^{1000}} > 1000^{1000^{1000}}.$$

Teda hľadané číslo je $x = 5$. □

**Úloha 4.7.** Nájdite najväčšie celé číslo $x$, pre ktoré platí

$$x^{x^{x^5}} < 1000^{1000^{1000}}.$$

*Riešenie.* Podľa predchádzajúcej úlohy vieme $x \geqq 5$. Na druhej strane

$$6^{6^{6^5}} = 6^{6^{6\cdot 1296}} > 6^{6\cdot (6^6)^{1000}} = (6^6)^{(6^6)^{1000}} > 1000^{1000^{1000}}.$$

Teda hľadané číslo je $x = 5$. □

**Úloha 4.8.** Nájdite najväčšie celé číslo $x$, pre ktoré platí

$$x^{x^{5^5}} < 1000^{1000^{1000}}.$$

*Riešenie.* Platí

$$10^{10^{5^5}} = 10^{10^{3125}} = 10^{10^{125}.1000^{1000}} > 1000^{1000^{1000}}.$$

Preto $x < 10$. Pre výpočet s $x = 9$ najprv odhadneme

$$3^{25} = (3^5)^4 . 3^5 < 250^4 . 256 = 250^4 . 4^4 = 1000^4.$$

S pomocou tohto odhadu dostávame

$$9^{9^{5^5}} = 9^{9^{3125}} = 9^{(3^{25})^{250}} < 9^{(1000^4)^{250}} = 9^{1000^{1000}} <$$

$$< 1000^{1000^{1000}}.$$

Preto hľadané číslo je $x = 9$. □

Čitateľa asi napadlo, že teraz by mala nasledovať úloha nájsť najväčšie celé číslo $x$ také, že

$$x^{9^{5^5}} < 1000^{1000^{1000}}.$$

Môže sa o to pokúsiť, ale asi nebude mať dosť trpezlivosti na dokončenie výpočtu. Dobre urobí, ak najskôr skúsi určiť počet cifier výsledku.

**Úloha 4.9.** Nájdite najväčšie celé číslo $x$ také, že

$$x^{x^x} < 4^{4^{4^4}}.$$

*Riešenie.* Platí

$$80^{80^{80}} < 4^{4\cdot 8^{80}\cdot 10^{80}} = 4^{4\cdot 8^{80}\cdot 1000^{26}\cdot 100} < 4^{2^{2+240+260+7}} =$$

$$= 4^{2^{509}} < 4^{4^{255}} < 4^{4^{4^4}},$$

teda $x = 80$ ešte danej nerovnosti vyhovuje. Aby sme ukázali, že $x = 81$ už nevyhovuje, dokážme najprv nerovnosť $3^{12} > 2^{19}$. Platí

$$3^{12} = 729^2 = 512^2.\left(\frac{729}{512}\right)^2 = 2^{18}.\left(\frac{729}{512}\right)^2 > 2^{18}.\left(\frac{729}{513}\right)^2 =$$

$$= 2^{18}.\left(\frac{27}{19}\right)^2 = 2^{18}.\frac{729}{361} > 2^{18}.2 = 2^{19}.$$

S využitím tohto vzťahu odhadujme

$$81^{81^{81}} > 4^{81^{81}} = 4^{3^{324}} = 4^{(3^{12})^{27}} > 4^{(2^{19})^{27}} =$$

$$= 4^{2^{513}} > 4^{4^{256}} = 4^{4^{4^4}}.$$

Teda hľadané číslo je $x = 80$. □

Nebolo logicky nutné, aby sme v riešení ukázali, ako sme výsledok $x = 80$ našli; stačí, že sme ho „uhádli“, a potom overili. Teraz však ukážeme, ako sme mohli $x$ nájsť. Najprv upravme

$$4^{4^{4^4}} = 4^{4^{256}} = 4^{64^{256/3}};$$

odtiaľ vidíme $x \leqq \left\lfloor \max\left(4, 64, \frac{256}{3}\right)\right\rfloor = 85.$

Z druhej strany máme

$$4^{4^{4^4}} = 4^{4\cdot 4^{255}} = 256^{2^{510}} = 256^{128^{510/7}},$$

a odtiaľ vidno $x \geqq \left\lfloor \min\left(256, 128, \frac{510}{7}\right)\right\rfloor = 72$. Teda už vieme $72 \leqq x \leqq 85$. Tento interval pre $x$ môžeme ďalej zužovať. Napríklad, ak odhadneme

$$4^{4^{4^4}} = 256^{2^{510}} = 256^{1024^{51}} > 256^{10^{153}} > 256^{100^{76}},$$

vidíme $x \geqq 76$. Keby sme boli odhadli

$$2^{510} = 2^{240} . 2^{270} = 8^{80} . 1024^{27} > 8^{80} . 10^{81} > 80^{80},$$

dostali by sme nerovnosť $x \geqq 80$. Ďalej skúsime číslo približne zo stredu zvyšujúceho intervalu. Platí, napríklad

$$82^{82} = 82 . (82^{3})^{27} > 2^{6} . (2^{19})^{27} = 2^{6+19.27} =$$

$$= 2^{519} > 4^{256} = 4^{4^{4}},$$

a preto $82^{82^{82}} > 4^{4^{4^{4}}}$. Teraz už vieme, že riešením úlohy je $x = 80$ alebo $x = 81$. Stačí teda skúsiť, či pre $x = 81$ daná nerovnosť platí alebo nie.

Čím viac sa približujeme hľadanej hodnote $x$, tým presnejšie odhady potrebujeme. Okrem toho sme videli, že základ možno väčšinou odhadovať hrubo, kým exponenty, a to zvlášť najvyššie, treba odhadovať jemnejšie.

**Úloha 4.10.** Nájdite najväčšie celé číslo $x$, pre ktoré platí

$$x^{x^{80}} < 4^{4^{4^{4}}}.$$

*Riešenie.* Na dôkaz $x < 84$ dopredu odhadnime

$$3 . 84^{80} = 3 . 4^{80} . 21^{80} > 3 . 4^{80} . 440^{40} > 3 . 4^{80} . 2^{120} .$$

$$. 55^{40} > 3 . 4^{140} . 3000^{20} = 3 . 4^{140} . 2^{60} . 375^{20} = 3 . 4^{170} .$$

$$. \left(\frac{375}{256}\right)^{20} . 4^{80} = 4^{250} . 3 . \left(\frac{375}{256}\right)^{20} > 4^{250} . 3 . 1{,}46^{20} >$$

$$> 4^{250} . 3 . 2{,}12^{10} = 4^{255} . 3 . 1{,}06^{10} > 4^{255} . 3 . 1{,}6 >$$

$$> 4^{255} . 4 = 4^{4^{4}}.$$

Potom dostávame $84^{84^{80}} > 64^{84^{80}} = 4^{3 \cdot 84^{80}} > 4^{4^{4^{4}}}$.

Na dôkaz nerovnosti $x \geqq 83$ najprv odhadnime $83^2 = 6889 < 2^{13}$, a preto $83 < 4^{13/4} = 4^{3,25}$. Ďalej

$$3{,}25 . 83^{80} < 3{,}25 . (64 . 1{,}297)^{80} = 4^{240} . 3{,}25 . 1{,}297^{80} <$$
$$< 4^{240} . 3{,}25 . 1{,}6823^{40} < 4^{240} . 3{,}25 . 2{,}831^{20} < 4^{240} . 3{,}25 .$$
$$. 8{,}015^{10} < 4^{240} . 3{,}25 . 2^{30} . 1{,}002^{10} = 4^{255} . 3{,}25 . 1{,}002^{10} <$$
$$< 4^{255} . 3{,}25 . 1{,}03 < 4^{255} . 4 = 4^{4^4}.$$

Teraz už ľahko zistíme

$$83^{83^{80}} < 4^{3 \cdot 25 \cdot 83^{80}} < 4^{4^{4^4}}.$$

Preto $x = 83$. □

**Úloha 4.11.** Nájdite najväčšie celé číslo $x$, pre ktoré platí

$$x^{83^{80}} \leqq 4^{4^{4^4}}.$$

*Riešenie I* (s kalkulačkou). Zrejme platí $x = \lfloor a \rfloor$, kde $a$ je koreňom rovnice

$$a^{83^{80}} = 4^{4^{256}}.$$

Teda

$$a = 4^{4^{256}/83^{80}} = 4^{(4^{16}/83^5)^{16}} \doteq 252{,}918,$$

a preto $x = 252$. □

Dosť umelá úprava exponentu pri výpočte $a$ bola potrebná, aby nedošlo k preplneniu (na kalkulačke počítajúcej s číslami menšími než $10^{100}$ nemožno priamo vypočítať $4^{256}$).

*Riešenie II* (s tabuľkami [1]). Platí $x = \lfloor a \rfloor$, kde $a = 4^{4^{256}/83^{80}}$, teda $\log a = \dfrac{4^{256}}{83^{80}} \log 4$. Z tabuľky Logaritmy faktoriálov zistíme

$$\log 4 = \log 4! - \log 3! = 0{,}60206 \pm 10^{-8},$$

$$\log 83 = \log 83! - \log 82! = 1{,}9190781 \pm 10^{-8},$$

a preto

$$\log \frac{4^{256}}{83^{80}} = 0{,}601112 \pm 4 \, . \, 10^{-6}.$$

Ďalej platí (s uvážením všetkých chýb)

$$\log \log 4 = 0{,}779642 - 1 \pm 6 \, . \, 10^{-6},$$

a preto

$$\log \log a = 0{,}380754 \pm 10^{-5},$$

$$2{,}4029 < \log a < 2{,}4031 ,$$

$$252{,}8 < a < 253 .$$

Preto $x = 252$. □

**Úloha 4.12.** Nech postupnosti $(a_0, a_1, a_2, \ldots)$, $(b_0, b_1, b_2, \ldots)$ sú definované rekurentnými vzorcami

$$a_0 = 1, \; a_{n+1} = 2^{a_n}, \; b_0 = 1, \; b_{n+1} = 6^{b_n} .$$

Nájdite prirodzené číslo $n$, pre ktoré platí

$$b_n \leqq a_{100} \leqq b_{n+1} .$$

*Riešenie.* Dokážeme, že pre všetky prirodzené $n \geqq 2$ platí

(1) $$6b_n < a_{n+3} < b_{n+1} ;$$

z toho už bude bezprostredne vyplývať $n = 97$.
Pre $n = 2$ máme

$$6b_2 = 6^7 < 8^{20000} < 2^{65536} = 4^{32768} < 6^{32768} < 6^{6^6} = b_3 ;$$

pretože $2^{65536} = 2^{2^{16}} = a_5$, platí $6b_2 < a_5 < b_3$. Ďalej dokazujeme matematickou indukciou; nech (1) platí pre nejaké $n \geqq 2$. Potom

$$6b_{n+1} = 6^{b_n+1} < 2^{3b_n+3} < 2^{6b_n} < 2^{a_{n+3}} = a_{n+4},$$

$$a_{n+4} = 2^{a_{n+3}} < 6^{a_{n+3}} < 6^{b_{n+1}} = b_{n+2},$$

teda $6b_{n+1} < a_{n+4} < b_{n+2}$, čo bolo treba dokázať. □

# 5. POSLEDNÉ ČÍSLICE MOCNÍN

Pripomíname, že pod poslednými číslicami nejakého prirodzeného čísla vždy myslíme posledné číslice jeho dekadického zápisu, pokiaľ výslovne neuvedieme iný základ. Ani pri zmene základu však nemeníme význam číslic 0 až 9.

**Úloha 5.1.** Nájdite poslednú číslicu čísla $A = 4^{1234567}$.

*Riešenie I.* Indukciou dokážeme, že pre každé $n \in \mathsf{N}$ končí $4^{2n+1}$ číslicou 4. Pre $n = 0$ to zrejme platí. Ak už vieme, že $4^{2n+1}$ končí číslicou 4, t. j. že platí $4^{2n+1} \equiv 4 \pmod{10}$, tak ľahko zistíme (počítame modulo 10)

$$4^{2(n+1)+1} = 4^{2n+1}.16 \equiv 4.6 \equiv 4 \pmod{10},$$

teda aj $4^{2(n+1)+1}$ končí číslicou 4. Tým je dôkaz indukciou ukončený. Podľa práve dokázaného tvrdenia, ktoré použijeme pre $n = \lfloor 1234567/2 \rfloor = 617283$, končí aj $A$ číslicou 4. □

*Riešenie II.* Dokážeme, že $10 | (A - 4)$. Pretože $A$ je párne, platí $2 | (A - 4)$, a treba ešte dokázať $5 | (A - 4)$. Počítajme modulo 5

$$A - 4 \equiv (-1)^{1234567} - 4 = -1 - 4 =$$
$$= -5 \equiv 0 \pmod 5,$$

teda skutočne $5 | (A - 4)$. Potom $10 | (A - 4)$, a teda $A$ končí číslicou 4. □

Táto úloha bola taká ľahká, že ju čitateľ zaiste vedel vyriešiť spamäti. Pravdepodobne pritom postupoval podľa prvého riešenia, ale indukciu urobil intuitívne: všimol si pravidelné striedanie číslic 4, 6 v postupnosti mocnín štvorky. Uvedené riešenia, najmä prvé z nich mali skôr upozorniť čitateľa na princípy, ktoré sám používa, než naučiť ho niečo nové. V ďalších úlohách už nevypisujeme riešenia tak podrobne.

**Úloha 5.2.** Nájdite poslednú číslicu čísla $B = 7^{4567890}$.

*Riešenie.* Čísla 7, 10 sú nesúdeliteľné, $\varphi(10) = 4$, a preto podľa Eulerovej vety platí (počítame modulo 10)

$$B \equiv 7^{4567890 \text{ MOD } 4} = 7^2 \equiv 9 \pmod{10}.$$

Teda posledná číslica čísla $B$ je 9. □

**Úloha 5.3.** Nájdite poslednú číslicu čísla $C = 13^{17^{19}}$.

*Riešenie.* Použijeme Eulerovu vetu a počítame modulo 10

$$C \equiv 3^{17^{19}} \equiv 3^{17^{19} \text{MOD } 4} = 3^{1^{19} \text{MOD } 4} = 3^1 = 3 \pmod{10}.$$

Teda posledná číslica čísla $C$ je 3. □

**Úloha 5.4.** Nájdite poslednú číslicu čísla $D = 17^{15^{13^{11}}}$.

*Riešenie.* Použijeme Eulerovu vetu a počítame modulo 10. Platí

$$D \equiv 7^{15^{13^{11}} \text{MOD } 4} = 7^{3^{13^{11} \text{MOD } 2} \text{MOD } 4} = 7^{3^1 \text{MOD } 4} =$$
$$= 7^3 \equiv 3 \pmod{10}.$$

Teda hľadaná posledná číslica je 3. □

Necháme čitateľovi na rozmyslenie, že výsledok by sa nezmenil, keby sme k „štvorposchodovej mocnine", ktorou je dané číslo $D$, na ďalšie „poschodia" pridali napríklad 9, 7, 5.

**Úloha 5.5.** Nájdite posledné dvojčíslie čísla $7^{1986}$.

*Riešenie.* Treba vlastne určiť $7^{1986}$ MOD 100.
Pretože $7^4$ MOD 100 = 2401 MOD 100 = 1, platí

$$7^{1986} \mathrm{MOD}\ 100 = 7^{4.496+2} \mathrm{MOD}\ 100 = (7^4\ \mathrm{MOD}\ 100)^{496} .$$
$$.(7^2\ \mathrm{MOD}\ 100)\ \mathrm{MOD}\ 100 = 1^{496} . 49\ \mathrm{MOD}\ 100 = 49 .$$

Teda hľadané posledné dvojčíslie je 49. □

Keby sme hľadali posledné dvojčíslie čísla $7^{1988}$, vyšlo by nám obdobným výpočtom číslo 1; hľadané dvojčíslie by potom bolo 01.

**Úloha 5.6.** Nájdite najmenšie celé kladné číslo $n$ také, že

$$327^{n+1} \equiv 327 \pmod{1000} .$$

*Riešenie.* Pretože $D(327, 1000) = 1$, je uvedená kongruencia ekvivalentná s kongruenciou

$$327^n \equiv 1 \pmod{1000} .$$

Táto kongruencia je zasa ekvivalentná so systémom kongruencií

$$327^n \equiv 1 \pmod{8}, \quad 327^n \equiv 1 \pmod{125} ;$$

tu sme využili rozpis $1000 = 8 . 125$, pričom $D(8, 125) = 1$. Druhá kongruencia dáva

$$77^n \equiv 1 \pmod{125} . \tag{1}$$

Pretože $\varphi(125) = 100$, podľa Eulerovej vety dostávame

$$77^{100} \equiv 1 \pmod{125}.$$

Preto najmenšie kladné riešenie $n$ kongruencie (1) je deliteľom čísla 100. Číslo $n$ však nie je deliteľom čísla 20 ani čísla 50, pretože (počítame modulo 125)

$$77^{20} = (75 + 2)^{20} \equiv \binom{20}{1} . 75 . 2^{19} + 2^{20} \equiv 0 + (2^{10})^2 \equiv$$

$$\equiv 24^2 \equiv 76 \not\equiv 1 \pmod{125},$$

$$77^{50} = (75 + 2)^{50} \equiv \binom{50}{1} . 75 . 2^{49} + 2^{50} \equiv 0 + (2^{10})^5 \equiv$$

$$\equiv 24^5 \equiv (25 - 1)^5 \equiv + \binom{5}{1} . 25 . 1^4 - 1^5 \equiv$$

$$\equiv -1 \not\equiv 1 \pmod{125}.$$

Teda najmenšie kladné riešenie kongruencie (1) je $n = 100$, a to zrejme vyhovuje aj prvej kongruencii (tej vyhovuje každé párne prirodzené $n$). Teda $n = 100$ je aj riešením úlohy. □

**Úloha 5.7.** Dokážte, že neexistuje celé kladné číslo $n$ také, že $7516^{n+1}$ končí štvorčíslím 7516.

*Riešenie.* Platí $4 \mid 7516$, $8 \mid 4^2$, a teda $8 \mid 7516^{n+1}$ pre každé celé kladné $n$. Avšak žiadne číslo končiace štvorčíslím 7516 nie je deliteľné ôsmimi. □

**Úloha 5.8.** Určite posledných šesť číslic čísla $A = 5^{678^{901^{234}}}$.

*Riešenie.* Treba určiť číslo $A$ MOD $10^6$, a na to najprv určíme $A$ MOD $2^6$, $A$ MOD $5^6$. Pretože $D(5, 64) = 1$

a $\varphi(64) = 32$, podľa Eulerovej vety platí $5^{32} \equiv 1 \pmod{64}$, a potom zrejme aj $A \equiv 1 \pmod{64}$. Ďalej zrejme platí $5^6 | A$, a preto pre $B = A$ MOD $10^7$ platí

$$B \equiv 1 \pmod{64}, \qquad B \equiv 0 \pmod{15625}$$

(mocniny $2^6$, $5^6$ sme vypočítali). Tieto kongruencie spolu s nerovnosťou $0 \leqq B < 10^6$ jednoznačne určujú $B$. Z druhej kongruencie vieme $B = 15625x$ pre nejaké celé číslo $x$; ľahko zistíme $0 \leqq x < 64$. Dosadením do prvej kongruencie dostávame

$$\begin{aligned} 15625x &\equiv 1 \pmod{64}, \\ 9x &\equiv 1 \pmod{64}, \\ -63x &\equiv -7 \pmod{64}, \\ x &\equiv 57 \pmod{64}, \end{aligned}$$

teda vzhľadom na nerovnosť pre $x$ dostávame $x = 57$, a potom

$$B = 57.15625 = 890625.$$

Teda posledné šesťčíslie čísla $A$ je 890625. □

Kongruenciu pre $x$ sme mohli tiež upraviť takto

$$\begin{aligned} 5^6x &\equiv 1 \pmod{64}, \\ x &\equiv 5^{26} \pmod{64}, \\ 5^6x &\equiv 5^{32} \pmod{10^6}. \end{aligned}$$

Pretože $B = 5^6x$, platí

$$\begin{aligned} B &= 5^{32}\text{MOD } 10^6 = 25^{16}\text{MOD } 10^6 = \\ &= 625^8\text{MOD } 10^6 = 390\,625^4\text{MOD } 10^6 = \\ &= 890\,625^2\text{MOD } 10^6 = 890\,625. \end{aligned}$$

V poslednom výpočte sme potrebovali päť umocnení na druhú, pretože $32 = 2^5$. Jedno (a to posledné) umocnenie sme si mohli ušetriť pomocou vzťahu $5^{16} \equiv 1 \pmod{64}$, ktorý síce nevyplýva z Eulerovej vety, ale ľahko ho dostaneme napríklad z binomického rozvoja pre $(4 + 1)^{16}$.

**Úloha 5.9.** Určte posledné trojčíslie čísla $A = 9^{9^9}$.

*Riešenie I* (s tabuľkami). Pretože $\varphi(1000) = 400$, budeme potrebovať $9^9$ MOD 400. Priamo z tabuliek zistíme, že posledné štvorčíslice čísla $9^9$ je 0489, teda $9^9$ MOD 400 = 89. Potom platí (počítame modulo 1000)

$$A \equiv 9^{89} = 3^{178} = 3^3.(3^{35})^5 \equiv 27.707^5 =$$
$$= 27.101^5.7^5 \equiv 27.501.807 \equiv 27.307 \equiv$$
$$\equiv 289 \pmod{1000}.$$

Teda $A$ MOD 1000 = 289, čo je hľadané posledné trojčíslie. □

Poznamenajme, že namiesto $\varphi(1000) = 400$ sme mohli uvažovať $\lambda(1000) = 100$, teda $9^{100} \equiv 1 \pmod{1000}$. Exponent 89 by sme tým však neznížili.

*Riešenie II*. Najprv zistíme $9^9$MOD 100.
Počítame modulo 100 a používame binomickú vetu, pričom násobky 100 už vynechávame.

$$9^9 = (10 - 1)^9 \equiv \binom{9}{1}.10 - 1 = 89 \pmod{100}.$$

Teraz ľahko zjistíme poslednú číslicu čísla $\binom{9^9}{2}$, pretože (počítame modulo 10)

$$\binom{9^9}{2} = 9^9.\frac{9^9 - 1}{2} \equiv 9.4 \equiv 6 \pmod{10}.$$

Ďalej znova používame binomickú vetu, ale počítame modulo 1000:

$$9^{9^9} = (10 - 1)^{9^9} \equiv -\binom{9^9}{2} . 100 + \binom{9^9}{1} . 10 - 1 \equiv$$

$$\equiv -600 + 890 - 1 \equiv 289 \pmod{1000}.$$

Teda posledné trojčíslie čísla $9^{9^9}$ je 289. □

Iný možný postup by bol určiť, že

$$A \text{ MOD } 125 = 39, \qquad A \text{ MOD } 8 = 1$$

a pomocou týchto hodnôt určiť $A$ MOD 1000.

**Úloha 5.10.** Určte posledné trojčíslie čísla $B = 8^{8^8}$.

*Riešenie.* Využijeme rozklad $1000 = 125 . 8$. Aby sme mohli určiť $B$ MOD 125, určíme najskôr $8^8$MOD 100. Platí (počítame modulo 100)

$$8^8 = 64^4 = 4\,096^2 \equiv (-4)^2 = 16 \pmod{100}.$$

Preto (teraz počítame modulo 125)

$$B \equiv 8^{8^8 \text{ MOD } 100} = 8^{16} = 2^{48} = 256^6 \equiv 6^6 =$$

$$= 216^2 \equiv (-34)^2 = 1\,156 \equiv 31 \pmod{125}.$$

Potom platí

$$B \text{ MOD } 1000 = 31 + k . 125$$

pre nejaké celé číslo $k$; zrejme $0 \leqq k \leqq 7$. Pretože

$$(B \text{ MOD } 1000) \text{ MOD } 8 = B \text{ MOD } 8 = 0,$$

máme

$$31 + k . 125 \equiv 0 \pmod 8,$$

$$5k \equiv 1 \pmod 8,$$

$$k \equiv 5 \pmod 8,$$

a teda $k = 5$. Potom

$$B \text{ MOD } 1000 = 31 + 5 . 125 = 656.$$

Teda hľadané posledné trojčíslie čísla $B$ je 656. □

**Úloha 5.11.** Určte posledné trojčíslie čísla $C = 7^{8^9}$.

*Riešenie.* Budeme počítať $C$ MOD 1000, pričom využijeme Eulerovu vetu pre moduly 8 a 125 a skutočnosť, že

$$nsn(\varphi(8), \varphi(125)) = 100.$$

Počítajme modulo 1000 ; platí

$$C \equiv 7^{8^9 \text{ MOD } 100} = 7^{512^3 \text{ MOD } 100} = 7^{12^3 \text{ MOD } 100} = 7^{28} =$$

$$= 2401^7 \equiv (400 + 1)^7 \equiv 7 . 400 + 1 \equiv 801 \pmod{1000}.$$

Teda číslo $C$ končí trojčíslím 801. □

**Úloha 5.12.** Určte poslednú číslicu sedmičkového zápisu čísla $A = 10^{10^{10}}$.

*Riešenie.* Máme vlastne určiť $A$ MOD 7. Pri počítaní modulo 7 platí

$$A \equiv 3^{10^{10}} \equiv 3^{10^{10} \text{ MOD } 6} = 3^4 \equiv 4 \pmod 7.$$

Teda hľadaná posledná číslica je štvorka. □

Určenie poslednej číslice z-adického zápisu čísla A pre ostatné základy menšie než 10 je ešte ľahšie, a čitateľ by to mal bez ťažkostí spraviť i spamäti.

**Úloha 5.13.** Určte posledné trojčíslie deviatkového zápisu čísla $A = 10^{10^{10}}$.

*Riešenie.* Budeme počítať modulo $9^3$ a používať binomickú vetu; zrejmé násobky $9^3$ budeme ihneď vynechávať, a využijeme tiež $9\mid(10^{10}-1)$, tedy aj $9\left|\binom{10^{10}}{2}\right.$.

$$A=(9+1)^{10^{10}}\equiv\binom{10^{10}}{2}.9^2+\binom{10^{10}}{1}.9+1\equiv$$

$$\equiv 0+10^{10}.9+1=(9+1)^{10}.9+1\equiv$$

$$\equiv(10.9+1).9+1\equiv 1.9^2+1.9+1\ (\mathrm{mod}\ 9^3).$$

Teda posledné trojčíslie deviatkového zápisu čísla $A$ je 111. □

**Úloha 5.14.** Určte posledné trojčíslie sedmičkového zápisu čísla $A=10^{10^{10}}$.

*Riešenie.* Budeme počítať modulo $7^3=343$ a využívať Eulerovu vetu. Počas výpočtu používame dekadické zápisy. Naprv určíme $10^{10}\mathrm{MOD}\,\varphi(343)$, t. j. $10^{10}\mathrm{MOD}$ 294. Využijeme rozklad $294=6.49$. Platí

$$10^{10}\mathrm{MOD}\ 49=100^5\mathrm{MOD}\ 49=2^5\mathrm{MOD}\ 49=32,$$

a preto $10^{10}\mathrm{MOD}\ 294=32+49\,k$ pre vhodné celé číslo $k$. Pretože $10^{10}\mathrm{MOD}\ 6=4$, má byť aj $(32+49k)\mathrm{MOD}\ 6=4$, teda $(2+k)\ \mathrm{MOD}\ 6=4$, odkiaľ vyplýva $k\equiv 2$ (mod 6).
Pretože však zrejme $0\leqq k\leqq 5$, máme $k=2$ a

$$10^{10}\mathrm{MOD}\ 294=32+49.2=130.$$

Teraz počítajme modulo 343. Platí

$$A\equiv 10^{10^{10}\mathrm{MOD}\ 294}=10^{130}=100^{65}=4.8^{21}.50^{65}=$$

$$=4.(7+1)^{21}.(49+1)^{65}\equiv 4.\left(\binom{21}{2}.7^2+21.7+1\right).$$

$$.(65.49 + 1) \equiv 4.(0 + 3.7^2 + 1).(2.7^2 + 1) \equiv$$
$$\equiv 4.(5.7^2 + 1) = 20.7^2 + 4 \equiv$$
$$\equiv 6.7^2 + 0.7 + 4 \pmod{343}.$$

Teda posledné trojčíslie sedmičkového zápisu čísla $A$ je 604. $\square$

# 6. DELITELNOSŤ

**Úloha 6.1.** Dokážte, že

$$43 | 3^{3^3} + 4^{4^4}.$$

*Riešenie.* Výpočtom podľa modulu 43 s využitím malej Fermatovej vety dostávame

$$3^{3^3} + 4^{4^4} \equiv 3^{27} + 4^{256 \text{ MOD } 42} = 3^3 . 81^6 + 4^4 \equiv$$

$$\equiv 3^3 . (-5)^6 + 256 \equiv 75^3 - 2 \equiv (-11)^3 - 2 =$$

$$= -11 . 121 - 2 \equiv -11 . (-8) - 2 = 86 \equiv$$

$$\equiv 0 \pmod{43},$$

teda $43 | 3^{3^3} + 4^{4^4}$. □

**Úloha 6.2.** Dokážte, že

$$73 | 9^{9^9} + 10^{10^{10}}.$$

*Riešenie.* Použijeme malú Fermatovu vetu. Dopredu si vypočítame čísla

$$u = 9^9 \text{ MOD } 72, \quad v = 10^{10} \text{ MOD } 72,$$

pričom využijeme rozklad $72 = 8 . 9$ a nesúdeliteľnosť čísel 8, 9. Platí

$$u \text{ MOD } 8 = 9^9 \text{ MOD } 8 = 1, \; u \text{ MOD } 9 = 9^9 \text{ MOD } 9 = 0.$$

Z druhého vzťahu (a z nerovnosti $0 \leqq u < 72$) vyplýva $u = 9k$ pre nejaké celé číslo $k$, $0 \leqq k < 8$. Dosadením do prvého vzťahu dostávame $9k \text{ MOD } 8 = 1$, $k \equiv 1 (\text{mod } 8)$, a teda $k = 1$. Preto $u = 9$. Pre číslo $v$ platí

$$v \text{ MOD } 8 = 10^{10} \text{MOD } 8 = 0,$$

$$v \text{ MOD } 9 = 10^{10} \text{ MOD } 9 = 1.$$

Z prvého vzťahu (a z nerovnosti $0 \leqq v < 72$) vyplýva $v = 8k$ pre nejaké celé $k$, $0 \leqq k < 9$. Dosadením do druhého vzťahu dostávame

$$8k \text{ MOD } 9 = 1, \quad 8k \equiv 1 \ (\text{mod } 9), k \equiv 8 \ (\text{mod } 9),$$

a teda $k = 8$, $v = 64$.

Teraz budeme počítať modulo 73

$$9^{9^9} + 10^{10^{10}} \equiv 9^{9^9 \text{MOD } 72} + 10^{10^{10} \text{MOD } 72} =$$

$$= 9^9 + 10^{64} = 9^9 + 100^{32} \equiv 9^9 + 27^{32} =$$

$$= 729^3 + 729^{16} \equiv (-1)^3 + (-1)^{16} \equiv 0 \ (\text{mod } 73),$$

a teda $73 | 9^{9^9} + 10^{10^{10}}$. □

Odteraz nebudeme výpočty obdobné výpočtom čísel $u$, $v$ rozpisovať tak podrobne. Poznamenávame, že $u$ sme mohli ľahšie vypočítať využitím vzťahu $9^2 \equiv 9 \ (\text{mod } 72)$; len z inštruktívnych dôvodov sme dali prednosť všeobecne použiteľnému postupu.

**Úloha 6.3.** Dokážte, že

$$89 | 11^{11^{11}} + 12^{12^{12}}.$$

*Riešenie.* Platí

$$11^{11} \text{ MOD } 8 = 3, \quad 11^{11} \text{ MOD } 11 = 0,$$

odkiaľ ľahko zistíme $11^{11} \text{ MOD } 88 = 11$.

Obdobne

$$12^{12}\ \mathrm{MOD}\ 8 = 0, \quad 12^{12}\ \mathrm{MOD}\ 11 = 1,$$

odkiaľ vyplýva $12^{12}\ \mathrm{MOD}\ 88 = 56$. Ďalej počítajme modulo 89; platí

$$11^{11^{11}} + 12^{12^{12}} \equiv 11^{11^{11}\,\mathrm{MOD}\,88} + 12^{12^{12}\,\mathrm{MOD}\,88} =$$
$$= 11^{11} + 12^{56} = 11^{11} + 144^{28} \equiv 11^{11} + 55^{28} =$$
$$= 11^{11}.(1 + 5^{28}.11^{17}) = 11^{11}.(1 + 625^{7}.11.121^{8}) \equiv$$
$$\equiv 11^{11}.(1 + 2^{7}.11.32^{8}) \equiv 11^{11}.(1 + 39.11.256^{5}) \equiv$$
$$\equiv 11^{11}.(1 + 39.11.(-11)^{5}) = 11^{11}.(1 - 39.11^{6}) =$$
$$= 11^{11}.(1 - 39.1331^{2}) \equiv 11^{11}.(1 - 39.(-4)^{2}) =$$
$$= 11^{11}.(-623) \equiv 11^{11}.0 = 0 \pmod{89}.$$

Teda platí $89 | 11^{11^{11}} + 12^{12^{12}}$. □

**Úloha 6.4.** Dokážte, že

$$11 | 13^{13^{13}} + 14^{14^{14}}.$$

*Riešenie.* Počítajme modulo 11, s využitím malej Fermatovej vety:

$$13^{13^{13}} + 14^{14^{14}} \equiv 13^{13^{13}\,\mathrm{MOD}\,10} + 14^{14^{14}\,\mathrm{MOD}\,10} =$$
$$= 13^{3} + 14^{6} \equiv 2^{3} + 3^{6} \equiv 8 + 5^{2} \equiv 8 + 3 \equiv$$
$$\equiv 0 \pmod{11},$$

a preto $11 | 13^{13^{13}} + 14^{14^{14}}$. □

**Úloha 6.5.** Dokážte, že

$$111 | 10^{10^{10}} + 11^{11^{11}}.$$

*Riešenie.* Označme $A$ číslo vpravo od znaku deliteľnosti. Pretože $111 = 3.37$ (a 3, 37 sú prvočísla, teda $D(3, 37) = 1$), stačí dokazovať $3|A$, $37|A$. Najprv počítajme modulo 3. Platí

$$10^{10^{10}} + 11^{11^{11}} \equiv 1^{10^{10} \mathrm{MOD}\, 2} + 2^{11^{11} \mathrm{MOD}\, 2} =$$

$$= 1 + 2 \equiv 0 \pmod 3,$$

a preto $3|A$. Pre prvočíslo 37 najprv uvážme, že platí

$$10^{10} \mathrm{MOD}\, 9 = 1, \qquad 10^{10} \mathrm{MOD}\, 4 = 0,$$

a preto $10^{10} \mathrm{MOD}\, 36 = 28$. Obdobne

$$11^{11} \mathrm{MOD}\, 9 = 2^{11 \mathrm{MOD}\, 6} \mathrm{MOD}\, 9 = 5,$$

$$11^{11} \mathrm{MOD}\, 4 = 3,$$

a preto $11^{11} \mathrm{MOD}\, 36 = 23$. Teraz počítajme modulo 37; platí

$$10^{10^{10}} + 11^{11^{11}} \equiv 10^{10^{10} \mathrm{MOD}\, 36} + 11^{11^{11} \mathrm{MOD}\, 36} =$$

$$= 10^{28} + 11^{23} = 10.1000^{9} + 11.121^{11} \equiv$$

$$\equiv 10.1^{9} + 11.10^{11} = 10 + 1100.1000^{3} \equiv$$

$$\equiv 10 + 1100 = 1110 \equiv 0 \pmod{37}.$$

Preto platí $37|A$. Predtým sme zistili $3|A$, spolu teda máme $111|A$. □

**Úloha 6.6.** Dokážte, že

$$483 | 4^{4^4} + 5^{5^5}.$$

*Riešenie.* Označme $A$ číslo vpravo od znaku deliteľnosti. Pretože $483 = 21.23 = 3.7.23$ a 3, 7, 23 sú prvočísla, stačí dokázať $3|A$, $7|A$, $23|A$. Výpočet modulo 3 dáva

$$A \equiv 1^{4^4} + 2^{5^5 \mathrm{MOD}\, 2} = 1 + 2 \equiv 0 \pmod 3.$$

Výpočet modulo 7 dáva

$$A \equiv 4^{4^4 \mathrm{MOD}\, 6} + 5^{5^5 \mathrm{MOD}\, 6} = 4^4 + 5^5 \equiv$$
$$\equiv (-3)^4 - (-2)^5 = 81 - 32 = 49 \equiv 0 \pmod 7.$$

Nakoniec, výpočet modulo 23 dáva

$$A \equiv 4^{4^4 \mathrm{MOD}\, 22} + 5^{5^5 \mathrm{MOD}\, 22} = 4^{14} + 5^{5.25^2 \mathrm{MOD}\, 22} =$$
$$= 4^{14} + 5^{5.3^2 \mathrm{MOD}\, 22} \equiv 2^{28 \mathrm{MOD}\, 22} + 5^{45 \mathrm{MOD}\, 22} =$$
$$= 2^6 + 5^1 = 64 + 5 = 69 \equiv 0 \pmod{23}.$$

Preto platí $3|A$, $7|A$, $23|A$, a teda aj $3.7.23 = 483|A$. □

**Úloha 6.7.** Dokážte, že

$$17 \nmid 2^{2^2} + 3^{3^3}.$$

*Riešenie.* Počítajme modulo 17, s využitím malej Fermatovej vety. Platí

$$2^{2^2} + 3^{3^3} \equiv 2^4 + 3^{27 \mathrm{MOD}\, 16} = 16 + 3^{11} =$$
$$= 16 + 9.27^3 \equiv 16 + 9.10^3 = 16 + 90.100 \equiv$$
$$\equiv 16 + 5.(-2) = 6 \pmod{17},$$

teda $17 \nmid 2^{2^2} + 3^{3^3}$. □

**Úloha 6.8.** Dokážte, že

$$3^{3^3} + 4^{4^4} \nmid 4^{4^4} + 5^{5^5}.$$

*Riešenie.* V úlohe 6.1 sme zistili, že platí $43|3^{3^3} + 4^{4^4}$. Teraz ukážme, že $43 \nmid 4^{4^4} + 5^{5^5}$.
Najprv zistíme

$$5^5 \mathrm{\ MOD\ } 42 = 125.25 \mathrm{\ MOD\ } 42 =$$
$$= (-1).25 \mathrm{\ MOD\ } 42 = -25 \mathrm{\ MOD\ } 42 = 17.$$

Teraz počítajme modulo 43 a s využitím malej Fermatovej vety. Platí

$$4^{4^4} + 5^{5^5} \equiv 4^{4^4 \mathrm{MOD}\, 42} + 5^{5^5 \mathrm{MOD}\, 42} = 4^4 + 5^{17} =$$
$$= 256 + 25.125^5 \equiv 256 + 25.(-4)^5 \equiv$$
$$\equiv 256.(1 - 25.4) \equiv 26\ (\mathrm{MOD}\ 43).$$

Teda $43 \nmid 4^{4^4} + 5^{5^5}$, a tým skôr $3^{3^3} + 4^{4^4} \nmid 4^{4^4} + 5^{5^5}$. □

Samozrejme, úplné riešenie úlohy 6.8 by sa nemalo odvolávať na úlohu 6.1. Prvočíslo $p = 43$ sme mohli „uhádnuť", resp. nájsť postupným výpočtom čísel $\left(3^{3^3} + 4^{4^4}\right) \mathrm{MOD}\, p$, ale výpočty pre $p < 43$ nemusíme v konečnom riešení uvádzať. Uviedli by sme len výpočet pre $p = 43$, t.j. v podstate odpísali riešenie úlohy 6.1.

**Úloha 6.9.** Dokážte, že

$$8^{8^8} + 9^{9^9} \nmid 9^{9^9} + 10^{10^{10}}.$$

*Riešenie.* Počítajme ľavú i pravú stranu podľa modulu 5, s využitím malej Fermatovej vety. Platí

$$8^{8^8} + 9^{9^9} \equiv 3^{8^8 \mathrm{MOD}\, 4} + 4^{9^9 \mathrm{MOD}\, 4} = 3^0 + 4^1 =$$
$$= 1 + 4 \equiv 0\ (\mathrm{mod}\ 5),$$
$$9^{9^9} + 10^{10^{10}} \equiv 9^{9^9} \equiv 4^1 = 4\ (\mathrm{mod}\ 5).$$

Teda platí $5 \mid 8^{8^8} + 9^{9^9}$, $5 \nmid 9^{9^9} + 10^{10^{10}}$, a preto

$$8^{8^8} + 9^{9^9} \nmid 9^{9^9} + 10^{10^{10}}. \ \square$$

Niekoľko nasledujúcich úloh nechávame čitateľovi ako cvičenie.

**Úloha 6.10.** Dokážte, že

$$13^{13^{13}} + 14^{14^{14}} \nmid 14^{14^{14}} + 15^{15^{15}}.$$

**Úloha 6.11.** Dokážte, že

$$12^{12^{12}} + 13^{13^{13}} \nmid 13^{13^{13}} + 14^{14^{14}}.$$

**Úloha 6.12.** Dokážte, že

$$11^{11^{11}} + 12^{12^{12}} \nmid 12^{12^{12}} + 13^{13^{13}}.$$

**Úloha 6.13.** Dokážte, že

$$5^{5^5} + 6^{6^6} \nmid 6^{6^6} + 7^{7^7}.$$

**Úloha 6.14.** Dokážte, že

$$6^{6^6} + 7^{7^7} \nmid 7^{7^7} + 8^{8^8}.$$

Posledné tri úlohy neodporúčame riešiť bez použitia samočinného počítača. Ešte viac by sa takéto odporúčanie týkalo nasledujúcej úlohy, keby sme pre ňu nemali celkom iný postup.

**Úloha 6.15.** Dokážte, že

$$7^{7^7} + 8^{8^8} \nmid 8^{8^8} + 9^{9^9}.$$

*Riešenie.* Číslo vpravo možno písať v tvare $a^2 + b^2$, kde $a = 8^{4 \cdot 8^7}$, $b = 3^{9^9}$ sú nesúdeliteľné celé čísla; preto nemá žiadneho prvočiniteľa tvaru $4k + 3$. Číslo vľavo však je tvaru $4k + 3$, a preto má aspoň jedného prvočiniteľa tohto tvaru. (Prvočíslo 2 neprichádza do úvahy, a súčin ľubovoľného počtu prvočísel tvaru $4k + 1$ je tiež tvaru $4k + 1$.) Preto platí

$$7^{7^7} + 8^{8^8} \nmid 8^{8^8} + 9^{9^9}. \quad \square$$

Rovnakým postupom možno vyriešiť aj nasledujúce dve úlohy.

**Úloha 6.16.** Dokážte, že

$$2^{2^2} + 3^{3^3} \nmid 9^{9^9} + 10^{10^{10}}.$$

**Úloha 6.17.** Dokážte, že

$$6^{6^6} + 7^{7^7} \nmid 8^{8^8} + 9^{9^9}.$$

**Úloha 6.18.** Dokážte, že

$$6^{6^6} + 8^{8^8} \nmid 7^{7^7} + 9^{9^9}.$$

*Riešenie.* Označme $A$ číslo vľavo, $B$ číslo vpravo od znaku $\nmid$. Zrejme $2^{6^6} | A$, a teda stačí dokázať $2^{6^6} \nmid B$. Na to počítajme podľa modulu 128

$$7^{7^7} = (8 - 1)^{7^7} \equiv -\frac{7^7.(7^7 - 1)}{2}.8^2 + 7^7.8 - 1 \equiv$$

$$\equiv -64 + (7^7 \text{ MOD } 16).8 - 1 = -64 +$$

$$+ (7.49^3 \text{ MOD } 16).8 - 1 = -64 + 7.8 - 1 =$$

$$= -9 \pmod{128},$$

$$9^{9^9} = (8 - 1)^{9^9} \equiv \frac{9^9.(9^9 - 1)}{2}.8^2 + 9^9.8 + 1 \equiv$$

$$\equiv 0.64 + (9^9 \text{ MOD } 16).8 + 1 = (9.81^4 \text{ MOD } 16).$$

$$.8 + 1 = 9.8 + 1 = 73 \pmod{128}.$$

Preto platí

$$B \equiv -9 + 73 = 64 \pmod{128},$$

teda $128 \nmid B$, a tým skôr $2^{6^6} \nmid B$, teda aj $A \nmid B$. □

# 7. MOCNINY

Slovo „mocnina“ v textoch úloh tejto kapitoly treba chápať ako „mocnina, ktorej základ je prirodzené číslo a exponent je prirodzené číslo väčšie než 1“. Teda napríklad spomedzi čísel od 1 do 20 mocninami sú 1, 4, 8, 9, 16. Pripomíname, že obdobne sa používa slovo „štvorec“ pre druhú mocninu (a v ruštine a angličtine aj ekvivalent slova „kocka“ pre tretiu mocninu; u nás to znie trochu neobvykle). Vo väčšine úloh pôjde o dôkaz toho, že nejaké veľké číslo nie je mocninou.

**Úloha 7.1.** Nech číslo

$$A = 100101102 \ldots 998999$$

vznikne tak, že napíšeme za sebou všetky trojciferné čísla v poradí podľa veľkosti. Dokážte, že $A$ nie je mocnina.

*Riešenie.* Určme najprv $A$ MOD 999. Na to stačí $A$ rozdeliť na 3-ciferné skupiny (od konca, ale tu na tom nezáleží), a určiť ich súčet $S$. Potom platí $A$ MOD 999 = = $S$ MOD 999; ak bude $S$ veľké, možno postup zopakovať. Takto dostávame

$$A \text{ MOD } 999 = (450.(100 + 999)) \text{MOD } 999 = 45$$

Pretože $999 = 27.37$, dostaneme odtiaľ ľahko

$$A \text{ MOD } 27 = 18.$$

Odtiaľ vidno, že $9|A$, $27\nmid A$, teda exponent prvočísla 3 v rozklade $A$ je rovný dvom. Preto $A$ nemôže byť vyššou než druhou mocninou. Avšak zrejme platí $A \equiv 3 \pmod 4$, teda $A$ nie je ani štvorec. □

**Úloha 7.2.** Nech číslo

$$B = 12345 \ldots 999910000$$

vznikne tak, že napíšeme za sebou všetky prirodzené čísla od 1 po 10000 v poradí podľa veľkosti. Dokážte, že $B$ nie je mocnina.

*Riešenie.* Keďže $B$ končí štyrmi nulami, tak keby $B$ bolo mocninou, bolo by aj štvorcom (každá štvrtá mocnina je súčasne štvorec). Potom by aj číslo $B/10000$ bolo štvorcom, ale to nie je možné, pretože

$$B/10000 \equiv 3 \pmod 4. \quad \square$$

**Úloha 7.3.** Nech číslo

$$C = 1000010001 \ldots 9999899999$$

vznikne tak, že napíšeme za sebou všetky päťmiestne čísla vo vzostupnom poradí. Dokážte, že číslo $C$ nie je mocnina.

*Riešenie.* Určme najprv $C$ MOD 999. Platí

$$C = \sum_{i=10000}^{99999} i \, . \, 10^{5.(99999-i)}.$$

Každé päťmiestne číslo $i$ možno jednoznačne vyjadriť v tvare $10000 + k + 3j$, $0 \leqq k \leqq 2$, $0 \leqq j \leqq 29999$, a preto

$$C = \sum_{k=0}^{2} \sum_{j=0}^{29999} (10000 + k + 3j) \, . \, 10^{5.(89999-k-3j)}.$$

Pretože $10^3 \equiv 1 \pmod{999}$, možno pri určovaní $C$ MOD 999 exponenty (so základom 10) znížiť o násobok 3. Pretože

$$5.(89999 - k - 3j) \equiv 2.(2 - k) \pmod{3},$$

môžeme dosiahnuť, že exponenty nebudú závisieť od $j$ a príslušné činitele možno vybrať pred druhú sumu. Tak dostaneme

$$C \equiv \sum_{k=0}^{2} 10^{2.(2-k)} . \sum_{j=0}^{29999} (10 + k + 3j) \pmod{999},$$

$$C \equiv \sum_{k=0}^{2} 10^{4-2k} . (30000.(10 + k) + 3.29999.15000) \pmod{999},$$

$$C \equiv \sum_{k=0}^{2} 10^{4-2k} . (300 + 30k + 3.29.15) \pmod{999}.$$

Ďalej počítajme modulo 999.

$$C \equiv \sum_{k=0}^{2} 10^{4-2k} . (300 + 30k + 1305) \equiv$$

$$\equiv 10.606 + 100.(606 + 30) + 1.(606 + 60) =$$

$$= 6060 + 63600 + 666 \equiv 66 + 663 + 666 =$$

$$= 1395 \equiv 396 \pmod{999}.$$

Teda zistili sme $C$ MOD 999 = 396.
Pretože $27 | 999$, platí

$$C \text{ MOD } 27 = 396 \text{ MOD } 27 = 18.$$

Z toho vyplýva $3^2 | C$, $3^3 \nmid C$, teda $C$ nemôže byť vyššou než druhou mocninou. Štvorcom však tiež nie je, pretože $C \equiv 3 \pmod{4}$. □

**Úloha 7.4.** Nech číslo

$$D = 10001001 \dots 99989999$$

vznikne tak, že napíšeme za sebou všetky štvormiestne prirodzené čísla vo vzostupnom poradí. Dokážte, že $D$ nie je mocnina.

*Riešenie.* Určíme $D$ MOD 999. Platí

$$D = \sum_{i=1000}^{9999} i \,.\, 10^{4.(9999-i)}.$$

Ak každé $i$ vyjadríme v tvare $1000 + k + 3j$, $0 \leqq k \leqq \leqq 2$, dostaneme

$$D = \sum_{k=0}^{2} \sum_{j=0}^{2999} (1000 + k + 3j) \,.\, 10^{4.(8999-k-3j)}.$$

Znížením exponentov o násobky troch a vybratím činiteľa nezávislého od $j$ pred druhú sumu dostaneme

$$D \equiv \sum_{k=0}^{2} 10^{2-k} \,.\, \sum_{j=0}^{2999} (1 + k + 3j) \quad (\mathrm{mod}\ 999).$$

Ďalej počítajme modulo 999:

$$D \equiv \sum_{k=0}^{2} 10^{2-k} \,.\, (3000 + 3000k + 3 \,.\, 2999 \,.\, 1500) \equiv$$

$$\equiv \sum_{k=0}^{2} 10^{2-k} (12 + 3k) = 1200 + 150 + 18 \equiv$$

$$\equiv 369 \ (\mathrm{mod}\ 999).$$

Pretože $27 | 999$, platí $D$ MOD $27 = 369$ MOD $27 = 18$, a preto $3^2 | D$, $3^3 \nmid D$. Teda $D$ nemôže byť vyššia než druhá mocnina. $D$ však nie je ani štvorec, pretože $D \equiv \equiv 3 \ (\mathrm{mod}\ 4)$. $\square$

**Úloha 7.5.** Nech číslo $A$ vznikne tak, že napíšeme za sebou dekadické zápisy prirodzených čísel od 1 po 6666 v ľubovoľnom poradí (ale každé práve raz). Dokážte, že $A$ nie je mocnina.

*Riešenie.* Pretože $10^k \equiv 1 \pmod 9$ pre každé celé nezáporné $k$, platí (počítame modulo 9)

$$A \equiv \sum_{i=1}^{6666} i = 6667 . 3333 \equiv 7 . 3 \equiv 3 \pmod 9.$$

Preto $3|A$, $3^2 \nmid A$, teda $A$ nie je mocninou. □

**Úloha 7.6.** Dokážte, že pri žiadnej voľbe znamienok nie je číslo

$$X = 60^{60^{60}} \pm 58^{58^{58}} \pm 56^{56^{56}} \pm \ldots \pm 4^{4^4} \pm 2^{2^2}$$

mocnina.

*Riešenie.* Platí $2^4|X$, $2^5 \nmid X$. Teda keby číslo $X$ bolo mocninou, bolo by aj štvorcom. Aby sme ukázali, že $X$ nie je štvorcom, označme $Y = 60^{30 \cdot 60^{59}}$.

Zrejme $X \neq Y^2$ (napríklad preto, že $32 \nmid X$ a $32 | Y^2$). Ak teraz ukážeme, že $X$ sa nachádza medzi $(Y - 1)^2$ a $(Y + 1)^2$, bude to znamenať, že $X$ nie je štvorec, pretože jediný štvorec medzi týmito číslami je $Y^2$. Na to odhadujme:

$$|X - Y^2| \leqq 58^{58^{58}} + 56^{56^{56}} + \ldots + 4^{4^4} + 2^{2^2} <$$
$$< 29 . 60^{58^{58}} < Y.$$

Odtiaľ už ľahko vyplýva

$$(Y - 1)^2 < Y^2 - Y < X < Y^2 + Y < (Y + 1)^2,$$

teda $X$ naozaj nie je štvorec. Podľa úvahy na začiatku riešenia potom $X$ nie je mocnina. □

**Úloha 7.7.** Dokážte, že číslo

$$B = 18^{17^{19}} + 18^{19^{17}}$$

nie je mocnina.

*Riešenie.* Pretože $17^{19} > 19^{17}$, možno číslo $B$ napísať v tvare

$$B = 18^{19^{17}}.\left(18^{17^{19}-19^{17}} + 1\right).$$

Činitele vpravo sú navzájom nesúdeliteľné. Preto keby $B$ bolo mocninou, bolo by aj devätnástou mocninou, a aj druhý činiteľ vpravo by bol devätnástou mocninou. Ukážeme však, že je deliteľný piatimi, no už nie je deliteľný $5^3$ (a tým skôr $5^{19}$).
Platí (počítame modulo 125):

$$18^{10} = (20 - 2)^{10} \equiv -\binom{10}{9}.20.2^9 + 2^{10} \equiv$$
$$\equiv 2^{10}.(-10.10 + 1) \equiv 24.26 = 25^2 - 1 \equiv$$
$$\equiv -1 \pmod{125},$$

a preto $18^{20} \equiv 1 \pmod{125}$. Preto exponent $17^{19} - 19^{17}$ budeme smieť redukovať modulo 20; urobme to dopredu (počítame modulo 20):

$$17^{19} - 19^{17} \equiv 17^{19 \text{ MOD } 4} - (-1)^{17} = 17^3 + 1 \equiv$$
$$\equiv (-3)^3 + 1 = -26 \equiv 14 \pmod{20}.$$

Preto platí (počítame modulo 125)

$$18^{17^{19}-19^{17}} + 1 \equiv 18^{14} + 1 = 18^{10}.18^4 + 1 \equiv$$
$$\equiv -324^2 + 1 \equiv -51^2 + 1 = -2601 + 1 \equiv$$
$$\equiv 25 \pmod{125}.$$

Odtiaľ vidíme, že druhý činiteľ je deliteľný $5^2$, ale nie $5^3$.

Preto tento činiteľ nemôže byť 19. mocnina, a teda $B$ nie je mocnina. □

Samozrejme, platí tiež $5^2|B$, $5^3 \nmid B$. Keby sme riešenie začali takto, zistili by sme tým, že $B$ môže byť nanajvýš druhá mocnina. Ďalej by sme mohli zistiť, že exponent dvojky v rozklade $B$ je nepárny; pritom by sme ani nepotrebovali zisťovať, či $17^{19} > 19^{17}$. Došli by sme k obdobnému sporu ako vyššie. Iná možnosť by bola vypočítať

$$B \text{ MOD } 7 = \left(18^{17^{19} \text{MOD } 6} + 18^{19^{17} \text{MOD } 6}\right) \text{MOD } 7 =$$

$$=(4^5 + 4^1) \text{ MOD } 7 = (2^{10} + 4) \text{ MOD } 7 =$$

$$= (2^4 + 4) \text{ MOD } 7 = 6.$$

Potom číslo $B$ nemôže byť štvorec, pretože 6 je kvadratický nezvyšok modulo 7.

**Úloha 7.8.** Dokážte, že číslo

$$C = 17^{18^{19}} + 19^{18^{17}}$$

nie je mocnina.

*Riešenie.* Oba sčítance v $C$ sú nepárne štvorce, a teda $C \text{ MOD } 8 = (1 + 1) \text{ MOD } 8 = 2$.
Potom $2|C$, $4 \nmid C$, a preto $C$ nemôže byť mocnina. □

Obdobným spôsobom, teda výpočtom modulo 8, možno riešiť nasledujúce dve úlohy.

**Úloha 7.9.** Dokážte, že číslo

$$17^{18^{19}} + 17^{19^{18}} + 18^{17^{19}} + 18^{19^{17}} + 19^{17^{18}} + 19^{18^{17}}$$

nie je mocnina.

**Úloha 7.10.** Dokážte, že číslo

$$3^{6^9} + 3^{9^6} + 6^{3^9} + 6^{9^3} + 9^{3^6} + 9^{6^3}$$

nie je mocnina.

**Úloha 7.11.** Dokážte, že číslo

$$D = 4^{6^8} + 4^{8^6} + 6^{4^8} + 6^{8^4} + 8^{4^6} + 8^{6^4}$$

nie je mocnina.

*Riešenie.* Najprv zistíme exponent prvočísla 2 v rozklade $D$. Exponenty prvočísla 2 v jednotlivých sčítancoch sú

$$2.6^8, 2.8^6, 4^8, 8^4, 3.4^6, 3.6^4 .$$

Z týchto čísel je najmenšie posledné; všetky ostatné sú väčšie. Preto exponent prvočísla 2 v rozklade $D$ je $3.6^4 = 3^5.2^4$; teda ak $D$ je mocninou, tak je i druhou alebo treťou mocninou. Počítajme teraz $D$ MOD 7, pričom exponenty hneď zredukujeme vzhľadom na vzťahy

$$4^3 \equiv 6^2 \equiv 8^1 \equiv 1 \pmod 7.$$

Platí

$$D \text{ MOD } 7 = (4^0 + 4^1 + 1 + 1 + 1 + 1) \text{ MOD } 7 = 2.$$

Pretože 2 je kubický nezvyšok modulo 7 (t. j.: kongruencia $x^3 \equiv 2 \pmod 7$ nemá riešenie), nemôže byť $D$ treťou mocninou. Vypočítajme ešte $D$ MOD 17. Pretože $\varphi(17) = 16$ delí exponenty všetkých šiestich sčítancov v čísle $D$ a 17 nedelí 4, 6, 8, platí

$$D \text{ MOD } 17 = (1 + 1 + 1 + 1 + 1 + 1) \text{ MOD } 17 = 6.$$

Číslo 6 je kvadratický nezvyšok modulo 17, pretože

$$6^8 = 36^4 \equiv 2^4 = 16 \not\equiv 1 \pmod{17},$$

a preto $D$ nemôže byť štvorec, teda $D$ nie je mocninou. □

V predloženom riešení sme nepočítali výrazy

$$D \text{ MOD } 3,\ D \text{ MOD } 5,\ D \text{ MOD } 11,\ D \text{ MOD } 13.$$

Pri hľadaní riešenia („na koncepte") by sme asi aj tieto výrazy vypočítali, pretože by však nevylúčili žiaden z dvoch zostávajúcich prípadov, bolo by zbytočné ich do riešenia uvádzať.

Z doterajších úloh čitateľ mohol získať dojem, že „veľké čísla" asi nie sú mocninami, ak len nie sú priamo ako mocniny zadané. Potom budú nasledujúce úlohy trochu prekvapením.

**Úloha 7.12.** Nájdite aspoň jednu trojicu po dvoch rôznych celých čísel $x$, $y$, z väčších než 1 a takých, že

$$x^{y^z} + x^{z^y}$$

je mocninou.

Pretože táto úloha má riešenie dokonca v jednociferných číslach, necháme ich nájdenie čitateľovi.

**Úloha 7.13.** Nájdite aspoň jednu deväticu po dvoch rôznych celých čísel $a$, $b$, $c$, $d$, $e$, $f$, $g$, $h$, $i$ väčších než 1 a takých, že

$$a^{b^c} + d^{e^f} = g^{h^i}.$$

*Riešenie.* Položme $g = 2^n$, kde $n = \frac{1}{9}(8^7 + 1)$; je $n = 233017$, ale nám stačí vedieť len $n \in \mathsf{P}$, $n > 4$. Ďalej položme $h = 3$, $i = 2$. Potom platí

$$g^{h^i} = (2^n)^9 = 2^{8^7+1} = 2.2^{8^7} = 2.2^{2^{21}}.$$

Čísla $a, b, c, d, e, f$ budeme voliť tak, aby

$$a^{b^c} = d^{e^f} = 2^{8^7}.$$

Platí

$$2^{2^{21}} = 2^{2 \cdot 2^{4 \cdot 5}} = 4^{16^5},\ 2^{2^{21}} = 2^{8 \cdot 2^{3 \cdot 6}} = 256^{8^6}$$

a z toho už vidno jednu z možností pre $a, b, c, d, e, f$. Všetky čísla $a$ až $i$ možno vyčítať zo vzorca

$$4^{16^5} + 256^{8^6} = (2^{233017})^{3^2}. \quad \square$$

Číslo $g$ sme pochopiteľne neuviedli v dekadickom zápise; ten by mal viac než 70 000 číslic, dal by sa nájsť len pomocou počítača a bol by aj tak celkom neprehľadný a nevhodný.

# 8. ÚLOHY S FAKTORIÁLMI

V týchto úlohách sa budú okrem iného vyskytovať faktoriály faktoriálov. Budeme ich značiť opakovaním výkričníka, bez pridávania zátvoriek. (Teda $n!!$ u nás znamená $(n!)!$.)

**Úloha 8.1.** Nájdite najväčšie prirodzené číslo $x$, pre ktoré platí

$$x!! < 10^{10^{10}}.$$

*Riešenie.* Platí

$$12!! < 10^9! < (10^9)^{10^9} = 10^{9\cdot 10^9} < 10^{10^{10}}.$$

Na druhej strane podľa Stirlingovho vzorca $n! > \left(\frac{n}{\mathrm{e}}\right)^n$, a preto

$$13!! > (4.10^9)! > (10^9)^{4\cdot 10^9} = 10^{36\cdot 10^9} > 10^{10^{10}}.$$

Teda hľadané číslo je $x = 12$. □

**Úloha 8.2.** Nájdite najväčšie prirodzené číslo $x$, pre ktoré platí

$$x!! < 30^{20^{10}}.$$

*Riešenie.* Ukážme najprv, že pre $x = 15$ už platí opačná nerovnosť; na to stačí ukázať, že

$$\log(15!!) > 20^{10}.\log 30.$$

Pretože $\log 30 < 1{,}478$ a $20^{10} = 1{,}024 . 10^{13}$, stačí dokazovať

$$\log(15!!) > 1{,}024 . 1{,}478 . 10^{13}.$$

Platí však

$$15! > 1{,}3076 . 10^{12} \quad \text{a} \quad 1{,}024 . 1{,}478 < 1{,}514,$$

teda stačí dokazovať

$$\log(1{,}3076 . 10^{12}!) > 1{,}514 . 10^{13}.$$

Zo Stirlignovho vzorca vyplýva

$$\log n! > n . \log \frac{n}{\mathrm{e}}$$

a preto

$$\log[(1{,}3076 . 10^{12})!] > 1{,}3076 . 10^{12} . \log \frac{1{,}3076 . 10^{12}}{\mathrm{e}} >$$

$$> 1{,}3076 . 10^{12} . 11{,}6821 > 1{,}52 . 10^{13} > 1{,}514 . 10^{13}.$$

Teda číslo $x = 15$ už úlohe nevyhovuje.
Pre $x = 14$ platí

$$14!! < 10^{11}! < (10^{11})^{10^{11}} = 10^{110 \cdot 10^{10}} < 10^{2^{10} \cdot 10^{10}} =$$

$$= 10^{20^{10}} < 30^{20^{10}}.$$

Hľadané číslo teda je $x = 14$. □

Dôkaz nerovnosti $x < 15$ bol oveľa náročnejší než dôkaz nerovnosti $x \geqq 14$. Je dosť pravdepodobné, že pri samostatnom riešení úlohy by čitateľ najprv našiel nerovnosti $x < 16$, $x \geqq 14$ a k správnej nerovnosti pre číslo 15 by prišiel až po niekoľkých pokusoch. Neúspešné pokusy však nie je potrebné v definitívnom riešení uvádzať.

**Úloha 8.3.** Nájdite najväčšie prirodzené číslo $x$, pre ktoré platí

$$x!! < 10^{20^{30}}.$$

*Riešenie.* Platí $\log 34! > 38{,}47$, a teda $34! > 2{,}9 . 10^{38}$, Preto

$$34!! > \left(\frac{34!}{\mathrm{e}}\right)^{34!} > (10^{38})^{2,9 \cdot 10^{38}} > 10^{10^{40}} > 10^{8^{10} \cdot 10^{30}} =$$

$$= 10^{2^{30} \cdot 10^{30}} = 10^{20^{30}},$$

a teda $x < 34$. Na druhej strane $\log 33! < 36{,}94$, teda $33! < 10^{37}$, a preto

$$33!! < 33!^{33!} < (10^{37})^{10^{37}} < 10^{10^{9} \cdot 10^{30}} < 10^{2^{30} \cdot 10^{30}} =$$

$$= 10^{20^{30}},$$

a teda $x \geqq 33$. Preto $x = 33$. □

**Úloha 8.4.** Zistite, na koľko núl končí číslo 1988!.

*Riešenie.* Exponent prvočísla 5 v rozklade čísla 1988! je

$$\left[\frac{1988}{5}\right] + \left[\frac{1988}{25}\right] + \left[\frac{1988}{125}\right] + \left[\frac{1988}{625}\right] =$$

$$= 397 + 79 + 15 + 3 = 494,$$

exponent prvočísla 2 je väčší (napríklad preto, že $\left[\frac{1988}{2}\right] > 494$). Preto 1988! je deliteľný číslom $10^{494}$, no nie $10^{495}$, a teda končí (v dekadickom zápise) 494 nulami. □

**Úloha 8.5.** Nádite najmenšie prirodzené číslo $x$ také, že

$$10^{10^{10}} \mid x!.$$

*Riešenie.* Pre $x$ musí platiť $2^{10^{10}} \mid x!$ a $5^{10^{10}} \mid x!$; využívajme najprv druhú podmienku. Exponent prvočísla 5 v čísle $x!$ je

$$\left\lfloor \frac{x}{5} \right\rfloor + \left\lfloor \frac{x}{25} \right\rfloor + \left\lfloor \frac{x}{125} \right\rfloor + \ldots < \frac{x}{5} + \frac{x}{25} + \frac{x}{125} + \\ + \ldots = \frac{x}{4},$$

a preto $\frac{x}{4} > 10^{10}$, teda $x > 4.10^{10}$. Označme $y = 4.10^{10}$ a počítajme exponent prvočísla 5 v rozklade čísla $y!$. Dostaneme ho ako súčet pätnástich čísel, z ktorých prvé je $\left\lfloor \frac{y}{5} \right\rfloor = 8.10^{9}$, a každé ďalšie vznikne z predchádzajúceho celočíselným delením piatimi. (Počet čísel nemusíme dopredu určovať; jednoducho ich prestaneme tvoriť, keď by začali vychádzať nuly.) Tento exponent vyjde 9999999997. Exponent prvočísla 5 v čísle $x!$ má byť o 3 väčší, čiže $x > y$, a v rozklade čísla

$$\frac{x!}{y!} = (y + 1).(y + 2). \ldots .(x - 1).x$$

sa musí prvočíslo 5 nachádzať s exponentom (aspoň) 3. Prvé tri činitele napravo deliteľné piatimi sú $y + 5$, $y + 10$, $y + 15$ (a pritom $25 \nmid (y + 5)$, $25 \nmid (y + 10)$, teda naozaj potrebujeme tři činitele). Preto musí byť $x \geqq y + 15 = 4.10^{10} + 15$. Pre $x = 4.10^{10} + 15$ je $5^{10^{10}} \mid x!$, a zrejme aj $2^{10^{10}} \mid x!$ (napríklad preto, že platí

$\left\lfloor \frac{x}{2} \right\rfloor \geqq 10^{10}\Big)$, a teda aj $10^{10^{10}} | x!$. Teda hľadané číslo je $x = 4.10^{10} + 15 = 40\,000\,000\,015$. □

**Úloha 8.6.** Nájdite posledné tri číslice čísla 1000! pred jeho koncovými nulami.

*Riešenie.* Najprv určíme počet núl na konci 1000!. Týchto núl je

$$\left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{25} \right\rfloor + \left\lfloor \frac{1000}{125} \right\rfloor + \left\lfloor \frac{1000}{625} \right\rfloor = 249.$$

Preto našou úlohou je vlastne určiť číslo $x = \frac{1000!}{10^{249}}$ MOD 1000. Využijeme pritom rozklad $1000 = 2^3.5^3 = 8.125$, určíme najprv čísla $x$ MOD 8, $x$ MOD 125 a z nich potom $x$.

Pretože $2^{252} | 1000!$, zrejme platí $x$ MOD $8 = 0$. Na určovanie $x$ MOD 125 určíme najprv číslo $\frac{1000!}{5^{249}}$ MOD 125. Pritom budeme využívať vzorec

$$(5k + 1).(5k + 2).(5k + 3).(5k + 4) \equiv$$
$$\equiv 24 \pmod{125}$$

pre každé $k \in \mathbb{Z}$ (ktorý sa ľahko overí roznásobením ľavej strany). Zostávajúce čísla deliteľné piatimi krátime s päťkami v menovateli. Postupne dostávame (počítame modulo 125):

$$\frac{1000!}{5^{249}} \equiv 24^{200}.\frac{200!}{5^{49}} \equiv 24^{200}.24^{40}.\frac{40!}{5^{9}} \equiv$$

$$\equiv 24^{200}.24^{40}.24^{8}.\frac{8!}{5^{1}} = 24^{248}.24.6.7.8 =$$

$$= 24^{250}.14 = (25 - 1)^{250}.14 \equiv (-1)^{250}.14 =$$
$$= 14 \pmod{125}.$$

Znova počítajme modulo 125.
Platí

$$x \equiv \frac{1000!}{10^{249}} \equiv 2^{300}.\frac{1000!}{10^{249}} = 2^{51}.\frac{1000!}{5^{249}} \equiv 2^{51}.14 =$$
$$= 2^{50}.28 \equiv 24^{5}.28 = (25 - 1)^{5}.28 \equiv -1.28 \equiv$$
$$\equiv 97 \pmod{125}.$$

Teda $x = 97 + 125y$ pre nejaké celé číslo $y$; pritom $0 \leqq y \leqq 7$, pretože $0 \leqq x \leqq 999$. Vieme však $x \text{ MOD } 8 = 0$, a preto

$$97 + 125y \equiv 0 \pmod 8,$$
$$5y \equiv -1 \pmod 8,$$
$$y \equiv 3 \pmod 8.$$

Teda $y = 3$, a potom $x = 97 + 3.125 = 472$. Posledné trojčíslie čísla 1000! pred jeho koncovými nulami teda je 472. □

**Úloha 8.7.** Určte zvyšok pri delení čísla 1000! číslom 1009.

*Riešenie.* 1009 je prvočíslo, a preto podľa Wilsonovej vety

$$1008! \equiv -1 \pmod{1009}.$$

Odtiaľ postupne dostávame

$$1000!.\prod_{i=1}^{8}(1000 + i) \equiv -1 \pmod{1009},$$

$$1000!\,.\prod_{i=1}^{8}(i-9) \equiv -1 \pmod{1009},$$

$$1000!\,.\,40320 \equiv -1 \pmod{1009},$$

$$1000!\,.\,(-40) \equiv -1 \pmod{1009},$$

$$1000!\,.\,(-9080) \equiv -227 \pmod{1009},$$

$$1000! \equiv 782 \pmod{1009}.$$

Teda hľadaný zvyšok je 782. □

**Úloha 8.8.** **Určte zvyšok pri delení čísla 1000! číslom** 1007.

*Riešenie.* **Platí** $1007 = 19.53 \mid 1000!$, **teda hľadaný** zvyšok je 0. □

**Úloha 8.9.** **Nech** $x$, $y$ **sú kladné reálne čísla také, že**

$$x^{x^{x^x}} = 3!!!\,,\ y^{y^{y^{y^y}}} = 3!!!!\,.$$

Zistite, ktoré z čísel $x$, $y$ je väčšie.

*Riešenie.* Zrejme $x > 1$, $y > 1$. **Označme** $A = x^{x^{x^x}}$, $B = y^{y^{y^y}}$, $C = y^B$. **Najprv ukážeme** $y < 3$. **Skutočne,**

$$C = 3!!!! = 720!! < 720^{720}! < (720^{720})^{720^{720}} =$$
$$= 720^{720^{721}} < 729^{720^{721}} = 3^{6\cdot 3^{6\cdot 721}} < 3^{3^{6\cdot 721+2}} <$$
$$< 3^{3^{3^8}} < 3^{3^{3^{3^2}}}.$$

Teraz stačí uvážiť, že umocňovanie je pre argumenty väčšie než 1 monotónna operácia. Teraz ukážeme sporom $y > x$. Keby bolo $y \leq x$, tak $B \leq A$ a potom

$$A! = C = y^B \leqq y^A < 3^A < \left(\frac{A}{\mathrm{e}}\right)^A < A!,$$

a to je spor. (Využili sme zrejmú nerovnosť $A \geqq 9$ a Stirlingov vzorec.) □

# 9. ČÍSLICE OKOLO DESATINNEJ ČIARKY

Úlohy v tejto kapitole by sa dali principiálne vyriešiť tak, že by sme príslušné čísla vyrátali s dostatočnou presnosťou; pre 2 číslice za desatinnou čiarkou by spravidla (no nie vždy) stačila presnosť na jednu tisícinu. Praktické ťažkosti však znova nastávajú preto, že uvažované čísla sú príliš veľké. Ukážeme niektoré obraty, ktorými sa možno priamemu výpočtu vyhnúť. Keby sa niekomu nepáčili formulácie úloh, v ktorých ide o nekonečné (a teda vlastne nenapísateľné) desatinné rozvoje, môže si každú úlohu

„Určiť $i$ miest pred desatinnou čiarkou a $j$ miest za desatinnou čiarkou v čísle $X$"

preformulovať na úlohu

„Určiť číslo $\lfloor 10^j . X \rfloor$ MOD $10^{i+j}$."

**Úloha 9.1.** Určte dve číslice pred a dve číslice za desatinnou čiarkou čísla

$$A = \sqrt{3^{6^9} + 3^{9^6}}.$$

*Riešenie.* Zrejme platí

$$A > \sqrt{3^{6^9}} = \sqrt{3^{2^9 . 3^9}} = 3^{2^8 . 3^9}$$

a na druhej strane

$$(3^{2^8 . 3^9} + 0{,}01)^2 > 3^{2^9 . 3^9} + 0{,}02 . 3^{2^8 . 3^9} >$$
$$> 3^{6^9} + 3^{2^8 . 3^9 - 4} > 3^{6^9} + 3^{(2^8 - 4) . 3^9} > 3^{6^9} + 3^{3^3 . 3^9} =$$
$$= 3^{6^9} + 3^{9^6}.$$

Spolu teda máme

$$3^{2^8.3^9} < A < 3^{2^8.3^9} + 0{,}01.$$

Teda prvé dve číslice za desatinnou čiarkou čísla $A$ sú nuly, a posledné číslice pred desatinnou čiarkou sú také ako posledné dve číslice čísla $3^{2^8.3^9}$. Ešte teda musíme určiť

$$3^{2^8.3^9} \text{ MOD } 100 = 3^{(2^8.3^9) \text{MOD } nsn(\varphi(25),\, \varphi(4))} \text{ MOD } 100 =$$

$$= 3^{2^8.3^9 \text{MOD } 20} \text{ MOD } 100 = 3^{(256.27^3) \text{MOD } 20} \text{ MOD } 100 =$$

$$= 3^{(16.3) \text{MOD } 20} \text{ MOD } 100 = 3^8 \text{ MOD } 100 = 61.$$

Teda hľadané číslice čísla $A$ sú $\ldots 61{,}00\ldots$ □

Určovanie väčšieho počtu číslic za desatinnou čiarkou by tento raz nerobilo problémy; skúste určiť napríklad tisíc týchto číslic. S kalkulačkou (alebo tabuľkami) však môžeme bez prílišnej námahy vyriešiť aj nasledujúcu úlohu.

**Úloha 9.2.** Zistite prvú nenulovú číslicu za desatinnou čiarkou čísla

$$A = \sqrt{3^{6^9} + 3^{9^6}}.$$

*Riešenie.* Označme $x$ zlomkovú časť čísla $A$. Pretože $|A| = 3^{2^8.3^9}$ podľa predchádzajúcej úlohy, máme

$$(3^{2^8.3^9} + x)^2 = 3^{6^9} + 3^{9^6}$$

a po úprave

$$2.3^{2^8.3^9}.x + x^2 = 3^{9^6}.$$

Pretože $0 < x < 1$, dostávame odtiaľ

$$\frac{3^{9^6} - 1}{2.3^{2^8.3^9}} < x < \frac{3^{9^6}}{2.3^{2^8.3^9}}.$$

Logaritmus pravej strany je

$$(9^6 - 2^8 . 3^9) . \log 3 - \log 2 \doteq -2150\,579{,}984 =$$
$$= 0{,}016 - 2\,150\,580$$

V rámci danej presnosti je aj logaritmus ľavej strany, a teda aj $\log x$, rovnaký. Teda

$$x \doteq 1{,}04 . 10^{-2150580},$$

čiže prvá nenulová číslica za desatinnou čiarkou v čísle $A$ je 1. □

Súčasne sme zistili aj počet núl medzi desatinnou čiarkou a prvou nenulovou číslicou; je ich 2 150 579. Poznamenajme, že log 3 a log 2 treba vziať dostatočne presne (napr. na 10 des. miest); číslo 1,04 vzniklo zaokrúhlením z 1,03 ..., ale trojka už nie je spoľahlivo určená.

**Úloha 9.3.** Zistite štyri číslice pred a štyri číslice za desatinnou čiarkou čísla

$$B = \sqrt[9]{5^{6^7} + 6^{7^5}}.$$

*Riešenie.* Napíšme $B$ v tvare $5^{2^7 . 3^5} + x$.
Pretože $\left(5^{2^7 . 3^5}\right)^9 = 5^{6^7}$, platí $x > 0$. Na druhej strane

$$\left(5^{2^7 . 3^5} + x\right)^9 = 5^{6^7} + 6^{7^5},$$
$$5^{6^7} + 9 . \left(5^{2^7 . 3^5}\right)^8 . x < 5^{6^7} + 6^{7^5},$$
$$x < \frac{6^{7^5}}{9 . \left(5^{2^7 . 3^5}\right)^8} .$$

Ale

$$\frac{6^{7^5}}{9 . \left(5^{2^7 . 3^5}\right)^8} < \frac{25^{7^5}}{5^{2^{10} . 3^5}} = 25^{7^5 - 2^9 . 3^5} < 25^{7^5 - 7^3 . 7^2 . 4} =$$
$$= 25^{-3 . 7^5} < 10^{-4},$$

teda hľadané číslice za desatinnou čiarkou sú nuly. Pre číslice pred desatinnou čiarkou musíme určiť $u = \lfloor B \rfloor \text{ MOD } 10^4$, kde $\lfloor B \rfloor = 5^{2^7 \cdot 3^5}$. Zrejme $\lfloor B \rfloor \text{ MOD } 5^4 = 0$ a ďalej

$$\lfloor B \rfloor \text{ MOD } 2^4 = 5^{2^7 \cdot 3^5} \text{ MOD } 16 =$$
$$= (5^4 \text{ MOD } 16)^{2^5 \cdot 3^5} \text{ MOD } 16 = 1.$$

Teda platí $u = 625k$ pre nejaké celé číslo $k$, $0 \leqq k < 16$, a súčasne $u \equiv 1 \pmod{16}$, teda $625k \equiv 1 \pmod{16}$, $k \equiv 1 \pmod{16}$, a teda $k = 1$. Potom $u = 625$. Preto hľadané číslice čísla $B$ sú $\ldots 0625{,}0000\ldots$ □

**Úloha 9.4.** Určte tri číslice pred a tri číslice za desatinnou čiarkou čísla

$$C = \sqrt[3]{8^{666} + 4^{666}}.$$

*Riešenie.* Platí

$$2^{666} = \sqrt[3]{8^{666}} < C < \sqrt[3]{8^{666} + 3 \cdot 4^{666} + 3 \cdot 2^{666} + 1} =$$
$$= 2^{666} + 1,$$

a preto $\lfloor C \rfloor = 2^{666}$. Označme $x$ zlomkovú časť čísla $C$. Platí

$$(2^{666} + x)^3 = 8^{666} + 4^{666},$$

$$8^{666} + 3x \cdot 4^{666} + 3x^2 \cdot 2^{666} + x^3 = 8^{666} + 4^{666},$$

$$3x \cdot 4^{666} + 3x^2 \cdot 2^{666} + x^3 = 4^{666}.$$

Odtiaľ s využitím $0 < x < 1$ dostávame

$$\frac{1}{3} \cdot \frac{4^{666} - 3 \cdot 2^{666} - 1}{4^{666}} < x < \frac{1}{3}.$$

Druhý činiteľ ľavej strany je však blízky k 1 (nám stačí, že je medzi 0,999 a 1), a preto hľadané číslice za desatinnou čiarkou sú trojky. Pre určenie číslic pred desatinnou čiarkou určíme $2^{666}$ MOD 1000. Najprv počítajme modulo 125; platí $\varphi(125) = 100$, a preto

$$2^{666} \equiv 2^{66} = (2^7)^9 . 2^3 \equiv 3^9 . 2^3 = 54^3 \equiv (50 + 4)^3 \equiv$$

$$\equiv 3 . 50 . 4^2 + 4^3 = 2464 \equiv 89 \pmod{125}.$$

Preto $2^{666} = 89 + k . 125$ pre nejaké prirodzené číslo $k$. Pritom ale $2^{666} \equiv 0 \pmod 8$, teda

$$89 + k . 125 \equiv 0 \pmod 8.$$

Odtiaľ máme $1 + 5k \equiv 0 \pmod 8$, a teda $k \equiv 3 \pmod 8$. Potom platí $2^{666} = 89 + (3 + 8n) . 125$ pre nejaké prirodzené číslo $n$, a teda $2^{666} \equiv 89 + 375 = 464 \pmod{1000}$.
Preto hľadané číslice čísla $C$ sú ...464,333... □

**Úloha 9.5.** Nájdite dve číslice pred a dve číslice za desatinnou čiarkou čísla

$$D = \sqrt{9^{603} + 9^{306}}.$$

*Riešenie.* Položme $D = 3^{603} + x$. Pretože $D^2 > 9^{603}$, platí $x > 0$. Ďalej platí

$$(3^{603} + x)^2 = 9^{603} + 9^{306},$$

$$9^{603} + 2x . 3^{603} + x^2 = 9^{603} + 3^{612},$$

$$2x . 3^{603} + x^2 = 3^{612},$$

$$x = \frac{3^9 - x^2 . 3^{-603}}{2}.$$

Odtiaľ (a z $x > 0$) dostávame $x < \frac{3^9}{2}$, a potom aj $x > \frac{3^9}{2} - \frac{3^{-585}}{8}$.

Preto hľadané číslice za desatinnou čiarkou sú 49. Pre číslice pred desatinnou čiarkou uvážme, že platí

$$\lfloor x \rfloor \text{ MOD } 100 = \left\lfloor \frac{3^9}{2} \right\rfloor \text{ MOD } 100 = \left\lfloor \frac{27^3}{2} \right\rfloor \text{ MOD } 100 =$$

$$= \left\lfloor \frac{19\,683}{2} \right\rfloor \text{ MOD } 100 = 41,$$

$$3^{603} \text{ MOD } 100 = 3^{603 \text{ MOD } 40} \text{ MOD } 100 =$$

$$= 3^3 \text{ MOD } 100 = 27,$$

$(\lfloor x \rfloor + 3^{603})$ MOD $100 = 68$, a preto hľadané číslice čísla $D$ sú ...68,49... □

**Úloha 9.6.** Určte dve číslice pred a štyri číslice za desatinnou čiarkou čísla

$$E = \sqrt[4]{7^{700} + 7^{600}}.$$

*Riešenie.* Položme $E = 7^{175} + x$; zrejme $x > 0$. Ďalej platí

$$(7^{175} + x)^4 = 7^{700} + 7^{600},$$

$$7^{700} + 4x \,.\, 7^{525} + 6x^2 \,.\, 7^{350} + 4x^3 \,.\, 7^{175} + x^4 =$$

$$= 7^{700} + 7^{600},$$

$$x = \frac{7^{600} - 6x^2 \,.\, 7^{350} - 4x^3 \,.\, 7^{175} - x^4}{4 \,.\, 7^{525}}.$$

Odtiaľ (a z podmienky $x > 0$) dostávame $x < \frac{7^{75}}{4}$ a potom $x > \frac{7^{75}}{4} - 0{,}0001$.

Platí $7^{75}$ MOD 4 = 3, teda zlomková časť čísla $\frac{7^{75}}{4}$ začína 75, a zlomková časť čísla $x$ (a teda aj $E$) začína číslicami 7499. Pre určenie číslic pred desatinnou čiarkou určíme $\lfloor x \rfloor$ MOD 100, na čo najprv potrebujeme

$$7^{75} \text{ MOD } 400 = 7^{4.18+3} \text{ MOD } 400 =$$
$$= ((7^4 \text{ MOD } 400)^{18} . 7^3) \text{ MOD } 400 =$$
$$= (1^{18} . 7^3) \text{ MOD } 400 = 343.$$

Potom

$$\lfloor x \rfloor \text{ MOD } 100 = \left\lfloor \frac{7^{75}}{4} \right\rfloor \text{ MOD } 100 = \left\lfloor \frac{7^{75} \text{ MOD } 400}{4} \right\rfloor =$$
$$= \left\lfloor \frac{343}{4} \right\rfloor = 85 .$$

Ďalej určíme

$$7^{175} \text{ MOD } 100 = ((7^4 \text{ MOD } 100)^{43} . 7^3) \text{ MOD } 100 =$$
$$= 343 \text{ MOD } 100 = 43.$$

Preto $\lfloor E \rfloor$ MOD 100 = (85 + 43) MOD 100 = 28, a hľadané číslice čísla $E$ sú ...28,7499... □

**Úloha 9.7.** Určte 7 číslic pred a 7 číslic za desatinnou čiarkou v čísle

$$F = \sqrt[7]{7^{700} + 7^{600}}.$$

*Riešenie.* Označme $u = 7.(F - 7^{100})$; potom $F = 7^{100} + \frac{u}{7}$.

Pretože $(7^{100})^7 < F^7 < \left(7^{100} + \frac{1}{7}\right)^7$, platí $0 < u < 1$.

Určíme $u$ presnejšie. Platí

$$\left(7^{100} + \frac{u}{7}\right)^7 < 7^{700} + u.7^{600} + 7^{500}.$$

Posledný člen na pravej strane je totiž väčší než súčet zvyšných členov z binomického vzorca, t. j.

$$\binom{7}{2}.7^{500}.\left(\frac{u}{7}\right)^2 + \binom{7}{3}.7^{400}.\left(\frac{u}{7}\right)^3 + \ldots + \left(\frac{u}{7}\right)^7$$

(dal by sa ešte zmenšiť). Preto platí

$$7^{700} + u.7^{600} + 7^{500} > 7^{700} + 7^{600},$$

$$u > \frac{7^{600} - 7^{500}}{7^{600}} = 1 - 7^{-100}.$$

Z toho pre $F$ vyplýva

$$7^{100} + 7^{-1} - 7^{-101} < F < 7^{100} + 7^{-1}$$

a odtiaľ (a z toho, že $\frac{1}{7}$ nemá v desatinnom rozvoji na 8. mieste nulu) zasa plynie, že $F$ má hľadané číslice rovnaké ako číslo $7^{100} + \frac{1}{7}$. Pre číslice pred desatinnou čiarkou počítajme modulo $10^7$:

$$7^{100} = (7^4)^{25} = (2400 + 1)^{25} \equiv \binom{25}{2}.2400^2 + \binom{25}{1}.$$

$$.2400 + 1 = 25.12.2400^2 + 25.2400 + 1 =$$

$$= 12.12\,000^2 + 60\,000 + 1 \equiv$$

$$\equiv 8\,000\,000 + 60\,000 + 1 = 8\,060\,001 \pmod{10^7}.$$

(Vynechané členy v rozvoji $(2400 + 1)^{25}$ boli násobkami $10^8$.) Číslice za desatinnou čiarkou ľahko získame delením. Teda hľadané číslice čísla $F$ sú ...8 060 001, 142 857 1... □

**Úloha 9.8.** Určte dve číslice pred a dve číslice za desatinnou čiarkou v čísle

$$A = (2 + \sqrt{3})^{1000}.$$

*Riešenie.* Budeme uvažovať postupnosť $(a_0, a_1, a_2, \ldots)$ danú predpisom

$$a_n = (2 + \sqrt{3})^n + (2 - \sqrt{3})^n.$$

(Jej členy sú celé čísla a platí $A \doteq a_{1000}$.)
Čísla $2 + \sqrt{3}$, $2 - \sqrt{3}$ sú korene kvadratickej rovnice

$$x^2 - 4x + 1 = 0,$$

preto postupnosť $(a_0, a_1, a_2, \ldots)$ vyhovuje rekurentnému predpisu

$$a_{n+2} = 4a_{n+1} - a_n.$$

Tento predpis spolu s rovnosťami

$$a_0 = 2, \quad a_1 = 4$$

danú postupnosť jednoznačne určuje. Teraz určíme $a_{1000}$ MOD 100 tak, že budeme počítať čísla $b_n = a_n$ MOD 100. Pritom zrejme $b_0 = 2$, $b_1 = 4$ a

$$b_{n+2} = (4b_{n+1} - b_n) \text{ MOD } 100$$

pre všetky $n$. Členy postupnosti $b_n$ budeme počítať až dovtedy, kým nezistíme opakovanie.

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $b_n$ | 2 | 4 | 14 | 52 | 94 | 24 | 2 | 84 | 34 | 52 | 74 | 44 |

| $n$ | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $b_n$ | 2 | 64 | 54 | 52 | 54 | 64 | 2 | 44 | 74 | 52 | 34 | 84 |

| $n$ | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|
| $b_n$ | 2 | 24 | 94 | 52 | 14 | 4 | 2 | 4 |

Vidíme teda, že platí

$$b_{30} = b_0, \quad b_{31} = b_1 .$$

Pretože každý člen postupnosti $(b_0, b_1, b_2, \ldots)$ je určený dvoma predchádzajúcimi členmi, matematickou indukciou dostávame

$$b_{n+30} = b_n,$$

a potom aj $b_n = b_{n \text{ MOD } 30}$ pre každé prirodzené číslo $n$. Špeciálne, pre $n = 1000$ máme $a_{1000}$ MOD $100 = b_{1000} = b_{10} = 74$. Ďalej platí

$$a_{1000} - 0{,}01 < a_{1000} - (2 - \sqrt{3})^{1000} = A < a_{1000} .$$

Preto hľadané číslice čísla $A$ sú ...73, 99... □

Najnamáhavejšou časťou riešenia predošlej úlohy bolo doplnenie tabuľky hodnôt $b_n$. Numerická chyba by znehodnotila celý ďalší výpočet. Preto by bolo dobré mať nejaké prostriedky na kontrolu. Jedna z možností je, aby sme počítali úplne rovnakým spôsobom $a_{1000}$ MOD 25, $a_{1000}$ MOD 4, a potom pomocou nich číslo $b_{1000}$ overili. Výhoda by tiež bola v tom, že namiesto periódy 30 by sme dostali periódy 15 a 2, teda stačilo by počítať menší počet členov. (Nové výpočty by mohli byť použité aj samostatne na výpočet čísla $b_{1000}$, a nielen na skúšku správnosti pôvodného výpočtu.) Iná možnosť úspory v počte počítaných členov $b_n$ bola všimnúť si, že pre $n \geq 2$ platí

$$b_{n-2} = (4b_{n-1} - b_n) \text{ MOD } 100.$$

Pretože platí $b_{14} = b_{16}$, vychádza odtiaľ $b_{15+k} = b_{15-k}$ pre $0 \leqq k \leqq 15$, teda členy $b_{17}$ až $b_{30}$ sa dali doplniť bez počítania. Obe metódy možno použiť súčasne, ak definujeme (nezmeneným vzorcom) $a_n$ pro všetky celé $n$ a vypočítame čísla $c_n = a_n$ MOD 25 pre $n = -1$ až 8. Pretože vyjde $c_{-1} = c_1$, $c_8 = c_7$, platí $c_{-n} = c_n$, $c_{15-n} = c_n$ pre všetky $n$, z čeho odvodíme $c_{1000} = c_5 = 24$.

**Úloha 9.9.** Zistite dve číslice pred a dve číslice za desatinnou čiarkou v čísle

$$B = (\sqrt{6} + \sqrt{2})^{100}.$$

*Riešenie*. Platí

$$B = ((\sqrt{6} + \sqrt{2})^2)^{50} = (8 + 4\sqrt{3})^{50}.$$

Položme

$$a_n = (8 + 4\sqrt{3})^n + (8 - 4\sqrt{3})^n$$

a skúmajme postupnosť $(a_0, a_1, a_2, \ldots)$.
Pretože $8 + 4\sqrt{3}$, $8 - 4\sqrt{3}$ sú korene kvadratickej rovnice

$$x^2 - 16x + 16 = 0,$$

vyhovuje postupnosť $(a_0, a_1, a_2, \ldots)$ rekurentnému predpisu

$$a_{n+2} = 16a_{n+1} - 16a_n.$$

Ďalej vieme $a_0 = 2$, $a_1 = 16$. Znova označme $b_n = a_n$ MOD 100 a počítajme členy postupnosti $(b_0, b_1, b_2, \ldots)$ až pokiaľ nezistíme opakovanie:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $b_n$ | 2 | 16 | 24 | 28 | 64 | 76 | 92 | 56 | 24 | 88 | 24 | 76 |

| $n$ | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $b_n$ | 32 | 96 | 24 | 48 | 84 | 76 | 72 | 36 | 24 | 8 | 44 | 76 |

| $n$ | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
|---|---|---|---|---|---|---|---|---|---|
| $b_n$ | 12 | 76 | 24 | 68 | 4 | 76 | 52 | 16 | 24 |

Vidíme teda

$$b_{31} = b_1, \qquad b_{32} = b_2,$$

a preto pre všetky $n \geqq 1$ platí

$$b_{n+30} = b_n.$$

Špeciálne $b_{50} = b_{20} = 24$, a preto

$$B + \left(8 - 4\sqrt{3}\right)^{50} \equiv 24 \pmod{100}.$$

Výpočtom na kalkulačke zistíme

$$\left(8 - 4\sqrt{3}\right)^{50} \doteq 32{,}0348$$

(stačí nám zistiť $32{,}03 < \left(8 - 4\sqrt{3}\right)^{50} < 32{,}04$), a potom už ľahko zistíme, že hľadané číslice čísla $B$ sú ...91, 96... □

Predložené riešenie úlohy 9.9 je samostatné, nezávislé od riešenia predchádzajúcej úlohy 9.8. S využitím tohto riešenia sme si mohli značnú časť výpočtov ušetriť. Platí totiž

$$B = \left(\sqrt{6} + \sqrt{2}\right)^{100} = \left(8 + 4\sqrt{3}\right)^{50} = 4^{50}.\left(2 + \sqrt{3}\right)^{50}$$

a z riešenia úlohy 9.8 vieme

$$\left(2 + \sqrt{3}\right)^{50} + \left(2 - \sqrt{3}\right)^{50} \equiv 74 \pmod{100}.$$

Ak túto kongruenciu vynásobíme číslom $4^{50}$, dostaneme

$$B + 4^{50}.\left(2 - \sqrt{3}\right)^{50} \equiv 4^{50}.74 \pmod{100}$$

a odtiaľ po úprave

$$B + (8 - 4\sqrt{3})^{50} \equiv 24 \pmod{100}.$$

**Úloha 9.10.** Zistite tri číslice pred a tri číslice za desatinnou čiarkou v čísle

$$C = (\sqrt{2} + \sqrt{5})^{1000}.$$

*Riešenie.* Označme

$$A = (\sqrt{2} + \sqrt{5})^{1000} + (\sqrt{2} - \sqrt{5})^{1000}.$$

Podľa binomickej vety platí

$$A = 2 . \sum_{k=0}^{500} \binom{1000}{2k} . 2^{500-k} . 5^{k},$$

teda $A$ je celé číslo. Určme $A$ MOD 1000.
Na to najprv zistime, ktoré členy sumy vpravo sú násobkami 500. Zrejme sú také všetky členy pre $3 \leq k \leq$ $\leq 498$; na to stačí uvážiť priamo vypísané exponenty čísel 2, 5 v tomto výraze. Avšak aj členy pre $k = 1, 2,$ 499 sú násobkami 500, pretože príslušné binomické koeficienty sú násobkami 250. Preto platí

$$A \equiv 2 . (2^{500} + 5^{500}) \pmod{1000}.$$

Aby sme určili $A$ MOD 1000, využijeme rozklad $1000 =$ $= 8 . 125$ (a nesúdeliteľnosť čísel 8, 125). Pri počítaní modulo 8 dostávame

$$A \equiv 2 . (2^{500} + 5^{500}) \equiv 2 . 25^{250} \equiv 2 . 1^{250} = 2 \pmod{8}.$$

Pri počítaní modulo 125 s využitím Eulerovej vety dostávame

$$A \equiv 2 . (2^{500} + 5^{500}) \equiv 2^{501} \equiv 2^{501 \text{ MOD } 100} =$$
$$= 2 \pmod{125}.$$

Teda platí $8|(A - 2)$, $125|(A - 2)$, a teda aj $1000|(A - - 2)$, t. j. $A$ MOD $1000 = 2$.
Teraz využijeme rovnosť

$$C = A - (\sqrt{2} - \sqrt{5})^{1000}$$

a odhad $0 < |\sqrt{2} - \sqrt{5}|^{1000} < |2{,}3 - 1{,}4|^{1000} < 0{,}001$.
Preto hľadané číslice čísla $C$ sú ...001,999... □

**Úloha 9.11.** Určiť dve číslice pred a dve číslice za desatinnou čiarkou čísla

$$D = (\sqrt{3} + \sqrt{5})^{1000}.$$

*Riešenie.* Platí $D = (8 + 2\sqrt{15})^{500}$. Uvažujme postupnosť $(a_0, a_1, a_2, \ldots)$ danú predpisom

$$a_n = (8 + 2\sqrt{15})^n + (8 - 2\sqrt{15})^n.$$

Pretože čísla $8 + 2\sqrt{15}$, $8 - 2\sqrt{15}$ sú korene kvadratickej rovnice

$$x^2 = 16x - 4,$$

vyhovuje postupnosť $(a_0, a_1, a_2, \ldots)$ rekurentnému predpisu

$$a_{n+2} = 16a_{n+1} - 4a_n.$$

Tento predpis spolu s rovnosťami

$$a_0 = 2, \qquad a_1 = 16$$

jednoznačne určuje postupnosť $(a_0, a_1, a_2, \ldots)$.

Aby sme určili $a_{500}$ MOD 100, počítajme čísla $b_n = a_n$ MOD 100, až kým nezistíme opakovanie. Členy postupnosti $(b_0, b_1, b_2, \ldots)$ budeme počítať podľa rekurentného predpisu

$$b_{n+2} = (16b_{n+1} - 4b_n) \text{ MOD } 100.$$

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $b_n$ | 2 | 16 | 48 | 04 | 72 | 36 | 88 | 64 | 72 | 96 | 48 | 84 |

| $n$ | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $b_n$ | 52 | 96 | 28 | 64 | 12 | 36 | 28 | 04 | 52 | 16 | 48 |

Platí teda $b_{21} = b_1$, $b_{22} = b_2$, a preto pre všetky $n \geqq 1$ platí $b_{20+n} = b_n$. Preto $b_{500} = b_{20+24.20} = b_{20} = 52$. Teda platí

$$D + \left(8 - 2\sqrt{15}\right)^{500} \equiv 52 \pmod{100}.$$

Ďalej odhadneme

$$0 < \left(8 - 2\sqrt{15}\right)^{500} < (8 - 2.3{,}8)^{500} = 0{,}4^{500} < 0{,}01.$$

Teda hľadané číslice čísla $D$ sú ...51,99... □

# 10. ALGEBRAICKÉ ROVNICE

**Úloha 10.1.** Zistite, či má kvadratická rovnica

$$7^{8^9}.x^2 + 8^{9^7}.x + 9^{7^8} = 0$$

reálne korene.

*Riešenie.* Diskriminant tejto rovnice je

$$D = 8^{2\cdot 9^7} - 4.7^{8^9}.9^{7^8}.$$

Ukážeme, že $D < 0$; na to odhadujme

$$8^{2\cdot 9^7} < 49^{2\cdot 9^7} = 7^{4\cdot 3^{14}} < 7^{2\cdot 3^{15}} = 7^{2\cdot (3^3)^5} < 7^{2\cdot (2^5)^5} =$$
$$= 7^{2^{26}} < 7^{2^{27}} = 7^{8^9} < 4.7^{8^9}.9^{7^8},$$

teda $D < 0$ a rovnica nemá reálne korene. □

**Úloha 10.2.** Dokážte, že kvadratická rovnica

$$5^{5^5}.x^2 + 6^{6^6}.x + 4^{4^4} = 0$$

má dva rôzne reálne iracionálne korene.

*Riešenie.* Diskriminant tejto rovnice je

$$D = 6^{2\cdot 6^6} - 4.5^{5^5}.4^{4^4} > 6.6^{5^5}.6^{4^4} - 4.5^{5^5}.4^{4^4} > 0,$$

teda rovnica má reálne korene. Tieto korene sú racionálne práve vtedy, keď $\sqrt{D}$ je racionálne (a teda prirodzené) číslo, t. j. keď $D$ je štvorec. Ukážeme však

$$\left(6^{6^6}-1\right)^2 < D < \left(6^{6^6}\right)^2.$$

Pravá nerovnosť je zrejmá a na dôkaz ľavej stačí uvážiť

$$\left(6^{6^6}-1\right)^2 < 6^{2\cdot 6^6} - 6^{6^6} < 6^{2\cdot 6^6} - 6^{1+5^5+4^4} =$$
$$= 6^{2\cdot 6^6} - 6.6^{5^5}.6^{4^4} < 6^{2\cdot 6^6} - 4.5^{5^5}.4^{4^4} = D.$$

Teda $D$ leží medzi dvoma po sebe idúcimi čtvorcami, čiže nemôže byť štvorec. Preto sú korene danej rovnice iracionálne. □

**Úloha 10.3.** Dokážte, že kvadratická rovnica

$$6^{9^9}.x^2 + 7^{9^9}.x + 8^{9^9} = 0$$

má dva rôzne reálne iracionálne korene.

*Riešenie*. Diskriminant tejto rovnice je

$$D = 7^{2\cdot 9^9} - 4.6^{9^9}.8^{9^9} = 49^{9^9} - 4.48^{9^9}.$$

Aby sme dokázali $D > 0$, musíme dokázať

$$\left(\frac{49}{48}\right)^{9^9} > 4.$$

Na to stačí odhad

$$\left(\frac{49}{48}\right)^{9^9} = \left(1+\frac{1}{48}\right)^{9^9} > 1 + \frac{9^9}{48} > 4.$$

Teda platí $D > 0$ a rovnica má dva reálne korene. Ešte treba dokázať, že tieto korene nie sú racionálne. Na to stačí ukázať, že $\sqrt{D}$ je iracionálne číslo, teda že $D$ nie je štvorcom. Na to určíme $D$ MOD 5. Pretože $\varphi(5) = 4$, $9^9$ MOD 4 $= 1$ (a 49, 48 nie sú násobky 5), platí $D$ MOD5 $= (49^1 - 4.48^1)$ MOD 5 $= (4 - 12)$ MOD 5 $= 2$.

Avšak 2 je kvadratický nezvyšok modulo 5, preto $D$ nie je štvorec. □

**Úloha 10.4.** Dokážte, že rovnica

$$(1) \qquad 7^{7^7}.x^3 + 8^{8^8}.x^2 + 9^{9^9}.x + 10^{10^{10}} = 0$$

má práve jeden reálny koreň.

*Riešenie.* Označme $f(x)$ ľavú stranu rovnice (1). Funkcia $f(x)$ reálne premennej $x$ je spojitá, $f\left(-10^{10^{10}}\right) < 0$ a $f(0) > 0$, teda rovnica (1) má reálný koreň (medzi $-10^{10^{10}}$ a 0). Nemôže mať viac reálnych koreňov, pretože funkcia $f(x)$ je rastúca.
Jej derivácia

$$f'(x) = 3.7^{7^7}.x^2 + 2.8^{8^8}.x + 9^{9^9}$$

je totiž kladná, pretože $f(0) > 0$ a rovnica $f'(x) = 0$ má diskriminant

$$\left(2.8^{8^8}\right)^2 - 4.3.7^{7^7}.9^{9^9} < 8^{3.8^8} - 9^{9^9} < 0,$$

teda nemá reálné korene. □

V niekoľkých ďalších úlohách sa budeme zaoberať rovnicou (1) a jej koreňmi. Pokiaľ budeme pracovať s komplexnými číslami, nebudeme vždy terminologicky rozlišovať tieto čísla a ich obrazy v rovine komplexných čísel.

**Úloha 10.5.** Dokážte, že obrazy koreňov rovnice (1) z predchádzajúcej úlohy nie sú vrcholy rovnostranného trojuholníka.

*Riešenie.* Odvodíme nutnú podmienku na to, aby korene rovnice

$$(2) \qquad Ax^3 + Bx^2 + Cx + D = 0$$

boli vrcholy rovnostranného trojuholníka a potom ukážeme, že rovnica (1) ju nespĺňa. Nech korene $x_1, x_2, x_3$ rovnice (2) sú vrcholy rovnostranného trojuholníka a $t = \frac{1}{3}(x_1 + x_2 + x_3)$ je jeho ťažisko. Čísla $x_1 - t$, $x_2 - t$, $x_3 - t$ majú rovnaké absolútne hodnoty a ich amplitúdy sa líšia o násobky 120°. Ich tretie mocniny sa potom navzájom rovnajú, preto $x_1, x_2, x_3$ sú pre nejaké komplexné číslo $u$ korene rovnice $(x - t)^3 = u$, teda po úprave

$$x^3 - 3tx^2 + 3t^2x - (t^3 + u) = 0.$$

Rovnica (2) je $A$-násobkom poslednej rovnice (pretože obe tieto kubické rovnice majú rovnaké korene), a teda

$$-A\,.\,3t = B,\ A\,.\,3t^2 = C,\ -A\,.\,(t^3 + u) = D.$$

Preto

$$B^2 = (A\,.\,3t)^2 = 3A\,.\,A\,.\,3t^2 = 3AC.$$

Nájdená nutná podmienka $B^2 = 3AC$ v prípade rovnice (1) dáva

$$8^{2\cdot 8^8} = 3\,.\,7^{7^7}\,.\,9^{9^9},$$

čo zrejme neplatí, napríklad preto, že ľavá strana je párna a pravá nepárna. Teda korene rovnice (1) nie sú vrcholy rovnostranného trojuholníka. □

Nutná a postačujúca podmienka na to, aby korene rovnice (2) boli vrcholy rovnostranného trojuholníka, je

$$B^2 = 3AC \quad \text{a} \quad BC \neq 9AD.$$

Pridanie druhého vzťahu zabezpečuje, že (2) je kubická rovnica (t. j. $A \neq 0$), a že nemá trojnásobný koreň.

V nasledujúcej úlohe ukážeme, že trojuholník, ktorým sme sa zaoberali, je „skoro rovnostranný“.

**Úloha 10.6.** Dokážte, že veľkosti uhlov trojuholníka s vrcholmi v koreňoch rovnice (1) z úlohy 10.4 sa líšia od 60° o menej než 1″.

*Riešenie*. Nech korene rovnice (1) sú $a$, $b \pm ic$, kde $a$, $b$, $c$ sú reálne čísla, $c > 0$. (Tu už využívame riešenie úlohy 10.4.) Označme

$$R = \frac{8^{8^8}}{7^{7^7}}, S = \frac{9^{9^9}}{7^{7^7}}, T = \frac{10^{10^{10}}}{7^{7^7}}.$$

Zo vzťahov medzi koreňmi a koeficientmi normovanej kubickej rovnice (ktorú dostaneme z (1) predelením číslom $7^{7^7}$) máme

$$a + 2b = -R, \quad 2ab + b^2 + c^2 = S,$$
$$a.(b^2 + c^2) = -T.$$

Uvažovaný trojuholník je rovnoramenný, so základňou kolmou na reálnu os a hlavným vrcholom $a$. Nech veľkosť uhla pri hlavnom vrchole je $2\alpha$. Potom $\operatorname{tg} \alpha =$ $= \frac{c}{|b - a|}$, a preto

$$\operatorname{tg}^2 \alpha - \frac{1}{3} = \frac{c^2}{(b-a)^2} - \frac{1}{3} = \frac{3c^2 - (b-a)^2}{3(b-a)^2} =$$
$$= \frac{4.(3c^2 - (b-a)^2)}{3.(2b - 2a)^2}.$$

Avšak $c^2 = S - 2ab - b^2$, $2b - 2a = -R - 3a$, a preto

$$\operatorname{tg}^2 \alpha - \frac{1}{3} = \frac{4.(3S - 6ab - 3b^2 - b^2 + 2ab - a^2)}{3.(-R - 3a)^2} =$$

$$= \frac{4.(3S - 4b^2 - 4ab - a^2)}{3.(R + 3a)^2} = \frac{4.(3S - (2b + a)^2)}{3.(R + 3a)^2} =$$

$$= \frac{12S - 4R^2}{3.(R + 3a)^2}.$$

Platí

$$12S - 4R^2 = \frac{12.9^{9^9}.7^{7^7} - 4.8^{2\cdot 8^8}}{7^{2\cdot 7^7}} >$$

$$> \frac{9^{9^9} - 8^{2\cdot 8^8+1}}{7^{2\cdot 7^7}} > 0,$$

a preto $\operatorname{tg}^2 \alpha - \frac{1}{3} > 0$. Na odhad z druhej strany najprv odhadneme číslo $a$; na to označíme $f(x)$ ľavú stranu rovnice (1); z úlohy 10.4 už vieme, že $f(x)$ je rastúca funkcia reálnej premennej $x$. Platí

$$f(-\sqrt[3]{T}) = 7^{7^7}.(-T + R.\sqrt[3]{T^2} - S.\sqrt[3]{T} + T) =$$

$$= 8^{8^8}.(10^{10^{10}})^{2/3}.(7^{7^7})^{-2/3} - 9^{9^9}.(10^{10^{10}})^{1/3}.(7^{7^7})^{-1/3} >$$

$$> 10^{6\cdot 10^9} - 10^{4\cdot 10^9} > 0 = f(a),$$

a preto $a < -\sqrt[3]{T}$. Ďalej platí

$$R^3 = 8^{3\cdot 8^8}.7^{-3\cdot 7^7} < 8^{10^{10}}.7^{-7^7} < 10^{10^{10}}.7^{-7^7} = T,$$

a preto $R < \sqrt[3]{T}$. Z dokázaných vzťahov vyplýva

$$|R + 3a| \geqq 3.|a| - R > 3.\sqrt[3]{T} - R > 2.\sqrt[3]{T}.$$

Preto platí

$$\operatorname{tg}^2 \alpha - \frac{1}{3} = \frac{12S - 4R^2}{3.(R + 3a)^2} < \frac{12S}{12\sqrt[3]{T^2}} =$$

$$= \frac{9^{9^9}}{7^{7^7}} \cdot \left(\frac{10^{10^{10}}}{7^{7^7}}\right)^{-2/3} = 9^{9^9}.\left(7^{7^7}\right)^{-1/3}.\left(10^{10^{10}}\right)^{-2/3} <$$

$$< 10^{10^9}.1.10^{-6.10^9} < 10^{-10}.$$

Spolu máme

$$\operatorname{tg} \alpha > 0,\ 0 < \operatorname{tg}^2 \alpha - \frac{1}{3} < 10^{-10},$$

a z týchto nerovností ľahko zistíme

$$\frac{1}{\sqrt{3}} < \operatorname{tg} \alpha < \frac{1}{\sqrt{3}} + 10^{-10}.$$

Pretože $0 < \alpha < 90°$, $\operatorname{tg} 30° = \frac{1}{\sqrt{3}}$ a

$$\operatorname{tg}(30° + 0{,}5'') = \frac{\operatorname{tg} 30° + \operatorname{tg} 0{,}5''}{1 - \operatorname{tg} 30° . \operatorname{tg} 0{,}5''} > \operatorname{tg} 30° +$$

$$+ \operatorname{tg} 0{,}5'' > \frac{1}{\sqrt{3}} + \frac{\pi}{2.180.60^2} > \frac{1}{\sqrt{3}} + 10^{-10},$$

máme $30° < \alpha < 30° + 0{,}5''$, teda veľkosť $2\alpha$ uhla pri hlavnom vrchole je medzi $60°$ a $60°0'1''$. Potom veľkosti uhlov pri základni sú medzi $59°59'59{,}5''$ a $60°$, teda tiež sa líšia od $60°$ o menej než $1''$. □

Odhad v úlohe 10.6 sme dosiahli s veľmi veľkou rezervou; na miesto jednej uhlovej sekundy mohla byť v jej texte napríklad triliónt ina uhlovej sekundy bez toho, aby sa riešenie muselo podstatne zmeniť.

Nasledujúca úloha sa dá vyriešiť rovnako ako úlohy 10.4 až 10.6, preto ju nechávame na riešenie čitateľovi. (Pritom bod b) vlastne nemusí robiť, ak vyrieši bod c) tak ako bola riešená úloha 10.6.)

**Úloha 10.7.** Uvažujme rovnicu

(3) $$7!!.x^3 + 8!!.x^2 + 9!!.x + 10!! = 0.$$

a) Dokážte, že rovnica (3) má práve jeden reálny koreň.
b) Dokážte, že obrazy koreňov rovnice (3) v komplexnej rovine nie sú vrcholy rovnostranného trojuholníka.
c) Určte uhly tohoto trojuholníka s presnosťou $\pm 1''$.

**Úloha 10.8.** Dokážte, že reálny koreň rovnice (1) z úlohy 10.4 je iracionálny.

*Riešenie.* Predpokladajme obrátene, že rovnica (1) má racionálny koreň a $\frac{r}{s}$ je jeho základný tvar (t. j. $r \in \mathsf{Z}$, $s \in \mathsf{P}$, $D(r, s) = 1$). Po dosadení do (1) a vynásobení $s^3$ dostávame

(4) $$7^{7^7}.r^3 + 8^{8^8}.r^2s + 9^{9^9}.rs^2 + 10^{10^{10}}.s^3 = 0.$$

Všetky členy okrem prvého sú násobkami čísla $s$, a preto aj prvý člen je násobkom $s$, t. j.
$s \mid 7^{7^7}.r^3$. Avšak $D(r, s) = 1$, a preto $s \mid 7^{7^7}$. Rovnako možno dokázať aj $r \mid 10^{10^{10}}$. Z týchto vzťahov a z toho, že reálny koreň rovnice (1) je záporný, vyplýva.

$$r = -2^m.5^n, \quad s = 7^p$$

pre nejaké celé čísla $m$, $n$, $p$ také, že

$$0 \leqq m \leqq 10^{10}, \quad 0 \leqq n \leqq 10^{10}, \quad 0 \leqq p \leqq 7^7.$$

Ak platí $0 < n < 10^{10}$, tak $n + 1 \leqq 2n$, $n + 1 \leqq 10^{10}$, a preto $5^{n+1}$ delí každé z čísel $7^{7^7}.r^3$, $8^{8^8}.r^2s$, $10^{10^{10}}.s^3$. Potom aj $5^{n+1} \mid 9^{9^9}.rs^2$, ale $5 \nmid 9^{9^9}$, $5 \nmid s$ (pretože $5 \mid r$), a teda $5^{n+1} \mid r$, čo je spor.

Preto $n = 0$ alebo $n = 10^{10}$.

Úplné obdobne, ak platí $0 < m < 10^{10}$, tak $2^{m+1} \mid 9^{9^9}.rs^2$, ale $2 \nmid 9^{9^9}$, $2 \nmid s$ a teda $2^{m+1} \mid r$, čo je spor. Preto $m = 0$ alebo $m = 10^{10}$.

Teraz počítajme modulo 3. Keďže $m$, $n$ sú párne a $7 \equiv 1 \pmod 3$, platí

$$r = -2^m.5^n \equiv -1.1 = -1 \pmod 3, \quad s = 7^p \equiv$$
$$\equiv 1 \pmod 3.$$

Z rovnice (4) potom dostávame

$$1.(-1)^3 + 1.(-1)^2.1 + 0.(-1).1^2 + 1.1^3 \equiv$$
$$\equiv 0 \pmod 3,$$

teda $1 \equiv 0 \pmod 3$, a to je spor. Preto rovnica (1) nemá racionálny koreň. □

Akonáhle sme zistili, že platí $n = 0$ alebo $n = 10^{10}$, mohli sme spor so (4) dostať tiež nasledujúcimi odhadmi:

Ak $n = 0$, tak $r \geqq -2^{10^{10}}$, a potom

$$7^{7^7}.r^3 + 8^{8^8}.r^2s + 9^{9^9}.rs^2 + 10^{10^{10}}.s^3 >$$
$$> -7^{7^7}.2^{3\cdot 10^{10}} + 0 - 9^{9^9}.2^{10^{10}}.7^{2\cdot 7^7} + 10^{10^{10}}.1 >$$
$$> -2^{3\cdot 10^{10}+3.7^7} - 2^{4\cdot 9^9+10^{10}+6\cdot 7^7} + 10^{10^{10}} >$$
$$> -2^{13\cdot 24\cdot 10^8} - 2^{3\cdot 5\cdot 10^9} + 10^{10^{10}} >$$
$$> -10^{4\cdot 24\cdot 10^8} - 10^{5\cdot 10^9} + 10^{10^{10}} > 0.$$

Ak $n = 10^{10}$, tak $-10^{10^{10}} \leqq r \leqq -5^{10^{10}}$, a potom

$$7^{7^7} . r^3 + 8^{8^8} . r^2 s + 9^{9^9} . r s^2 + 10^{10^{10}} . s^3 <$$
$$< - 7^{7^7} . 5^{3 \cdot 10^{10}} + 8^{8^8} . 10^{2 \cdot 10^{10}} . 7^{7^7} + 0 + 10^{10^{10}} . 7^{3 . 7^7} <$$
$$< - 10^{0 \cdot 7^7 + 0.698 \cdot 3 \cdot 10^{10}} + 10^{8^8 + 2 \cdot 10^{10} + 7^7} + 0 + 10^{10^{10} + 3 . 7^7} <$$
$$< - 10^{2094 \cdot 10^7} + 10^{2003 \cdot 10^7} + 10^{1001 \cdot 10^7} < 0.$$

**Teda (4) neplatí, a preto rovnica (1) nemá racionálny koreň.**

# 11. INÉ ÚLOHY

**Úloha 11.1.** Dokážte, že existuje $10^{10}$ po sebe idúcich zložených prirodzených čísel menších než $10^{10^{10}}$.

*Riešenie I.* Pre každé prirodzené číslo $x$ označme $P(x)$ súčin všetkých prvočísel nepresahujúcich $x$. Uvažujme konečnú postupnosť

$$P(10^{10}) - 10^{10} - 1,\ P(10^{10}) - 10^{10},\ \ldots,$$
$$P(10^{10}) - 3,\ P(10^{10}) - 2.$$

Pretože zrejme $P(10^{10}) > 2.10^{10} + 1$, sú všetky jej členy celé čísla väčšie než $10^{10}$. Každý z nich má prvočíselný deliteľ menší než $10^{10}$ (pre prvý člen môžeme vziať 101 a pre každý ďalší člen $P(10^{10}) - i$ niektorý prvočíselný deliteľ čísla $i$), sú to teda zložené čísla. Ostáva len ukázať, že sú menšie než $10^{10^{10}}$ a na to stačí dokázať nerovnosť $P(10^{10}) < 10^{10^{10}}$.

Pre každé prirodzené číslo $n$ je číslo $\binom{2n}{n}$ deliteľné všetkými prvočíslami $p$ medzi $n$ a $2n$. Skutočne, ak $n < p < 2n$, tak $p \mid (2n)!$, ale $p \nmid n!$, a preto $p \mid \dfrac{(2n)!}{(n!)^2}$.

Využitím tejto vlastnosti a nerovnosti $\binom{2n}{n} < 2^{2n}$ pre $n = 5.10^9$, $25.10^8$ a $125.10^7$ postupne dostávame

$$P(10^{10}) \leqq \binom{10^{10}}{5\,.\,10^9}.P(5\,.\,10^9) < 2^{10^{10}}.P(5\,.\,10^9) \leqq$$

$$\leqq 2^{10^{10}}.\binom{5\,.\,10^9}{25\,.\,10^8}.P(25\,.\,10^8) < 2^{10^{10}+5\cdot 10^9}.P(25\,.\,10^8) \leqq$$

$$\leqq 2^{15\cdot 10^9}.\binom{25\,.\,10^8}{125\,.\,10^7}.P(125\,.\,10^7) < 2^{175\cdot 10^8}.P(125\,.\,10^7).$$

Pre každé $k \geqq 1$ je z 30 po sebe idúcich čísel $30k + i$, $0 \leqq i \leqq 29$ najviac $\varphi(30) = 8$ prvočísel; každé z ostatných 22 čísel totiž je deliteľné dvoma, tromi alebo piatimi. Preto počet prvočísel menších než $125\,.\,10^7$ nepresahuje

$$30 + \left[\frac{125\,.\,10^7}{30}\right].8 < 30 + 42\,.\,10^6.8 < 34\,.\,10^7,$$

teda platí

$$P(125\,.\,10^7) < (125\,.\,10^7)^{34\cdot 10^7} < (10^{10})^{34\cdot 10^7} = 10^{34\cdot 10^8}.$$

Spolu potom dostávame

$$P(10^{10}) < 2^{175\cdot 10^8}.10^{34\cdot 10^8} < 8^{60\cdot 10^8}.10^{34\cdot 10^8} <$$

$$< 10^{60\cdot 10^8+34\cdot 10^8} < 10^{10^{10}},$$

čo bolo treba dokázať. □

Riešenie by sme mohli podstatne skrátiť využitím vzorca $P(n) \leqq 4^n$ platného pre všetky $n \in \mathsf{P}$; podstatnú ideu z jeho dôkazu sme v riešení vlastne uviedli. Ďalšie riešenie, ktoré uvedieme, bude kratšie a dosiahneme podstatne silnejšie tvrdenie než sa žiada v úlohe. Jeho nevýhodou však je, že sa v ňom používajú podstatne silnejšie matematické vety. Preto napríklad v MO a podobných súťažiach by bolo vhodnejšie prvé riešenie.

*Riešenie II.* Označme $A$ počet prvočísel menších než $B = 10^{10^{10}}$. Tieto prvočísla rozdelia ostatných $B - A$ prirodzených čísel nepresahujúcich $B$ do $A$ neprázdnych intervalov po sebe idúcich celých čísel (medzi 2, 3 je totiž prázdny interval). Teda aspoň jeden z nich obsahuje aspoň $\left[\frac{B-A}{A}\right] = \left[\frac{B}{A}\right] - 1$ čísel. Avšak $A \leqq \frac{B}{\ln B - 4}$, a preto

$$\left[\frac{B}{A}\right] - 1 \geqq \left[\frac{B}{\frac{B}{\ln B - 4}}\right] - 1 = [\ln B] - 5 =$$

$$= [10^{10} \ln 10] - 5 \geqq 2{,}3 . 10^{10}.$$

Teda existuje aspoň $2{,}3 . 10^{10}$ po sebe idúcich zložených prirodzených čísel menších než $10^{10^{10}}$. □

**Úloha 11.2.** Dokážte, že číslo $B + 1$, kde $B = 10^{10^{10}}$, nemá prvočíselný deliteľ menší než 12 000.

*Riešenie.* Predpokladajme, že $p$ je prvočíslo, $p \mid (B + 1)$. Potom platí $10^{10^{10}} \equiv -1 \pmod p$, $10^{2 \cdot 10^{10}} \equiv 1 \pmod p$. Zrejme $D(10, p) = 1$, a potom z malej Fermatovej vety vyplýva $10^{p-1} \equiv 1 \pmod p$. Podľa Euklidovho algoritmu existujú celé čísla $x$, $y$ také, že platí

$$D(3 . 10^{10}, p - 1) = x . 2 . 10^{10} - y . (p - 1);$$

ľahko možno tiež zariadiť $x, y \in \mathbb{N}$.
Potom platí

$$10^{x . 2 . 10^{10}} \equiv 10^{y . (p-1)} \pmod p,$$

a odtiaľ

$$10^{D(2 . 10^{10}, p-1)} \equiv 1 \pmod p.$$

Na druhej strane máme

$$10^{D(10^{10}, p-1)} \not\equiv 1 \pmod p, \text{ lebo } 10^{10^{10}} \not\equiv 1 \pmod p,$$

a preto

$$D(10^{10}, p-1) \neq D(2.10^{10}, p-1).$$

To je možné len tak, že platí $2^{11} | (p-1)$, t. j. $p$ je tvaru $2048k + 1$. Avšak žiadne číslo tohto tvaru menšie než 12 000 (t. j. pre $k \leqq 5$) nie je prvočíslo, pretože

$$3|2049, \ 17|4097, \ 5|6145, \ 3|8193, \ 7|10\,241.$$

Preto $p \geqq 2048.6 + 1 > 12\,000$, čo bolo treba ukázať. □

Keby sme chceli odhad 12 000 zvýšiť na 24 000, museli by sme okrem iného dokázať, že 12 289 a 18 433 nie sú delitele čísla $B + 1$. To by sme mohli najľahšie urobiť tak, že by sme vypočítali čísla $B$ MOD 12 289, $B$ MOD 18 433 za predpokladu, že 12 289, 18 433 sú prvočísla. Pri týchto výpočtoch by sme použili malú Fermatovu vetu. Pritom by sme nemuseli overovať, že 12 289, 18 433 sú skutočne prvočísla; ak by totiž boli zložené, určite by nedelili číslo $B + 1$.

**Úloha 11.3.** Dokážte, že číslo $B + 1$, kde $B = 10^{10^{10}}$, má aspoň jedenásť rôznych prvočíselných deliteľov.

*Riešenie.* Označme $A_i = 10^{2^{10}.5^i}$ (teda $B = A_{10}$). Pre každé $i \in \mathbb{N}$ platí

$$A_{i+1} + 1 = (A_i^4 - A_i^3 + A_i^2 - A_i + 1).(A_i + 1)$$

(my však tento rozklad potrebujeme len pre $i = 9, 8, \ldots, 0$). Označme $C_i = A_i^4 - A_i^3 + A_i^2 - A_i + 1$. Platí

$$C_i - (A_i^3 - 2A_i^2 + 3A_i - 4).(A_i + 1) = 5,$$

teda ak nejaké prvočíslo $p$ delí $C_i$ aj $A_i + 1$, tak $p|5$, teda $p = 5$. Avšak $5 \nmid A_i + 1$, a preto sú čísla $A_i + 1, C_i$ nesúdeliteľné. Potom je $C_i$ nesúdeliteľné aj s každým deliteľom čísla $A_i + 1$. Teda

$$B + 1 = C_9C_8C_7C_6C_5C_4C_3C_2C_1C_0.(A_9 + 1)$$

je rozklad čísla $B + 1$ na jedenásť po dvoch nesúdeliteľných činiteľov (zrejme väčších než 1). Každý z nich má prvočíselný deliteľ, pričom tieto delitele sú po dvoch rôzne. Teda $B + 1$ má aspoň jedenásť prvočíselných deliteľov. $\square$

**Úloha 11.4.** Nech $B = 10^{10^{10}}$ a $\varphi$ znamená Eulerovu funkciu. Rozhodnite, ktoré z čísel $\varphi(B)$, $\varphi(B + 1)$ je väčšie.

*Riešenie.* Pre každé $x \in \mathbb{N}$ platí

$$\varphi(x) = x.\prod_{p|x}\left(1 - \frac{1}{p}\right)$$

(súčin sa berie cez všetky prvočíselné delitele $x$). Podľa tohoto vzorca

$$\varphi(B) = B.\left(1 - \frac{1}{2}\right)\cdot\left(1 - \frac{1}{5}\right) = \frac{2}{5}B.$$

Odhadneme teraz $\varphi(B + 1)$ zdola. Na to rozložíme množinu $\mathsf{Q}$ všetkých prvočíselných deliteľov čísla $B + 1$ do štyroch množín

$$\mathsf{Q}_1 = \{p \in \mathsf{Q}; p \leqq 10^6\},\ \mathsf{Q}_2 = \{p \in \mathsf{Q}; 10^6 < p \leqq 10^8\},$$

$$\mathsf{Q}_3 = \{p \in \mathsf{Q}; 10^8 < p \leqq 10^{10}\}; \mathsf{Q}_4 = \{p \in \mathsf{Q}; 10^{10} < p\}.$$

Potom zrejme platí

$$\varphi(B+1) = (B+1) . \prod_{p \in Q_1} \left(1 - \frac{1}{p}\right) . \prod_{p \in Q_2} \left(1 - \frac{1}{p}\right) .$$
$$. \prod_{p \in Q_3} \left(1 - \frac{1}{p}\right) . \prod_{p \in Q_4} \left(1 - \frac{1}{p}\right) .$$

Odhadneme súčiny na pravej strane; budeme pritom využívať výsledok získaný v úlohe 11.2, že každý prvočíselný deliteľ čísla $B + 1$ je tvaru $2048k + 1$ a väčší než 10 000. Podľa toho možno každý činiteľ v prvom súčine odhadnúť zdola číslom $1 - \frac{1}{10^4}$; činitele v ostatných troch súčinoch možno po rade zdola odhadnúť číslami $1 - \frac{1}{10^6}$, $1 - \frac{1}{10^8}$, $1 - \frac{1}{10^{10}}$. Vzhľadom na vyššieuvedený tvar prvočíselných deliteľov čísla $B + 1$ mohutnosti množín $Q_1$, $Q_2$, $Q_3$ po rade neprevýšia 500, $5 . 10^4$, $5 . 10^6$. Mohutnosť $n$ množiny $Q_4$ odhadneme zo vzťahu $\prod_{p \in Q_4} p \leqq B + 1$. Odtiaľ vyplýva $(10^{10})^n \leqq B$, teda $10n \leqq 10^{10}$, teda $n \leqq 10^9$. Preto platí

$$\varphi(B+1) > (B+1) . \left(1 - \frac{1}{10^4}\right)^{500} . \left(1 - \frac{1}{10^6}\right)^{5 . 10^5} .$$
$$. \left(1 - \frac{1}{10^8}\right)^{5 . 10^6} . \left(1 - \frac{1}{10^{10}}\right)^{10^9} ,$$

$$\varphi(B+1) > (B+1) . \left(1 - \frac{500}{10^4}\right) . \left(1 - \frac{5 . 10^4}{10^6}\right) .$$
$$. \left(1 - \frac{5 . 10^6}{10^8}\right) . \left(1 - \frac{10^9}{10^{10}}\right) ,$$

$$\varphi(B+1) > (B+1) .$$
$$. \left(1 - \frac{500}{10^4} - \frac{5 . 10^4}{10^6} - \frac{5 . 10^6}{10^8} - \frac{10^9}{10^{10}}\right) ,$$

$$\varphi(B + 1) > \frac{3}{4}(B + 1) > \frac{2}{5}B.$$

**Teda platí** $\varphi(B + 1) > \varphi(B)$. □

**Úloha 11.5.** Pre číslo $B = 10^{10^{10}}$ dokážte nerovnosť

$$\varphi(B + 1) > 0{,}98.(B + 1).$$

Túto úlohu necháme na vyriešenie čitateľovi. Jedna z možností zlepšovania odhadu z predchádzajúcej úlohy je rozdeliť množinu Q na viac podmnožín. Ďalej možno využiť, že niektoré z čísel tvaru $2048k + 1$ majú deliteľa 3 alebo 5.

**Úloha 11.6.** Zistite, koľkokrát sa číslo $B = 10^{10^{10}}$ nachádza v Pascalovom trojuholníku.

*Riešenie.* Máme vlastne zistiť počet usporiadaných dvojíc $(x, y)$ takých, že $0 \leqq y \leqq x$ a

$$\binom{x}{y} = B\,.$$

Také sú zrejme dvojice $(B, 1)$, $(B, B - 1)$. Ukážeme, že ďalšie dvojice $(x, y)$ už nevyhovujú; z dôvodov symetrie Pascalovho trojuholníka sa môžeme obmedziť na prípad $0 \leqq 2y \leqq x$. Prípad $y = 0$ zrejme nevyhovuje a prípad $y = 1$ dáva $x = B$ (čo už máme). Preto stačí skúmať $y \geqq 2$.

Pretože $5^{10^{10}} \mid \binom{x}{y}$, pri sčítaní čísel $x - y$, $y$ v sústave o základe 5 nastáva aspoň $10^{10}$ prenosov, a teda číslo $x$ je v tejto sústave aspoň $(10^{10} + 1)$-ciferné, t. j. $x \geqq \geqq \left(5^{10^{10}}\right)$. Potom však $y \geqq 2$ dáva

$$\binom{x}{y} \geqq \binom{5^{10^{10}}}{2} = \frac{5^{10^{10}}.(5^{10^{10}} - 1)}{2} > 10^{10^{10}},$$

teda takto nedostaneme ďalšie výskyty čísla $B$. Preto sa číslo $B$ nachádza v Pascalovom trojuholníku práve dvakrát, a to ako

$\binom{B}{1}$ a ako $\binom{B}{B-1}$. □

**Úloha 11.7.** Zistite, koľkokrát sa číslo $A = \binom{10\,000}{3\,000}$ nachádza v prvých 50 000 riadkoch Pascalovho trojuholníka.

*Riešenie.* Máme vlastne zistiť počet usporiadaných dvojíc $(x, y)$ takých, že $x < 50\,000$ a $\binom{x}{y} = A$. Dve také dvojice sú (10 000, 3000) a (10 000, 7000), a pre $x = 10\,000$ už ďalšie také dvojice zrejme neexistujú. Ukážeme sporom, že neexistujú ani pre ostatné $x < 50\,000$. Na to predpokladajme $\binom{x}{y} = A$ a označme $z = x - y$; zrejme smieme predpokladať $y \leqq z$. Teraz rozlíšme dva prípady podľa toho, či je $x$ menšie alebo väčšie než 10 000.

*Prípad I.* Ak $x < 10\,000$, tak $y > 3000$; inak by bolo $\binom{x}{y} < A$. Uvážme teraz prvočíslo $p = 3001$. Pretože

$$\left[\frac{10\,000}{p}\right] > \left[\frac{7000}{p}\right] + \left[\frac{3000}{p}\right],$$

platí $p|A$, a teda aj $p\left|\binom{x}{y} = \frac{x!}{y!z!}\right.$.

Avšak $z \geqq y \geqq p$, a preto $p|y!$, $p|z!$, a teda $p^3|x!$, teda $x \geqq 3p = 9003$.
Teraz uvážme prvočíslo $q = 6997$. Pretože

$$\left[\frac{10\,000}{q}\right] = 1 = \left[\frac{7000}{q}\right] + \left[\frac{3000}{q}\right]$$

(a $q^2 > 10\,000$, teda násobky čísel $q^2$, $q^3$, ... sa tu nevyskytnú), platí $q \nmid A$. Avšak $q|x!$, a preto $q|y!$ alebo $q|z!$. Pretože $z \geqq y$, platí $q|z!$, a teda $z \geqq q = 6997$. Teraz znova uvážme $p = 3001$. Platí $z \geqq 2p$, a preto $p^2|z!$. Keďže $p|y!$ a $p\left|\frac{x!}{y!z!}\right.$, musí platiť $p^4|x!$. Teda $x \geqq 4p$, a to je spor s predpokladom $x < 10\,000$.

*Prípad II*. Nech teraz $x > 10\,000$; potom $y < 3000$. Uvážme teraz prvočíslo $p = 7001$. Platí $p|A$, $p|z!$, a preto $p^2|x!$, teda $x \geqq 2p = 14\,002$. (Opakujú sa úvahy z prípadu I, preto ich už zapisujeme stručnejšie.)

Teraz uvážme prvočíslo $p_1 = 9973$. Pretože $z = x - y > p_1$, platí $p_1|z!$. Avšak $p_1|A$, a preto $p_1^2|x!$, teda $x \geqq 2p_1 = 19\,946$.

Už vieme $z \geqq 19\,946 - 2999 = 16\,947$. Uvážme teraz prvočíslo $p_2 = 8467$. Platí $z \geqq 2p_2$, teda $p_2^2|z!$, a pretože $p_2|A$, platí $p_2^3|x!$, teda $x \geqq 3p_2 = 25\,401$.

Ďalej uvážime prvočíslo $p_3 = 9967$. Platí $z \geqq 25\,401 - 2999 > 2p_3$, teda $p_3^2|z!$, Kežďe $p_3|A$, máme $p_3^3|x!$, teda $x \geqq 3p_3 = 29\,901$. Teraz položme $p_4 = 8967$. Znova platí $p_4|A$ a pretože $z = x - y \geqq 26\,902 > 3p_4$, platí $p_4^3|z!$, a potom $p_4^4|x!$, teda $x \geqq 4p_4 = 35\,868$. Úplne obdobne pre $p_5 = 8209$ zistíme $p_5^4|z!$, $p_5^5|x!$, a teda $x \geqq 5p_5 = 41\,045$. Teraz zvolíme $p_6 = 9511$ a zistíme $p_6^4|z!$, $p_6^5|x!$, teda $x \geqq 5p_6 > 47\,555$. Nakoniec zvoľme $p_7 = 8893$. Pretože $z \geqq 5p_7$, platí $p_7^5|z$, a pretože $p_7|A$, platí potom $p_7^6|x!$, teda $x \geqq 6p_7 > 50\,000$. Ani tento prípad teda nedáva žiadne ďalšie výskyty čísla $A$ v prvých 50 000 riadkoch Pascalovho trojuholníka.

Teda v uvedených riadkoch sa číslo $A$ nachádza práve dvakrát, a to ako $\binom{10\,000}{3000}$ a $\binom{10\,000}{7000}$. □

Nebolo by príliš ťažké ďalej zvyšovať dolný odhad pre $x$ a dokázať napríklad, že číslo $A$ sa už ďalšíkrát nenachádza v prvých 100 000 riadkoch Pascalovho trojuholníka. Vystačili by sme pritom s tabuľkou prvočísel do 10 000 ako doteraz. S využitím istého faktu z odseku 3.3 však možno dôjsť podstatne ďalej.

**Úloha 11.8.** Dokážte, že číslo $A = \binom{10\,000}{3000}$ sa nachádza v prvých desiatich miliónoch riadkov Pascalovho trojuholníka práve dvakrát.

*Riešenie.* Nech $x$, $y$, $z$ majú rovnaký význam ako v riešení predchádzajúcej úlohy. Z tohto riešenia vieme, že pre $x \leqq 14\,000$ existujú práve dve riešenia rovnice $\binom{x}{y} = A$. (Teda z prípadu II nám stačí len úvaha s $p = 7001$.) Nech odteraz $14\,000 < x \leqq 10^7$. Pretože

$$\binom{x}{154} \leqq \binom{10^7}{154} < (10^7)^{154} = 10^{1078} < 3^{3000} <$$

$$< \frac{10\,000}{3\,000} \cdot \frac{9999}{2999} \cdot \ldots \cdot \frac{7002}{2} \cdot \frac{7001}{1} = \binom{10\,000}{3\,000},$$

musí byť $y > 154$. Podľa vety 3.4, bod b však potom existuje prvočíslo $p$, $x - y < p \leqq x$. Potom $p \mid \binom{x}{y}$, ale $p \nmid A$ (pretože $p > x - y > 14\,000 - 3000 > 10\,000$), a preto $\binom{x}{y} \neq A$. Teda číslo $A$ sa od 14 000-ho po $10^7$-ty riadok Pascalovho trojuholníka už nenachádza, čo bolo treba dokázať. □

Toto riešenie je kratšie než vyššieuvedené riešenie (ľahšej) úlohy 11.7. ale využívali sme v ňom istý fakt o prvočíslach, ktorého overenie bez počítača by bolo namáhavé, aj keby sme mali k dispozícii tabuľky prvočísel po $10^7$.

Pre nasledujúcu úlohu pripomeňme, že mrežové body v rovine (s danou pravouhlou súradnicovou sústavou) sú jej body s celočíselnými súradnicami.

**Úloha 11.9.** Určte počet mrežových bodov na kružnici s polomerom $B = 10^{10^{10}}$ a stredom v začiatku súradnicovej sústavy.

*Riešenie.* Rovnica uvažovanej kružnice je $x^2 + y^2 = B^2$. Ak obvyklým spôsobom priradíme komplexné čísla bodom roviny, tak máme vlastne určiť počet gaussovských celých čísel $a + b\mathrm{i}$ takých, že $a^2 + b^2 = B^2$, t. j. $|a + b\mathrm{i}| = B$.
Rozklad čísla $B^2$ na gaussovské prvočísla je

$$B^2 = (1 + \mathrm{i})^{4\cdot 10^{10}}.(2 + \mathrm{i})^{2\cdot 10^{10}}.(2 - \mathrm{i})^{2\cdot 10^{10}}.$$

Ak $a^2 + b^2 = B^2$, tak $(a + b\mathrm{i})|B^2$, preto

$$a + b\mathrm{i} = \mathrm{i}^k.(1 + \mathrm{i})^r.(2 + \mathrm{i})^s.(2 - \mathrm{i})^t$$

pre nejaké celé čísla $k$, $r$, $s$, $t$,

$$0 \leqq k \leqq 3,\ 0 \leqq r \leqq 4.10^{10},\ 0 \leqq s \leqq 2.10^{10},$$
$$0 \leqq t \leqq 2.10^{10}.$$

(Pritom toto vyjadrenie je jednoznačné.)
Ďalšiu podmienku na $r$, $s$, $t$ dostaneme zo vzťahu

$$a - b\mathrm{i} = (-\mathrm{i})^k.(1 - \mathrm{i})^r.2\,(-\mathrm{i})^s.(2 + \mathrm{i})^t;$$

potom

$$B^2 = (a + bi).(a - bi) = 2^r.5^{s+t}.$$

Odtiaľ vidno $r = 2.10^{10}$, $t = 2.10^{10} - s$. Teda vo vyjadrení pre $a + bi$ možno voliť len $k$, $s$; parametre $r$, $zt$ sú už potom jednoznačne určené. Možností pre voľbu $k$, $s$ spolu je

$$4.(2.10^{10} + 1) = 8.10^{10} + 4,$$

a ľahko sa preverí, že každá už vyhovuje. Teda na kružnici s polomerom $B$ a stredom v začiatku súradnicovej sústavy leží $8.10^{10} + 4$ mrežových bodov. $\square$

# LITERATÚRA


[1] *J. Brož - V. Roskovec - M. Valouch:* Fyzikální a matematické tabulky. Praha, SNTL 1980.

[2] *H. Davenport:* Vysšaja arifmetika. Moskva, Nauka 1965.

[3] *U. S. Davydov - Š. Znám:* Teória čísel. Základné pojmy a zbierka úloh. Bratislava, SPN 1966.

[4] *A. Kufner:* Nerovnosti a odhady. ŠMM 39, 1975.

[5] *A. J. Markuševič:* Rekurentní posloupnosti. Praha, SNTL 1954.

[6]) *W. Sierpiński:* Teoria liczb. Warszawa — Wroclaw, 1950.

[7]) *W. Sierpiński:* Teoria liczb II. Warszawa, PWN 1959.

[8] *M. Valouch - M. A. Valouch:* Sedmimístné logaritmy čísel od 1 do 120 000. Praha, JČSMF 1932.

[9] *M. Valouch - M. A. Valouch:* Sedmimístné logaritmy čísel od 1 do 110 000 a goniometrických funkcí v šedesátinném dělení. Praha, NČSAV 1956.

[10] *I. M. Vinogradov:* Základy theorie čísel. Praha, NČSAV 1953.

[11] *A. Vrba:* Princip matematické indukce. ŠMM 40, 1977.

[12] *A. Vrba:* Kombinatorika. ŠMM 45, 1980.

[13] *Š. Znám:* Teória čísel. Bratislava, Alfa 1977.

[14] *L. Schoenfeld:* Sharper bounds for the Chebyshev functions $\vartheta(x)$ and $\psi(x)$, II. Math. Computation *30* (1976), n. 143, 337—360.

Seznam dosud vydaných svazků edice

ŠKOLA MLADÝCH MATEMATIKŮ

v nakladatelství Mladá fronta

---

1. *František Hradecký - Milan Koman - Jan Vyšín:* Několik úloh z geometrice jednoduchých těles, 1961, 1963 a 1977
2. *Jiří Sedláček:* Co víme o přirozených číslech, 1961, 1965 a 1976
3. *Jaroslav Šedivý:* Shodná zobrazení v konstruktivních úlohách, 1962
4. *Miroslav Šisler - Jiří Jarník:* O funkcích, 1962 a 1963
5. *František Veselý:* O nerovnostech, 1963
6. *Rudolf Výborný:* Matematická indukce, 1963 a 1966
7. *Jaroslav Šedivý:* O podobnosti v geometrii, 1963 a 1967
8. *Jiří Váňa:* O rovnicích s parametry, 1964 a 1970
9. *Jan Vyšín:* Konvexní útvary, 1964
10. *Jiří Sedláček:* Faktoriály a kombinační čísla, 1964
11. *Josef Holubář:* Geometrická místa bodů v prostoru, 1965
12. *Karel Havlíček:* Prostory o čtyřech a více rozměrech, 1965
13. *Miroslav Šisler - Josef Andrys:* O řešení algebraických rovnic, 1966
14. *František Veselý:* O dělitelnosti čísel celých, 1966
15. *Milan Koman:* Jak vyšetřujeme geometrická místa metodou souřadnic, 1966
16. *Stanislav Horák:* Kružnice, 1966
17. *Jaromír Hroník:* Úlohy o maximech a minimech funkcí, 1967
18. *Karel Havlíček:* Analytická geometrie a nerovnosti, 1967
19. *Jiří Jarník:* Komplexní čísla a funkce, 1967
20. *Bruno Budinský - Stanislav Šmakal:* Goniometrické funkce, 1968

21. *Alois Apfelbeck:* Kongruence, 1968
22. *Tibor Šalát:* Dokonalé a spriatelené čísla, 1969
23. *Jaroslav Morávek - Milan Vlach:* Oddělitelnost množin, 1969
24. *Ján Gatial - Milan Hejný:* Stavba Lobačevského planimetrie, 1969
25. *Leo Bukovský - Igor Kluvánek:* Dirichletov princíp, 1970
26. *Karel Hruša:* Polynomy v moderní algebře, 1970
27. *Stanislav Horák:* Mnohostěny, 1970
28. *Bruno Budinský - Stanislav Šmakal:* Vektory v geometrii, 1971
29. *František Zítek:* Vytvořující funkce, 1972
30. *Milan Koman - Jan Vyšín:* Malý výlet do moderní matematiky, 1972 a 1974
31. *Oldřich Odvárko:* Booleova algebra, 1973
32. *Jan Vyšín - Jitka Kučerová:* Druhý výlet do moderní matematiky, 1973
33. *Jaroslav Morávek:* O dynamickém programování, 1973
34. *Ladislav Rieger:* O grupách, 1974
35. *Alois Kufner:* Co asi nevíte o vzdálenosti, 1974
36. *Ján Černý:* O aplikáciach matematiky, 1976
37. *Beloslav Riečan - Zdena Riečanová:* O pravdepodobnosti, 1976
38. *Juraj Bosák:* Latinské štvorce, 1976
39. *Alois Kufner:* Nerovnosti a odhady, 1975
40. *Antonín Vrba:* Princip matematické indukce, 1977
41. *Bohdan Zelinka:* Rovinné grafy, 1977
42. *Ladislav Beran:* Uspořádané množiny, 1978
43. *Jiří Jarník:* Posloupnosti a řady, 1979
44. *Bohdan Zelinka:* Matematika hrou i vážně, 1979
45. *Antonín Vrba:* Kombinatorika, 1980
46. *Jaroslav Šedivý:* Shodnost a podobnost v konstrukčních úlohách, 1980
47. *Arnošt Niederle:* Zajímavé dvojice trojúhelníků, 1980
48. *František Veselý:* O nerovnostech a nerovnicích, 1982

49. *Pavel Vít:* Řetězové zlomky, 1982
50. *Adam Płocki:* O náhodě a pravděpodobnosti, 1982
51. *N. B. Vasiljev - V. L. Gutenmacher:* Přímky a křivky, 1982
52. *Alois Kufner:* Symetrické funkce, 1982
53. *Ján Gatial - Tomáš Hecht - Milan Hejný:* Hry takmer matematické, 1982
54. *Josef Holubář:* Množiny bodů v prostoru, 1983
55. *Ljubomir Davidov:* Funkcionální rovnice, 1984
56. *Jiří Sedláček:* Faktoriály a kombinační čísla, 1985
57. *Stanislav Horák:* Nerovnosti v trojúhelníku, 1986
58. *Herbert Kästner - Peter Göthner:* Algebra, každý začátek je lehký, 1986
59. *Jaroslav Morávek - Milan Vlach:* Oddělitelnost množin, 1987
60. *Jiří Tůma:* Matematické hlavolamy a základy teorie grup, 1988

# OBSAH

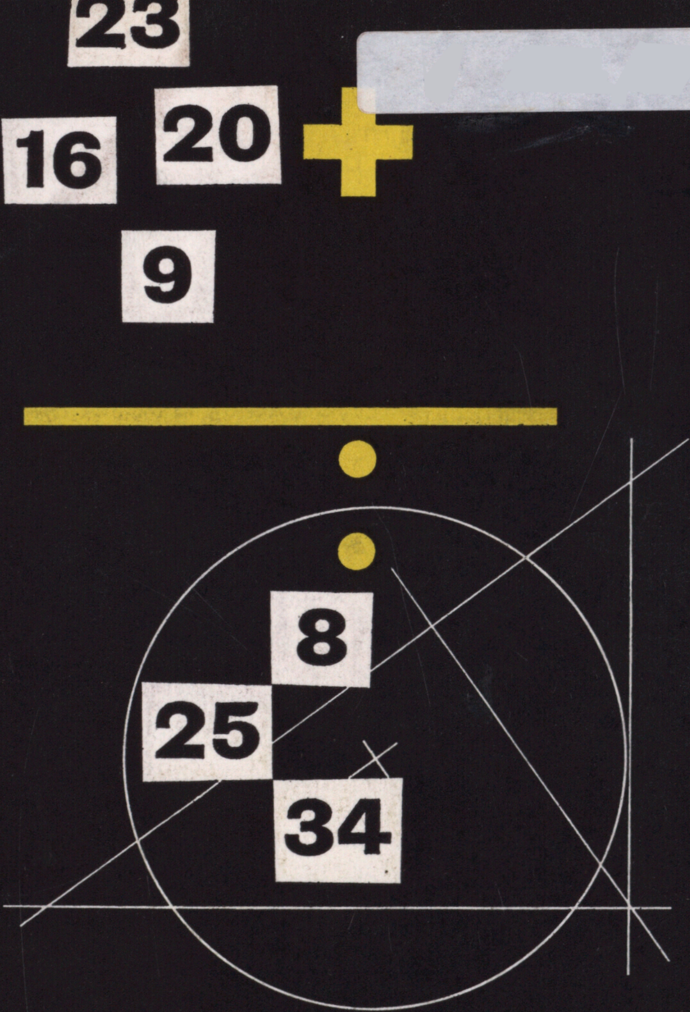
ŠKOLA MLADÝCH MATEMATIKŮ

IVAN KOREC

# Úlohy o veľkých číslach

Pro účastníky matematické olympiády
vydává ÚV matematické olympiády
v nakladatelství Mladá fronta
Řídí akademik Josef Novák
Obálku navrhl Jaroslav Příbramský
K tisku připravil Vladimír Doležal
Technický reaktor Vladimír Vácha
Odpovědná redaktorka Blanka Fučíková
Publikace číslo 5021
Edice Škola mladých matematiků, svazek 61
Vytiskl Mír, novinářské závody, n. p.
závod 1, Praha 1, Václavské nám. 15
5,18 AA, 5,65 VA, 1. vydání, 136 stran.
Náklad 4500 výtisků. Praha 1988. 508/21/82.5

23-087-88 03/2 Cena brož. výtisku 7 Kčs




23 - 087 - 88
03/2
Cena brož
7 Kčs