3. Prehľad viet z teórie čísel

In: Ivan Korec (author): Úlohy o veľkých číslach. (Slovak). Praha: Mladá fronta, 1988. pp. 10–45.

Persistent URL: http://dml.cz/dmlcz/404180

3. PREHĽAD VIET Z TEÓRIE ČÍSEL

1. ZÁKLADNÉ OZNAČENIA A ČÍSELNÉ SÚSTAVY

Množinu všetkých celých nezáporných čísel budeme označovať N a množinu všetkých celých kladných čísel budeme označovať 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 Z, resp. 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 ako 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 Σ, Π 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 $\sum_{p \leq K}$, $\prod_{p \leq K}$ 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 $1{,}95 \leqq x \leqq 2{,}05$.

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 $0 \leq a_i < z$ 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 číslicach 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.

Podotkneme 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 číslicach, a prípadne počítať konečné úseky týchto rozvojov.

V textoch úloh zásadne hovoríme o číslicach čísla x namiesto presnejšieho, no zdĺhavejšieho vyjadrovania sa o číslicach 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 $a.c = b$. Budeme písať $a \nmid b$, ak neplatí $a|b$.

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

$$a = b.q + r \quad a \quad 0 \leq r < b.$$

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

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

(ktoré v podstate preberáme z programovacieho jazyka PASCAL). Symboly DIV a MOD sú symboly čiastočných operácií na množine $\mathbf{Z}$, a budeme ich písať medzi ich argumenty, obdobne ako $+, -, \ldots$ Výraz $a.b \text{ MOD } m$ budeme vždy rozumieť ako $(a.b) \text{ MOD } m$; vo výraze $a.(b \text{ MOD } m)$ teda nesmieme vynechať zátvorku. Naproti tomu, $a + b \text{ MOD } m$ znamená $a + (b \text{ MOD } m)$. 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* $a, b \in \mathbf{Z}, m, n \in \mathbf{P}$ *platí*

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

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* $a, b, c \in \mathbf{Z}$ *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 $a \geq b > 0$, $c = a$ DIV DIV b) možno určiť $D(a, b)$ pre každé $a, b \in \mathbf{N}$; 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* $a, b \in \mathbf{Z}$, $a \neq 0$ *alebo* $b \neq 0$, *tak* $D(a, b)$ *je najmenšie kladné celé číslo, ktoré sa dá vyjadriť v tvare* $x.a + y.b$, $x, y \in \mathbf{Z}$. *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 treticho 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* $x, y, z \in \mathbf{Z}$ *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 binára operáciu.

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

Veta 2.9. *Nech* $a, b, c \in \mathbf{Z}$, *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 $i, j, m \in \mathbf{P}$. 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

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

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.

8. 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, ...

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 $\lfloor \sqrt{a} \rfloor$. 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* $n \geq 55$ *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* $n \geq 2$ *existuje prvočíslo* p *medzi* n *a* $2n$ *(t. j.* $n < p < 2n$*).*

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

c) *Pre každé* $n \geq 7$ *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* $n \geq n_0$ *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*

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

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*

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

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* $k \mid e_i$, *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 φ 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 φ. 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 φ, τ, S vyjadrenú vo vete 4.4 nazývame *multiplikatívnosť*.

5. KONGRUENCIE A ZVYŠKOVÉ TRIEDY

Pre $a, b \in \mathbf{Z}$, $m \in \mathbf{P}$ 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* $m \in \mathbf{P}$ *je kongruentnosť modulo* m *reláciou ekvivalencie, t. j. pre každé,* $a, b, c \in \mathbf{Z}$ *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 $\{(a, b) \in \mathbf{Z} \times \mathbf{Z};\ a \equiv b (\mathrm{mod}\ m)\}$) je reláciou ekvivalencie na $\mathbf{Z}$, zodpovedá jej istý rozklad množiny $\mathbf{Z}$. 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* $a, b, c, d \in \mathbf{Z}$, $m \in \mathbf{P}$ *a platí*

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

tak platí aj

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

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* $a, b, c \in \mathbf{Z}$. $m \in \mathbf{P}$. *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 zvýškových 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, $m_2 \in \mathbf{P}$, a_1, $a_2 \in \mathbf{Z}$. *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*

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

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

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

Veta 5.5. *Sústava kongruencií*

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

má riešenie práve vtedy, keď

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

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

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

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*

$$ax + by = c, \tag{5.9}$$

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*

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

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 $D(a, m) \mid b$.

6. UMOCŇOVANIE ZVYŠKOVÝCH TRIED

Ak je $a \equiv b (\mathrm{mod}\ m)$, tak pre každé $n \in \mathbf{N}$ 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 $r, s \in \mathbf{P}$) 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 $a \in \mathbf{Z}$ platí*

(6.1) $$a^p \equiv a (\mathrm{mod}\ p).$$

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

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

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

Zovšeobecnenie vzorca (6.2) na prípad zloženého modulu dáva nasledujúca veta; φ 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*

(6.3) $$a^{\varphi(m)} \equiv 1\ (\mathrm{mod}\ m).$$

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 $a.b \equiv 1(\mathrm{mod}\ m)$). 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 $a^r \equiv 1(\mathrm{mod}\ m)$. (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

$$a^n \equiv 1(\mathrm{mod}\ m) \text{ práve vtedy, keď } r \mid n.$$

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

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

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

nazveme *index čísla* a a označíme ho $\mathrm{ind}\,(a)$. (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 $\mathrm{ind}\,(a)$ 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*:

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

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

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

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

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

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

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

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

Teda $\text{ind}\,(x) \in \{19, 39, 59\}$, 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

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

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

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 $\text{ind}\,(a)$ (pre modul m), a je kvadratický zvyšok podľa modulu m práve vtedy, keď $\text{ind}\,(a)$ 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 $3 | \mathrm{ind}\ (a)$. 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

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

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 $a, b \in \mathbf{Z}$, 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 $a, b \in \mathbf{Z}$, 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 $i \mid a$. 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* $a \in G - \{0\}$ *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* $e_1, \ldots, e_k \in P$. *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

$$0! = 1, \quad (n+1)! = n!.(n+1) \tag{9.1}$$

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

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

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*

$$n! = \prod_{p \leqq n} p^{e_p} \text{ kde } e_p = \sum_{k=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor \tag{9.3}$$

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 $m, n \in \mathbf{N}$, $m \leqq n$ 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) $$n! \doteq \sqrt{2\pi n}.\left(\frac{n}{e}\right)^n$$

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

$$< \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \cdot \left(1 + \frac{1}{11n}\right)$$

a pre všetky $n \geqq 8$

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

$$< \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \cdot \left(1 + \frac{1}{12n} + \frac{1}{288n^2}\right).$$

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

(9.8) $$\ln(n!) = n.(\ln n - 1) + \frac{1}{2}\ln(2\pi n) +$$

$$+ \frac{1}{12n} - \frac{1}{360n^3} + \frac{1}{1260n^5} - \frac{1}{1680n^7} + \frac{1}{1188n^9} - \dots$$

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

$$a_{n+2} = p.a_{n+1} + q.a_n. \tag{10.1}$$

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

$$x^2 = p.x + q \tag{10.2}$$

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

$$a_n = u.x_1^n + v.x_2^n. \tag{10.3}$$

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

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

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

$$a_n = u.x_1^n + v.nx_1^n, \tag{10.4}$$

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

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

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

$$a_n = u_1 . r^n \cos n\alpha + v_1 . r^n \sin n\alpha . \tag{10.5}$$

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

$$a_{n+k} = p_{k-1}a_{n+k-1} + p_{k-2}a_{n+k-2} + \ldots + p_0 a_n \tag{10.6}$$

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

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

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*

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

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

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

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

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

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

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

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

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

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

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**

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

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