Úvod do elementárnej teórie čísel

Milan Paštéka

1 Prirodzené a celé čísla, Matematické dôkazy

Začneme štúdiom základných množín. Symbolom $\mathbb{N} := \{1, 2, 3, \dots, \}$ budeme označovať množinu prirodzených čísel. Pre množinu celých čísel budeme používať symbol $\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \dots\}$.

Množina celých čísel má túto dôležitú a pritom jednoduchú vlastnosť: **Každá neprázdna zdola ohraničená podmnožina $\mathbb{Z}$ obsahuje najmenší prvok.**

Príklad 1. Pomocou tejto vlastnosti dokážeme sporom, že $\sqrt{2}$ nie je zlomok. Predpokladajme, že táto hodnota je zlomok. Teda

$$\sqrt{2} = \frac{p}{q} \tag{1}$$

pre nejaké $p, q \in \mathbb{N}$. Označme si M množinu všetkých kladných menovateľov q takých, že pre vhodné $p \in \mathbb{N}$ platí rovnosť (1). Podľa predpokladu máme $M \neq \emptyset$. Umocnrním a úpravou dostávame

$$2q^2 = p^2.$$

Z toho vyplýva, že p je párne číslo. Teda $p = 2p_1$. Po dosadení dostávame

$$2q^2 = 4p_1^2$$

a teda

$$q^2 = 2p_1^2.$$

Preto aj q musí byť párne. Položme $q = 2q_1$. Znovu po dosadení máme

$$4q_1^2 = 2p_1^2.$$

Po úprave máme

$$\sqrt{2} = \frac{p_1}{q_1}.$$

Pričom je zrejmé $q_1 < q$. Teda množina M ku každému prvku obsahuje menší prvok. To je spor. ∘

1.1 Delenie so zvyškom

Celé čísla sa dajú sčítať a násobiť. Trochu komplikovanejšia je otázka delenia. Jeden zo spôsobov je, že delením čísla a číslom $b \neq 0$ dostaneme zlomok $\frac{a}{b}$. Ten ale nie vždy nadobúda celočíselnú hodnotu. Iný spôsob delenia, známy už zo základnej školy, je delenie so zvyškom.

Veta 1. Ak $a \in \mathbb{Z}$ a $m \in \mathbb{N}$, tak existujú jednoznačne určené čísla $q \in \mathbb{Z}$ a $r \in \{0, \ldots, m-1\}$, pre ktoré platí rovnosť

$$a = mq + r\,.$$

Dôkaz. Množina $\{k \in \mathbb{Z}; km \leq a\}$ je zhora ohraničená. Označme q, jej najväčší prvok. Potom

$$qm \leq a < (q+1)m\,.$$

Preto hodnota $r = a - qm$ neprevyšuje $m-1$. Úpravou dostávame požadované vyjadrenie $a = qm + r$. Tým sme dokázali existenciu daného vyjadrenia a. Zostáva dokázať jeho jednoznačnosť. Predpokladajme, že $a = qm + r, a = q_1 m + r_1$. To znamená

$$qm + r = q_1 m + r_1\,. \tag{2}$$

Po úprave dostávame rovnosť

$$(q - q_1)m = r_1 - r\,.$$

Hodnota $r_1 - r$ je teda násobkom čísla m. Z predpokladov vyplýva $|r_1 - r| \in \{0, \ldots, m-1\}$. Táto množina však obsahuje iba jediný násobok m a to nulu. Preto $|r_1 - r| = 0$. To znamená, $r_1 = r$. Z toho vyplýva podľa (2), že aj $mq = mq_1$, a teda po vykrátení číslom m, dostávame $q_1 = q$. □

Číslo q z predchádzajúcej vety sa nazýva **neúplný podiel** a po delením a r sa nazýva **zvyšok** a po delením.

Príklad 2. Reálnemu číslu α sa dá priradiť celé číslo

$$[\alpha] := \max\{z \in \mathbb{Z}; \alpha \leq z\}.$$

Táto hodnota sa nazýva **celá časť** α. Hodnota $\{\alpha\} = \alpha - [\alpha]$ sa nazýva **zlomková časť** α. Vidíme, že $[\alpha] \in \mathbb{Z}$ a $\{\alpha\} \in [0, 1)$. Pre $a \in \mathbb{Z}, m \in \mathbb{N}$ platí

$$a = mq + r, r \in \{0, \ldots m-1\} \Leftrightarrow q = \left[\frac{a}{m}\right], r = m\left\{\frac{a}{m}\right\}.$$

∘

Príklad 3. Reálne čísla sa dajú vyjadriť v tvare g - dických rozvojov, $g \in \mathbb{N}, g > 1$. Každé číslo $\alpha \in [0, 1)$ sa dá jednoznačne vyjadriť

$$\alpha = \sum_{n=1}^{\infty} \frac{a_n}{g^n}, a_n \in \{0, \ldots, g-1\},$$

pričom pre nekonečne veľa n platí $a_n < g - 1$. Zjednodušene takéto vyjadrenie zapisujeme

$$\alpha = 0, a_1 a_2 a_3 \ldots .$$

Pri tomto vyjadrení sa dá dokázať $a_n = [g\{g^{n-1}\alpha\}]$.

Ak α je nenulové racionálne číslo, teda $\alpha = \frac{p}{q}, p, q \in \mathbb{N}$, tak

$$a_n = \Big[g\Big\{\frac{pg^{n-1}}{q}\Big\}\Big] = \Big[\frac{g}{q}q\Big\{\frac{pg^{n-1}}{q}\Big\}\Big].$$

Ak r_n bude zvyšok pg^{n-1} po delení q, tak podľa predošlého príkladu dostávame z poslednej rovnosti

$$a_n = \Big[\frac{g}{q}r_n\Big].$$

Príklad 4. Funkcia $\{x\}$ je periodická s periodou 1. Systém funkcií $1, \cos 2\pi x, \sin 2\pi x, \ldots, \cos 2n\pi x, \sin 2n\pi x, \ldots,$ je úpný ortonormálny systém. Keď si rozvinieme $\{x\}$ do Fourierovo radu, tak pre $x \in (0,1)$ platí

$$\{x\} = \frac{1}{2} - \sum_{n=1}^{\infty} \frac{1}{\pi n} \sin 2n\pi x.$$

S Parsevalovej rovnosti potom vyplýva

$$\frac{2}{3} = \frac{1}{2} + \sum_{n=1}^{\infty} \frac{1}{\pi^2 n^2}.$$

Z toho po úprave dostávame

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}. \tag{3}$$

Ak si uvedomíme nerovnosť

$$\sum_{n=N}^{\infty} \frac{1}{n^2} \leq \int_{N-1}^{\infty} \frac{dx}{x^2} = \frac{1}{N-1},$$

tak pre $N \in \mathbb{N}$ dostávame

$$\sum_{n=1}^{N} \frac{1}{n^2} = \frac{\pi^2}{6} + R_N. \tag{4}$$

kde $|R_N| \leq \frac{1}{N-1}$.

1.2 Deliteľnosť a delitele

Pripomenieme pojem deliteľnosti. Ak a, b sú celé čísla, tak hovoríme, že a **delí** b práve vtedy, keď b je celočíselným násobkom a. V tomto prípade hovoríme tiež, že a je **deliteľom** b, alebo aj b je **deliteľné** a. Budeme to označovať $a|b$. Je to teda vtedy, keď zvyšok a po delení $|b|$ je rovný 0.

Táto relácia má nasledujúce jednoduché vlastnosti: Ak a, b, c sú celé čísla, tak:

1) $a|a$**,**
2) $a|b \wedge b|a \Rightarrow a = \pm b$**,**
3) $a|b \wedge b|c \Rightarrow a|c$**,**
4) $a|b \wedge a|c \Rightarrow a|b + c$**.**

Príklad 5. Ak $a, b \in \mathbb{Z}$ a $m \in \mathbb{N}$, tak a, b majú rovnaký zvyšok po delení m práve vtedy, keď $m|b - a$. ∘

Príklad 6. Pre každé prirodzené číslo m existuje prirodzené číslo v tvare $1111 \ldots 1000 \ldots 0$ deliteľné m. Dokáže sa to takto:
Zažujme čísla $1, 11, 111, \ldots, 111 \ldots 1$. Posledné má m jednotiek. Ak je jedno z týchto čísel deliteľné m, tak to je to spomínané číslo. Ak nie, to znamená, že ani jedno nedáva po delení m zvyšok 0. Teda tých m čísel má maximálne $m - 1$ zvyškov po delení m. Teda niektoré dve musia mať rovnaké zvyšky. Preto ich rozdiel je deliteľný m.

∘

V predošlom príklade sme použili tzv. **Dirichletov princíp** — niekedy sa nazýva aj **Dirichletov holubníkový princíp**: Ak chceme umiestnit m holubov do $m-1$ holubníkov, tak v aspoň jednom holubníku musia byť dva holuby. Podobne sa dá vyriešiť aj nasledujúce

Príklad 7. Ak $a_1, \ldots, a_m$ sú celé čísla, $m \in \mathbb{N}$, tak pre nejaké indexy $i \leq j$ platí $m|a_i + a_{i+1} + \cdots + a_j$. ∘

Príklad 8. Je známe, že ak $a \in \mathbb{Z}$ a $2|a$ a $3|a$, tak aj $6|a$. Prečo to platí? Vyplýva to z nasledujúcich jednoduchých úvah. Číslo 1 môžeme vyjadriť v tvare $1 = 3 - 2$. Teda po vynásobení tohoto číslom a dostávame

$$a = a \cdot 1 = 3a - 2a\,. \tag{5}$$

Z predpokladu $2|a$ vyplýva, že $a = 2a_1$, podobne z predpokladu $3|a$ dostávame $a = 3a_2$ pre vhodné $a_1, a_2 \in \mathbb{Z}$. Ak dosadíme do rovnosti (5) dostávame

$$a = a \cdot 1 = 3a - 2a = 3 \cdot 2a_1 + 2 \cdot 3a_2 = 6a_1 + 6a_2\,.$$

To znamená, že $a = 6(a_1 + a_2)$, vidíme, že a je celočíselným násobkom 6-tky. Z príkladu **??** teraz vidíme, že $6|n^3 - n$ pre $n \in \mathbb{N}$. ∘

Príklad 9. Podobne sa dá dokázať napríklad $7|a \wedge 8|a \Rightarrow 56|a$. ∘

V predošlých príkladoch bolo dôležité to, že sa vhodným spôsobom dalo vyjadriť číslo 1. Preštudujeme to teraz trochu podrobnejšie. Ak $a, b \in \mathbb{Z}$ a $a \neq 0$, tak hodnota

$$\max\{d \in \mathbb{N}; d|a \wedge d|b\} := (a, b)$$

sa nazýva **najväčší spoločný deliteľ** čísel a, b. V prípade $a = 0, b = 0$ definujeme $(0, 0) = 0$.

Príklad 10. Ak $x \in \mathbb{Z}$, tak $(x + 1, x) = 1$ a $(x + 1, x - 1) = 1$ alebo 2. ∘

V teórii čísel aj v jej zovšeobecneniach, napríklad v algebre, má veľký význam nasledujúca vlastnosť najväčšieho spoločného deliteľa. V literatúre býva niekedy uvádzaná ako Bezoutova rovnosť.

Veta 2. Nech $a, b \in \mathbb{Z}$**. Položme** $d = (a, b)$**. Potom existujú** $x, y \in \mathbb{Z}$**, pre ktoré**

$$d = ax + by\,.$$

Dôkaz. Ak $a = 0, b = 0$, tak $(0, 0) = 0 = 0 \cdot 0 + \cdot 0$. Teda pre tento prípad veta platí. Nech aspoň jedno, z uvažovaných čísel a, b sa nerovná 0. Dôležitú úlohu bude hrať množina

$$M = \{ax + by; x, y \in \mathbb{Z}\}\,.$$

Z predpokladu, že aspoň jedno z čísel a, b je nenulové, vyplýva, že M obsahuje aj prirodzené čísla. Označme d_0 najmenšie prirodzené číslo patriace do M. Určite platí

$$d_0 = ax + by \tag{6}$$

pre nejaké $x, y \in Z$. Z (6) dostávame $d|d_0$, a teda $d \leq d_0$. Ukážeme, že platí aj opačná nerovnosť. Po vydelenía hodnotou d_0 so zvyškom dostávame

$$a = a_1 d_0 + r,$$

pričom $0 \leq r < d_0$. Zvyšok r si môžeme vyjadriť

$$r = a - a_1 d_0\,.$$

Ak dosadíme za d_0 podľa rovnosti (6) dostávame

$$r = a - a_1(ax + by) = a(1 - a_1 a)x - a_1 by\,.$$

Teda ak by platilo $r > 0$, tak r by bolo prirodznené číslo z M, ktoré by bolo menšie ako d_0 — spor s minimalitou d_0. Preto $r = 0$. To znamená $d_0|a$. Rovnakým spôsobom sa dokáže aj $d_0|b$. Preto d_0 je spoločný deliteľ a aj b, a teda $d_0 \leq d$. □

Príklad 11. Pre $a, b \in \mathbb{Z}$ je (a, b) deliteľné každým spoločným deliteľom a a b. ∘

Príklad 12.
Pomocou vety 6 sa dá dokázať že pre $a, b, c \in \mathbb{Z}$ platí$(ac, bc) = |c|(a, b)$. ∘

Príklad 13.
Ak $a, b \in \mathbb{Z}$, tak $(a - b, a + b) = (a, b)$, alebo $(a - b, a + b) = 2(a, b)$. ∘

Celé čísla a, b sa nazývajú **nesúdeliteľné** práve vtedy, keď $(a, b) = 1$.

Veta 3. Celé čísla (a, b) sú nesúdeliteľné práve vtedy, keď

$$ax + by = 1 \tag{7}$$

pre vhodné $x, y \in Z$.

Dôkaz. Jedna implikácia vyplýva priamo z vety 6 .
Ak platí (7) a $d = (a, b)$, tak $d|1$, a teda $d = 1$. □

Príklad 14. Dá sa dokázať pre $a, b \in \mathbb{Z}$ $a \neq 0$, že $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$. ∘

Príklad 15. Ak a, b sú nenulové celé čísla a $(a, b) = ax + by$ pre $x, y \in Z$, tak $(x, y) = 1$. ∘

Príklad 16. Ak $a, b_1, b_2 \in \mathbb{Z}$ a $(a, b_1) = 1$, zároveň $(a, b_2) = 1$, tak aj $(a, b_1 b_2) = 1$. Dokáže sa to vynásobením rovností $ax+b_1y = 1, ax_1+b_2y_1 = 1$. ∘

Príklad 17. Ak $a, b, c \in \mathbb{Z}$ a $(b, c) = 1$, tak $(ca, b) = 1$. ∘

Príklad 18. Ak f je funkcia definovaná na intervale $[1, \infty)$, ktorá má dve celočíselné nesúdeliteľné periody, tak $f(x + 1) = f(x)$ pre každé $x \in [1, \infty)$. ∘

Veta 4. Ak $a, b, c \in \mathbb{Z}$ a $a|bc$ a $(a, b) = 1$, tak $a|c$.

Dôkaz. Z vety 3 dostávame pomocou podmienky $(a, b) = 1$ rovnosť

$$1 = ax + by.$$

Pre vhodné $x, y \in \mathbb{Z}$. Po vynásobení číslom c platí

$$c = c \cdot 1 = acx + bcy.$$

Pretože $a|bc$ môžeme vyjadriť: $bc = ka$, pre nejaké $k \in \mathbb{Z}$. Po dosadení za bc do poslednej rovnosti dostáveme

$$c = acx + kay = a(cx + ky).$$

□

Príklad 19. Ak $a \in \mathbb{Z}$ a $5|3a$, tak $5|a$. ∘

Nasledujúce dva príklady sú tiež na Dirichletov princíp

Príklad 20. Pre každe prirodzené číslo m, také že $(m, 10) = 1$, existuje prirodzené číslo v tvare $11 \ldots 1$ deliteľné m. ∘

Príklad 21. Nech $m \in \mathbb{N}$ a $q_1, q_2, q_3, \ldots$ je taká postupnosť celých čísel, že $(m, q_n) = 1$ pre $n \in \mathbb{N}$. Potom existuje $j \leq m$, také že $m|q_j \ldots q_m - 1$. ∘

Príklad 22. Ak $a, b, c \in \mathbb{Z}$, tak rovnica

$$ax + by = c,$$

pričom x, y sa hľadajú v $\mathbb{Z}$, sa nazýva **lineárna diofantická rovnica**. Dá sa dokázať, že je riešiteľná práve vtedy, keď $(a, b)|c$. V takom prípade všetky jej riešenia sú $x = x_0 + \frac{b}{(a,b)}t$, $y = y_0 - \frac{a}{(a,b)}t$, kde t prebiaha $\mathbb{Z}$ a x_0, y_0 je jedno pevne dané riešenie. ∘

Veta 5. Nech $a, b, c \in \mathbb{Z}$ a $(a, b) = 1$. Potom $a|c \wedge b|c \Rightarrow ab|c$.

Dôkaz. Z podmienky $a|c$ vyplýva $c = ac_1$. Z ďalšej podmienky dostávame $b|ac_1$. Z nesúdeliteľnosti a a b preto vyplýva $b|c_1$, teda $c_1 = bc_2$. Po dosadení za c_1 dostávame $c = abc_2$. □

Príklad 23.
Predošlá veta sa dá dokázať aj rovnakým postupom ako v príklade 5. ∘

1.3 Prvočísla

Prirodzené číslo $p > 1$ sa nazýva **prvočíslo** práve vtedy, keď pre každé $d \in \mathbb{N}$ platí $d|p \Rightarrow d = 1 \vee d = p$. Sú to napríklad $2, 3, 5, 17, 23$ atp.

Príklad 24.
a) Ak $p > 2$ je prvočíslo tak $p = 4k + 1$ alebo $4k + 3$,
b) Ak $p > 3$ je prvočíslo tak $p = 4k + 1$ alebo $6k + 3$,
c) ak $p = mk + n$, $m, n \in \mathbb{N}$, je prvočíslo väčšie ako n tak $(m, n) = 1$.
∘

Príklad 25. Ak p_1, p_2 sú rôzne prvočísla, tak $(p_1, p_2) = 1$. ∘

Príklad 26. Ak p je prvočíslo a $a \in \mathbb{Z}$, tak $p|a$ alebo $(a, p) = 1$. ∘

Príklad 27. Ak p je prvočíslo a $a, b \in \mathbb{Z}$ a $p|ab$, tak $p|a$ alebo $p|b$. ∘

Veta 6. Ak $m \in \mathbb{N}$ a $m > 1$ tak hodnota $\min\{d \in \mathbb{N}; d > 1 \wedge d|m\}$ je prvočíslo.

Dôkaz. Nech d je uvedená hodnota. Ak by d nebolo prvočíslo, tak $d = d_1 d_2$, pričom $1 < d_1 < d, 1 < d_2 < d$. Je zrejmé, že napríklad $d_1|m$ a to je spor s minimalitou d. □

Prirodzené číslo väčšie ako 1 ktoré nie je prvočíslo sa nazýva **zložené číslo**.

Veta 7. Ak m je zložené číslo, tak existuje prvočíslo $p \leq \sqrt{m}$, také že $p|m$.

Dôkaz. Ak m je zložené číslo, tak $m = m_1 m_2$, pričom $m_1 > 1, m_2 > 1$. Ak by $m_1 > \sqrt{m}$ aj $m_2 > \sqrt{m}$, tak by $m = m_1 m_2 > m$ a to je spor. Nech napríklad $m_1 \leq \sqrt{m}$. Ak p je minimálny deliteľ m_1 rôzny od 1, tak $p|m$ a $p \leq \sqrt{m}$. □

Veta 8. Existuje nekonečne veľa prvočísel.

Dôkaz. Predpokladajme, že $p_1, \ldots, p_k$ sú prvočísla. Uvažujme prirodzené číslo

$$m = p_1 \ldots p_k + 1.$$

Ak p je najmenší deliteľ tohoto čísla rôzny od 1, tak p je prvočíslo, ale evidentne sa p nerovná ani jednému z prvočísel $p_1, \ldots, p_k$. Teda ku každej konečnej množine prvočísel existuje prvočíslo, ktoré do nej nepatrí. Z toho vyplýva, že konečná množina nemôže obsahovať všetky prvočísla. Teda množina prvočísel je nekonečná. □

Veta 9. Pre každé prirodzené číslo $n > 1$ existujú jednoznačne určené prvočísla $p_1 < p_2 < \cdots < p_k$ a prirodzené čísla $\alpha_1, \ldots, \alpha_k$, také že

$$n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}. \tag{8}$$

Dôkaz. Najprv dokážeme existenciu rozkladu (47). Nech p_1 je minimálny deliteľ n. Potom existuje $\alpha_1 \geq 1$, také že

$$n = p_1^{\alpha_1} n_1, (p_1, n_1) = 1\,.$$

Podobne dostaneme, že pre nejaké prvočíslo $p_2 > p_1$ platí $n_1 = p_2^{\alpha_2} n_2$ a $(n_2, p_2) = 1$. To znamená

$$n = p_1^{\alpha_1} p_2^{\alpha_2} n_2\,,$$

pričom $n > n_1 > n_2$. Takto po konečnom počte krokov dostávame existenciu rozkladu (47).

Teraz dokážeme jednoznačnosť. Predpokladajme, že $n = q_1^{\beta_1} \ldots q_s^{\beta_s}$, kde $q_1 < q_2 < \cdots < q_s$ sú prvočísla. Potom

$$p_1^{\alpha_1} \ldots p_k^{\alpha_k} = q_1^{\beta_1} \ldots q_s^{\beta_s}.$$

Z tejto rovnosti vyplýva, že p_1 delí niektorý z činiteľov na pravej strane, teda $p_1 | q_j^{\beta_j}$. Pretože p_1, q_j sú prvočísla, je to možné iba v prípade $p_1 = q_j$. Ale p_1 je minimálny prvočíselný deliteľ n, a teda musí platiť $p_1 = q_1$. Dostáveme preto rovnosť

$$p_1^{\alpha_1} \ldots p_k^{\alpha_k} = p_1^{\beta_1} \ldots q_s^{\beta_s}.$$

Ak by bolo $\alpha_1 < \beta_1$, tak po vykrátení by sme dostali

$$p_2^{\alpha_2} \ldots p_k^{\alpha_k} = p_1^{\beta_1 - \alpha_1} \ldots q_s^{\beta_s}.$$

Teda p_1 by delilo pravú stranu, ale nedelilo ľavú. To by bol spor. Podobne by sme dostali spor, ak by sme predpokladali $\alpha_1 > \beta_1$. Teda musí platiť $\alpha_1 = \beta_1$. Takto by sme postupne dokázali $\alpha_i = \beta_i$ a $k = s$. □

Príklad 28. Ak $a, b \in \mathbb{N}$ a $a^3 = b^4$, tak $a = a_1^4$ a $b = b_1^3$ pre vhodné $a_1, b_1 \in \mathbb{N}$. ∘

Príklad 29. Ak $a, b \in \mathbb{N}$, $(a, b) = 1$ a $ab = c^n$ pre dané $n \in \mathbb{N}$, tak $a = a_1^n, b = b_1^n$. ∘

Príklad 30. Ak $n_1, n_2 \in \mathbb{N}$,a $n_1 = p_1^{\alpha_1} \ldots p_k^{\alpha_k}, n_2 = p_1^{\beta_1} \ldots p_k^{\beta_k}$, pričom $\alpha_i, \beta_i \geq 0$, tak

$$(n_1, n_2) = n = p_1^{\gamma_1} \ldots p_k^{\gamma_k},$$

kde $\gamma_i = \min\{\alpha_i, \beta_i\}$ pre $i = 1, \ldots, k$. ∘

Príklad 31. Podobným spôsobom ako nekonečnosť množiny prvočísel sa dá dokázať:
a) existuje nekonečne veľa prvočísel v tvare $3k+2$,
b) existuje nekonečne veľa prvočísel v tvare $4k+3$,
c) existuje nekonečne veľa prvočísel v tvare $6k+5$. ∘

Príklad 32. Hlavná veta aritmetiky poskytuje aj iný pohľad na nekonečnosť množiny prvočísel. Predpokladajme, že $p_1, \dots, p_k$ sú všetky prvočísla. Potom

$$\sum_{n=1}^{\infty} \frac{1}{n} = \sum_{\alpha_1=0}^{\infty} \cdots \sum_{\alpha_k=0}^{\infty} \frac{1}{p_1^{\alpha_1}} \cdots \frac{1}{p_k^{\alpha_k}} =$$

$$= \sum_{\alpha_1=0}^{\infty} \frac{1}{p_1^{\alpha_1}} \cdots \sum_{\alpha_k=0}^{\infty} \frac{1}{p_k^{\alpha_k}} = \frac{1}{1-\frac{1}{p_1}} \cdot \dots \cdot \frac{1}{1-\frac{1}{p_k}} < \infty.$$

Dostali sme spor s divergenciou harmonického radu. ∘

Príklad 33. Zaujímavý dôkaz nekonečnosti množiny prvočísel publikoval v roku 1955 H. Fürstenberg. Využíval pri tom topologické úvahy. Nech $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Označme

$$a + (m) = \{a + km; k = 0, 1, 2, \dots\},$$

pričom $a \in \mathbb{N}_0$ a $m \in \mathbb{N}$. Namiesto $0 + (m)$ budeme písať iba (m). Tieto množiny sa nazývajú **zvyškové triedy** modulo m. Množina $S \subset \mathbb{N}_0$ sa nazýva **otvorená**, ak pre každé $a \in S$ existuje také $m \in \mathbb{N}$, že $a + (m) \subset \mathbb{N}$. Otvorená množina je aj $\emptyset$ a $\mathbb{N}$. Priamo z definície vyplýva, že zjednotenie ľubovoľného systému otvorených množín je otvorená množina.

Ak S_1, S_2 sú otvorené množiny a $a \in S_1 \cap S_2$, tak pre nejaké m_1, m_2 platí $a + (m_1) \subset S_1, a + (m_2) \subset S_2$. Platí $a + (m_1 m_2) \subset a + (m_1) \subset S_1$ a $a + (m_1 m_2) \subset a + (m_2) \subset S_2$. Preto $a + (m_1 m_2) \subset S_1 \cap S_2$. Teda aj $S_1 \cap S_2$ je otvorená množina. Keď si uvedomíme, že

$$\mathbb{N}_0 = (m) \cup 1 + (m) \cup \cdots \cup m - 1 + (m)$$

je disjunktný rozklad, dostávame, že aj množina $\mathbb{N}_0 \setminus (m)$ je otvorená. Nech existuje iba konečný počet prvočísel, označme ich $p_1, \dots, p_n$. Každé číslo z $\mathbb{N}_0$ okrem 1 je deliteľné nejakým prvočíslom. Preto

$$\{1\} = \mathbb{N}_0 \setminus \bigcup_{j=1}^{n} (p_j) = \bigcap_{j=1}^{n} \Big(\mathbb{N}_0 \setminus (p_j) \Big).$$

Teda množina $\{1\}$ by bola za daného predpokladu prienikom konečného počtu otvorených množín. To znamená že by to bola otvorená množina a to je spor.

$\circ$

2 Kongruencie

Ak $a, b \in \mathbb{Z}$ a $m \in \mathbb{N}$ tak hovoríme, že a a b sú **kongruentné modulo** m práve vtedy keď dávajú rovnaký zvyšok po delení m. Túto skutočnosť budeme označovať $a \equiv b \pmod{m}$. Ak čísla a, b nie sú kongruetné modulo m hovoríme, že sú **inkongruetné** modulo m a označujeme to $a \not\equiv b \pmod{m}$.

Podľa príkladu 5 dostávame

Veta 10. Ak $a, b \in \mathbb{Z}$ **a** $m \in \mathbb{N}$ **tak**

$$a \equiv b \pmod{m} \iff m|b-a.$$

Relácia $a \equiv b \pmod{m}$ sa nazýva **kongruencia modulo** m.

Pomocou provnávania zvyškov sa dá odvodiť, že kongruencia modulo m je relácia ekvivalencie, teda

Veta 11. Ak $m \in \mathbb{N}$ **a** $a, b, c \in \mathbb{Z}$**, tak**
$a \equiv a \pmod{m}$,
$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$,
$a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

Príklad 34. Ak $r_1 \equiv r_2 \pmod{m}$ tak

$$\cos\left(\frac{2\pi r_1}{m}\right) = \cos\left(\frac{2\pi r_2}{m}\right) \wedge \sin\left(\frac{2\pi r_1}{m}\right) = \sin\left(\frac{2\pi r_2}{m}\right)$$

. $\circ$

Budeme hovoriť, že celé čísla $r_1, \ldots, r_j$ tvoria **úplný zvyškový systém modulo** m, ak pre každé $i \in \{0, \ldots, m-1\}$ existuje jediné r_i také, že $r_i \equiv i \pmod{m}$.

Príklad 35. Úplný zvyškový systém modulo 5 je $0, 1, 2, 3, 4$ ale aj 500, $421, 457, 658, 504$. $\circ$

Príklad 36. Úplný zvyškový systém modulo m tvorí m čísel. $\circ$

Príklad 37. Celé čísla $r_1, \ldots, r_m$ také, že $r_i \not\equiv r_j \pmod{m}$ pre $i \neq j$, tvoria úplný zvyškový systém modulo m. $\circ$

Príklad 38. m po sebe idúcich celých čísel tvorí úplný zvyškový systém modulo m. ∘

Príklad 39. Pomocou príkladu 34 sa dá dokázať : Ak $r_1, \ldots, r_m$ je úplný zvyškový sýstem modulo m, tak

$$\sum_{j=1}^{m} \cos\left(\frac{2\pi r_j}{m}\right) + i \sin\left(\frac{2\pi r_j}{m}\right) = 0.$$

∘

Dôležitú úlohu majú nasledujúce súvislosti s operáciami ščítania a násobenia. Kongruencie sa dajú ščítať a násobiť podobne ako rovnosti.

Veta 12. Nech $m \in \mathbb{N}$**,** $a, b, a_1, a_2 \in \mathbb{Z}$**. Potom z predpokladov** $a \equiv a_1 \pmod{m}$ **a** $b \equiv b_1 \pmod{m}$**, vyplýva** $a + b \equiv a_1 + b_1 \pmod{m}$ **a** $aa_1 \equiv bb_1 \pmod{m}$**.**

Dôkaz. Dokážeme iba druhú časť. Prvú si dokáže prípadný čítateľ sám. Platí rovnosť

$$aa_1 - bb_1 = a_1(a - b) + b(a_1 - b_1).$$

Podľa predpokladu sú oba ščítance na pravej strane deliteľné číslom m a teda $m | aa_1 - bb_1$. □

Príklad 40. Podľa predošlej vety sa dá dokázať napríklad, že číslo $6^n + 4 \cdot 11^n$ je deliteľné piatimi pre každé $n \in \mathbb{N}$. ∘

Príklad 41. Platí kongruencia

$$10 \equiv 1 \pmod{9},$$

a teda podľa vety 12 dostávame

$$10^n \equiv 1 \pmod{9}, n = 1, 2, 3, \ldots.$$

Po jednoduchých úvahách z toho vyplýva, že každé prirodzené číslo je kongruentné so svojim ciferným súčtom modulo 9.

Príklad 42. Ako už bolo spomínané, každé reálne číslo sa dá vyjadriť v tvare g - adického rozvoja, $g > 1$. Dokážeme, že číslo je racionálne práve vtedy, keď je jeho g - adický rozvoj periodický. Stačí to dokázať pre prvky $[0, 1)$. Ak je rozvoj daného čísla periodický, tak pomocou súčtu geometrického radu sa dá vypočítať zlomok, ktorému sa dané číslo rovná.

Naopak, nech $\alpha = \frac{p}{q}$. Potom podľa príkladu 42 platí

$$\alpha = 0, a_1 a_2 a_3 \ldots,$$

kde $a_n = \left[\frac{g}{q} r_n\right]$, pričom

$$r_n \equiv p g^{n-1} \pmod{q}.$$

Hodnoty r_n sú z množiny $\{0, \ldots, q-1\}$, preto aspoň raz sa musí nejaká opakovať. To znamená, že existuje $n_0, s \in \mathbb{N}$ také, že $r_{n_0} = r_{n_0+s}$. Teda

$$p g^{n_0-1} \equiv p g^{n_0+s-1} \pmod{q}.$$

Z toho vyplýva, že pre $n \geq n_0$ platí

$$p g^{n-1} \equiv p g^{n+s-1} \pmod{q},$$

a teda $r_n = r_{n+s}$ a teda $a_n = a_{n+s}$. ∘

Príklad 43. Ak $f(x)$ je polynóm s celočíselnými koeoficientami a $r_1 \equiv r_2 \pmod{m}$, tak $f(r_1) \equiv f(r_2) \pmod{m}$. ∘

Príklad 44. Ak $r_1, \ldots, r_m$ je úplný zvyškový systém modulom m, tak

$$r_1 + \cdots + r_m \equiv \frac{m(m-1)}{2} \pmod{m}.$$

Príklad 45. Ak $f(x_1, \ldots, x_m)$ je symetrický polynóm s celočíselnými koeficientami a $r_1, \ldots, r_m$ je úplný zvyškový systém modulo m, tak

$$f(r_1, \ldots, r_m) \equiv f(0, \ldots, m-1) \pmod{m}.$$

∘

Veta 13. Nech $m \in \mathbb{N}$**,** $a, b, c \in \mathbb{Z}$**. Ak** $(c, m) = 1$**, tak**

$$ac \equiv bc \pmod{m} \Longrightarrow a \equiv b \pmod{m}.$$

Dôkaz. Z predpokladu vyplýva

$$m | bc - ac = (b-a)c.$$

Pretože $(c, m) = 1$, dostávame takto $m | b - a$. □

Príklad 46. Ak $r_1, \ldots, r_m$ je úplný zvyškový systém modulo m a $(a, m) = 1$,$b \in \mathbb{Z}$, tak aj $ar_1 + b, \ldots, ar_m + b$ je úplný zvyškový systém modulo m. ∘

Príklad 47. Ak platia predpoklady predošlého príkladu, tak

$$\left\{\frac{ar_1+b}{m}\right\}+\cdots+\left\{\frac{ar_m+b}{m}\right\}=\frac{m-1}{2}.$$

Vyplýva to z príkladu 2, odkial vieme, že zvyšok $c\in\mathbb{Z}$ po delení m je $m\{\frac{c}{m}\}$. ∘

Príklad 48. Nech $m_1,m_2\in\mathbb{N}$ sú nesúdeliteľné. Predpokladajme ďalej, že $r_1,\ldots,r_{m_1}$ je úplný zvyškový systém modulo m_1 a $s_1,\ldots,s_{m_2}$ je úplný zvyškový systém modulo m_2. Dá sa dokázať, že v takom prípade je $r_jm_2+s_km_1, j=1,\ldots,m_1, k=1,\ldots,m_2$, úplný zvyškový systém modulo m_1m_2. ∘

Príklad 49. Dá sa dokázať : Ak $(a,m)=1$, tak existuje $n>1$ také, že $a^n\equiv 1 \pmod m$. Vyplýva to z toho, že aspoň dva razy sa v postupnosti $a,a^2,a^3,\ldots$, musí vyskytnúť rovnaký zvyšok po delení m. ∘

Ak $(a,m)=1$ tak najmenšie take $k\in\mathbb{N}$ pre ktoré

$$a^k\equiv 1 \pmod m$$

sa nazýva **rád** a modulo m. Označovať ho budeme $\mathbf{ord}_m(a)$.

Príklad 50. $\mathbf{ord}_5(2)=4$, $\mathbf{ord}_7(2)=3$. ∘

Veta 14. Ak $m\in\mathbb{N}$**,** $a\in\mathbb{Z}$ **a** $(a,m)=1$**. tak**

$$a^n\equiv 1 \pmod m \Leftrightarrow \mathbf{ord}_m(a)|n.$$

Dôkaz. Jedna implikácia je triviálna. Dokážeme druhú. Nech

$$a^n\equiv 1 \pmod m.$$

Ak $r=\mathbf{ord}(a)$, tak môžeme deliť so zvyškom a dostávame $n=rk+r'$ pričom $r'\in\{0,\ldots,r-1\}$. Po dosadení do danej kongruancie za n dostávame

$$a^{r'}\equiv 1 \pmod m.$$

Ak by bolo $r'>0$ dostali by sme spor s minimalitou r. Preto $r'=0$ a teda $r|n$. □

Za prepokladov predošlej vety z nej vyplýva

$$a^{n_1}\equiv a^{n_2} \pmod m \Leftrightarrow n_1\equiv n_2 \pmod{\mathbf{ord}(a)}. \tag{9}$$

Príklad 51. Ak $(a,m)=1$,$a \not\equiv 1 \pmod{m}$ a p je také prvočíslo, že $a^p \equiv 1 \pmod{m}$, tak $p = \mathbf{ord}_m(a)$. ∘

Príklad 52. Ak $(a,m)=1$, a $a^{n_1} \equiv 1 \pmod{m}$, $a^{n_2} \equiv 1 \pmod{m}$, pre nejake $n_1, n_2 \in \mathbb{N}$, tak $\mathbf{ord}_m(a)|(n_1,n_2)$. ∘

Príklad 53. Nech a, b sú celé čísla nesúdeliteľné s daným $m \in \mathbb{N}$. Predpokladajme, že $\mathbf{ord}_m(a), \mathbf{ord}_m(b)$ sú nesúdeliteľné. Dokážeme, že

$$\mathbf{ord}_m(ab) = \mathbf{ord}_m(a)\mathbf{ord}_m(b).$$

Je zrejmé, že

$$(ab)^{\mathbf{ord}_m(a)\mathbf{ord}_m(b)} \equiv 1 \pmod{m}.$$

Nech pre $r \in \mathbb{N}$ platí $(ab)^r \equiv 1 \pmod{m}$. To znamená

$$a^r b^r \equiv 1 \pmod{m}.$$

Ak umocníme túto kongruenciu na $\mathbf{ord}_m(b)$, dostávame

$$a^{\mathbf{ord}_m(b)r} \equiv 1 \pmod{m}.$$

Preto z vety 14 vyplýva $\mathbf{ord}_m(a)|\mathbf{ord}_m(b)r$. Pretože čísla $\mathbf{ord}_m(a)$ a $\mathbf{ord}_m(b)$ sú nesúdeliteľné dostávame $\mathbf{ord}_m(a)|r$. Úplne rovnako dokážeme $\mathbf{ord}_m(b)|r$, a teda $\mathbf{ord}_m(a)\mathbf{ord}_m(b)|r$. ∘

Príklad 54. Pomocou predošlého príkladu dokážeme:
Ak $R = \max\{\mathbf{ord}_m(x); (x,m)=1\}$, tak pre každé $a \in \mathbb{Z}$ také, že $(a,m)=1$ platí

$$\mathbf{ord}_m(a)|R.$$

Nech by to neplatilo. Potom v kánonickom rozklade R sa vyskytuje niektoré prvočíslo s menším exponentom ako v niektorom $\mathbf{ord}_m(a)$, pre nejaké a, $(a,m)=1$. Označme toto prvočíslo p. Predpokladajme, že p vystupuje v kánonickom rozklade $\mathbf{ord}_m(a)$ a exponentom $\alpha \in \mathbb{N}$ a v kánonickom rozklade R s exponentom β, pričom $\beta > \alpha$. Nech $R = p^\beta R_1$ a $(p, R_1) = 1$ a $\mathbf{ord}_m(a) = p^\alpha A$ a rovnako $(p, A) = 1$. Číslo a^A je rádu p^β modulo m. R je rádom nejakého prvku $\mathbb{Z}_m^*$. Označme ho b. Potom b^{p^α} je rádu R_1. Ale podľa predošlého platí $(R_1, p^\alpha) = 1$. Podľa predošlého príkladu je číslo $a^A b^{p^\alpha}$ rádu $p^\beta R_1 > R$. To je spor s maximalitou R.
∘

2.1 Eulerova funkcia

Nech $m \in \mathbb{N}$. Označme

$$\mathbb{Z}_m^* = \{j \in \mathbb{N}; j \leq m, (m, j) = 1\}.$$

Celé čísla $r_1, \ldots, r_k$ budeme nazývať **redukovaný zvyškový systém** modulo m, ak pre každú hodnotu $j \in \mathbb{Z}_m^*$ existuje jediné $\ell, 1 \leq \ell \leq k$ také, že

$$r_\ell \equiv j \pmod{m}.$$

Príkladom takéhoto systém je napríklad $\mathbb{Z}_m^*$, dajme tomu aj $\{-j; j \in \mathbb{Z}_m^*\}$. Je zrejmé, že každý redukovaný systém modulo m obsahuje toľko prvkov koľko $\mathbb{Z}_m^*$. Počet prvkov redukovaného zvyškového systému modulo m budeme označovať $\varphi(m)$. Táto funkcia sa nazýva **Eulerova funkcia**.

Príklad 55. Ak $s_1, \ldots, s_{\varphi(m)}$ sú celé čísla nesúdeliteľné s m, navzájom inkongruetné modulo m, tak tvoria redukovaný zvyškový systém modulo m. ∘

Príklad 56. Ak $s_1, \ldots, s_{\varphi(m)}$ je redukovaný zvyškový systém modulo m a $a \in \mathbb{Z}$ pričom $(a, m) = 1$, tak aj $as_1, \ldots, as_{\varphi(m)}$ je redukovaný zvyškový systém modulo m. ∘

Príklad 57. Nech m_1, m_2 sú nesúdeliteľné prirodzené čísla. Predpokladajme, že $r_1, \ldots, r_{\varphi(m_1)}$ je redukovaný zvyškový systém modulo m_1 a čísla $s_1, \ldots, s_{\varphi(m_2)}$ tvoria redukovaný zvyškový systém modulo m_2. Dokážeme, že

$$r_j m_2 + s_k m_1, j = 1, \ldots, \varphi(m_1), k = 1, \ldots, \varphi(m_2),$$

je redukovaný zvyškový systém modulo $m_1 m_2$.

Najprv dokážeme, že tieto čísla sú nesúdeliteľné s $m_1 m_2$. Vyplýva to z toho, že $(r_j m_2 + s_k m_1, m_1) = (r_j m_2, m_1) = 1$. Rovnako dostávame $(r_j m_2 + s_k m_1, m_2) = 1$. Preto dané čísla sú nesúdeliteľné aj s $m_1 m_2$.

Nech $z \in \mathbb{Z}$ a $(z, m_1 m_2) = 1$. Pre vhodné $a, b \in \mathbb{Z}$ platí

$$1 = am_1 + bm_2, (a, m_2) = 1, (b, m_1) = 1.$$

Potom

$$z = z \cdot 1 = zam_1 + zbm_2. \tag{10}$$

Z toho, že $(za, m_2) = 1$ a $(zb, m_1) = 1$ dostávame, že existujú j, k pre ktoré

$$za \equiv s_k \pmod{m_2}, zb \equiv r_j \pmod{m_1}.$$

To znamená $za = s_k + \ell_2 m_2, zb = r_j + \ell_1 m_1$. Po dosadení do (10) dostávame

$$z = s_k m_1 + \ell_1 m_1 m_2 + r_j m_2 + \ell_2 m_1 m_2 \equiv s_k m_1 + r_j m_2 \pmod{m_1 m_2}.$$

To, že tieto čísla sú inkongruetné modulo $m_1 m_2$ sa dokáže rovnako ako v príklade 48.

Z tohoto príkladu vyplýva aj

Veta 15. Ak $m_1, m_2 \in \mathbb{N}$ **a** $(m_1, m_2) = 1$**, tak**

$$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2).$$

Ak túto vetu použijeme na kánonický rozklad prirodzeného čísla $m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$, tak po istých úpravách dostaneme

$$\varphi(m) = m \prod_{j=1}^{n} \Big(1 - \frac{1}{p_j}\Big). \tag{11}$$

Príklad 58. Nech $m \in \mathbb{N}$ a $d|m$. Označme

$$S_d = \{j \in N; j \le m, (j, m) = d\}.$$

Potom $a \in S_d$ práve vtedy, keď $a = a_1 d$ pričom $(a_1, \frac{m}{d}) = 1$. Z toho vyplýva $|S_d| = \varphi(\frac{m}{d})$. Preto ak $1 = d_1, \dots, d_s = m$ sú všetky prirodzené delitele m, tak

$$m = \sum_{j=1}^{d} \varphi\Big(\frac{m}{d_j}\Big).$$

To je ekvivalentné s rovnosťou

$$m = \sum_{j=1}^{d} \varphi(d_j). \tag{12}$$

Príklad 59. Dokážeme rovnosť

$$\sum_{\substack{j \le m \\ (m,j)=1}} j = \frac{m\varphi(m)}{2}, \tag{13}$$

pre $m \in \mathbb{N}$. Nech $d_1, \dots, d_s$ sú všetky delitele m menšie ako m okrem 1. Podľa predošlého príkladu v tomto prípade máme

$$\sum_{k=1}^{s} \varphi\Big(\frac{m}{d_k}\Big) = m - 1 - \varphi(m). \tag{14}$$

Sumu na ľavej strane (13) môžeme vyjadriť

$$\sum_{\substack{j\le m\\(m,j)=1}} j = \frac{m(m-1)}{2} - \sum_{k=1}^{s} \sum_{\substack{j\le m\\(j,m)=d_k}} j. \tag{15}$$

Rovnosť $(j,m)=d_k$ platí práve vtedy, keď $j=\ell d_k$ a $(\ell, \frac{m}{d_k})=1$. Preto

$$\sum_{\substack{j\le m\\(j,m)=d_k}} j = \sum_{\substack{\ell\le \frac{m}{d_k}\\(\ell,\frac{m}{d_k})=1}} d_k\ell = d_k \sum_{\substack{\ell\le \frac{m}{d_k}\\(\ell,\frac{m}{d_k})=1}} \ell.$$

Po dosadení do (15) dostávame

$$\sum_{\substack{j\le m\\(m,j)=1}} j = \frac{m(m-1)}{2} - \sum_{k=1}^{s} d_k \sum_{\substack{\ell\le \frac{m}{d_k}\\(\ell,\frac{m}{d_k})=1}} \ell. \tag{16}$$

Teraz môžeme postupovať matematickou indukciou. Pre $m=1$ rovnosť (13) platí . Predpokladajme, že platí ak do (13) dosadíme za m čísla menšie ako m. Potom z rovnosti (16) dostávame

$$\sum_{\substack{j\le m\\(m,j)=1}} j = \frac{m(m-1)}{2} - \frac{m}{2}\sum_{k=1}^{s} \varphi\Big(\frac{m}{d_k}\Big)$$

A teda podľa (14) dostávame, že tvrdenie platí aj pre m. ∘

2.2 Eulerova veta

Veta 16. Ak $m\in\mathbb{N}$ **a** $a\in\mathbb{Z}$**, kde** $(a,m)=1$**, tak**

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

Dôkaz. Nech $a_1,\dots,a_k, k=\varphi(m)$, je redukovaný zvyškový systém modulo m. Potom aj $aa_1,\dots,aa_k$ je redukovaný zvyškový systém modulo m. Preto

$$aa_1\cdot\dots\cdot aa_k \equiv a_1\cdot\dots\cdot\dots a_k \pmod m.$$

Preusporiadaním činiteľov dostávame

$$a^k(a_1\cdot\dots\cdot a_k) \equiv a_1\cdot\dots\cdot\dots a_k \pmod m.$$

Po vykrátení oboch strán faktorom $a_1 \cdot \cdots \cdot \ldots a_k$ dostávame

$$a^k \equiv 1 \pmod{m}.$$

□

Príklad 60. Ak $(a, m) = 1$ a a^{-1} je inverzný prvok k a modulo m, tak

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

Príklad 61. Z predošlej vety vyplýva, že pre $m \in \mathbb{N}$ a $a \in \mathbb{Z}$ také, že $(a, m) = 1$ a prirodzené čísla $r_1 \equiv r_2 \pmod{\varphi(m)}$ platí

$$a^{r_1} \equiv a^{r_2} \pmod{m}.$$

Príklad 62. Ako sme už dokázali skôr, každý zlomok $\frac{p}{q}$ sa dá pre $g \in \mathbb{N}, g > 1$ vyjadriť v tvare periodického g - adického rozvoja

$$\frac{p}{q} = z + 0, a_1 \ldots a_k \overline{c_1 \ldots c_n},$$

pričom hodnota $0, a_1 \ldots a_k$ sa nazýva **predperióda**. Ak má predperióda 0 číslic ,teda neexistuje, rozvoj nazývame **rýdzoperiodický**. Dokážeme, že g **- adický rozvoj zlomku** $\frac{p}{q}$**,** $(p, q) = 1$ **je rýdzoperiodický práve vtedy, keď** $(q, g) = 1$. Môžeme predpokladať $\frac{p}{q} \in [0, 1)$.

Ak

$$\frac{p}{q} = 0, \overline{a_1 \ldots a_n},$$

tak

$$g^n \frac{p}{q} = Z + 0, \overline{a_1 \ldots a_n} = Z + \frac{p}{q},$$

kde $Z \in \mathbb{N}$. Z toho po úprave vyplýva

$$(g^n - 1)p = Zq.$$

Z tejto rovnosti a podmienky $(p, q) = 1$ vyplýva $q | g^n - 1$. To znamená $(g, q) = 1$.

Naopak, nech $(g, q) = 1$. Ak sa vrátime k príkladu 42, vieme, že

$$\frac{p}{q} = 0, a_1 a_2 a_3 \ldots$$

pričom $a_n = \left[\frac{g}{q} r_n\right]$, kde $r_n \in \{0, \ldots, q-1\}$ a

$$r_n \equiv p g^{n-1} \pmod{q},$$

pre $n = 1, 2, 3, \ldots$. Z toho vyplýva podľa Eulerovej vety $r_n \equiv r_{n+\varphi(q)} \pmod{q}$. A teda $a_n = a_{n+\varphi(q)}$ pre každé $n = 1, 2, 3, \ldots$.

Príklad 63. Nech $\frac{p}{q} = 0, \overline{a_1 \dots a_n}$, je g - adický rozvoj. Súčislie $a_1 \dots a_n$ sa nazýva **minimálna** perióda daného zlomku, ak pre každé $k < n$ a $c_1, \dots, c_k$, $c_i \leq g - 1$ platí

$$\frac{p}{q} \neq 0, \overline{c_1 \dots c_k}.$$

V takom prípade z Eulerovej vety vyplýva, že dĺžka minimálnej periódy je deliteľom $\varphi(q)$.

M. Kučera uvádza v Rozhledoch Matematicko Fyzikálních tzv. **Midyho vetu.**

Príklad 64. Midyho veta hovorí o dekadickom rozvoji zlomku $\frac{1}{p}$, $p > 5$ je prvočíslo: **Ak** $\frac{1}{p} = 0, \overline{a_1 a_2 \dots a_{2n}}$ **má minimálnu periódu párnej dĺžky, tak** $a_i + a_{n+i} = 9, i = 1, \dots, n$**.** Dokáže sa to takto: Označme si $x = a_1 \dots a_n, y = a_{n+1} \dots a_{2n}$ prirodzené x, y s príslušným dekadickým rozvojom. Potom dostáveme

$$\frac{10^{2n}}{p} = 10^{2n-1}x + 10^{n-1}y + \frac{1}{p}.$$

To môžeme upraviť na tvar

$$\frac{10^{2n} - 1}{p} = 10^{2n-1}x + 10^{n-1}y = 10^{n-1}(10^n x + y). \tag{17}$$

Z toho vyplýva, že $p|10^{2n} - 1 = (10^n - 1)(10^n + 1)$. Ak by platilo $p|10^n - 1$, tak $10^n \equiv 1 \pmod{p}$ a dostávame spor s tým, že minimálna perióda daného zlomku je $2n$. Preto musí platiť $p|10^n + 1$. Z rovnosti (17) teda vyplýva $10^n - 1|10^{n-1}(10^n x + y)$. To znamená $10^n - 1|10^n x + y = (10^n - 1)x + x + y$. Nakoniec dostávame $10^n - 1|x + y$. Preto

$$x + y = k(10^n - 1), \ k \in \mathbb{N}.$$

Z dekadického rozvoja x, y vyplýva, že obidve čísla sú menšie ako 10^n. Z poslednej rovnosti preto vyplýva $k(10^n - 1) < 2 \cdot 10^n$. To je možné len vtedy, keď $k = 1$. Preto $x + y = 10^n - 1$. Z toho vyplýva tvrdenie.

Príklad 65. Postup z predchádzajúceho príkladu sa dá zovšeobecniť. Ak m je také prirodzené číslo, že pre nejaké $n \in \mathbb{N}$ platí $m|10^n + 1$, tak

$$\frac{1}{m} = 0, \overline{a_1 \dots a_{2n}},$$

pričom $a_i + a_{n+i} = 9$, $i = 1, \dots, n$.

Kučera v spomínanom čánku uvádza aj tzv. Ginsbergovu vetu, ktorá študuje prípad $\frac{1}{p} = 0, \overline{a_1 \dots a_{3n}}$.

Ak p je prvočíslo, tak $\varphi(p) = p - 1$. V tomto prípade preto z Eulerovej vety vyplýva

$$(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}. \tag{18}$$

Po vynásobení tejto kongruencie dostávame tvrdenie, ktoré nesie názov **Malá Fermatova veta**:

Veta 17. Ak p je prvočíslo, tak pre každé celé číslo a platí

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

Príklad 66. Ak p je prvočíslo $k \in \{1, \dots, p-1\}$ tak $p | \binom{p}{k}$. Preto playí

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Takto sa dá Malá Fermatova veta dokázať nezávisle od Eulerovej vety matematickou indukciou.

Príklad 67. Ak p je prvočíslo a $s_1, \dots, s_p$ je úplný zvyškový systém a $m \in \mathbb{N}$ pričom $p - 1 | m$, tak z (18) dostávame

$$\sum_{j=1}^{p} s_j^m \equiv -1 \pmod{p}.$$

Hodnota R z príkladu 54 je deliteľlom $\varphi(m)$. Ale, ako uvidíme neskôr, prípad $R = \varphi(m)$ je veľmi zriedkavý. Z vety 10 vyplýva

Veta 18. Ak m_1, m_2 sú nesúdeliteľné prirodzené čísla a $a, b \in \mathbb{Z}$, tak

$$a \equiv b \pmod{m_1} \wedge a \equiv b \pmod{m_2} \Leftrightarrow a \equiv b \pmod{m_1 m_2}$$

Príklad 68. Nech $m \in \mathbb{N}$ je prirodzené číslo, ltoré má v kanonickom rozklade aspoň dve nepárne prvočísla. Potom pre každé $a \in \mathbb{Z}$ platí

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}.$$

Ak m obsahuje v kánonickom rozklade dve nepárne prvočísla, tak sa dá vyjadriť v tvare $m = m_1 m_2$, pričom $(m_1, m_2) = 1$ a káďé z týchto čísel je deliteľné nepárnym prvočíslom. To znamená, že $\varphi(m_1), \varphi(m_2)$ sú párne čísla. Potom $\varphi(m_1) | \frac{\varphi(m)}{2}$ a teda

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m_1}.$$

Rovnako sa dá dokázať aj

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m_2}.$$

Podľa vety 18 to znamená

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}.$$

∘

2.3 Šifrovanie

Z predošlého príkladu vidíme, že v prípade $r \equiv 1 \pmod{\varphi(m)}$ platí

$$a^r \equiv a \pmod{m}, \tag{19}$$

ak $(a, m) = 1$.

Pomocou týchto výsledkov Ron Rivest, Adi Shamir, Leonard Adleman vytvorili algoritmus na šifrovanie a dešifrovanie informácií . Podľa prvých písmen ich priezvisk nesie tento algoritmus názov RSA. Správu, ktorú chceme zašifrovať, zakódujeme do čísla a. Zvolíme $s \in \mathbb{N}$ také, že $(s, \varphi(m)) = 1$. Správu zašifrujeme tak, že toto číslo umocníme na s modulo m, teda

$$b \equiv a^s \pmod{m}.$$

Hodnotu b pošleme prímateľovi. Predpokladáme pritom, že prímateľ pozná hodnotu p takú, že $ps \equiv 1 \pmod{\varphi(m)}$. Tento potom vypočíta b^p modulo m a dostáva

$$a \equiv b^p \pmod{m}.$$

Všetci poznajú m aj s. Prímateľ pozná p. Otázkou je do akej miery je táto šifra bezpečná. Či to niekto nepovolaný nedešifruje. Odosielateľ pozná naviac aj hodnotu $\varphi(m)$. Práve vďaka nej vypočíta číslo p, pretože

$$p \equiv s^{\varphi(\varphi(m))-1} \pmod{\varphi(m)}.$$

Trik je práve v tom, že nikto okrem odosielateľa nepozná hodnotu $\varphi(m)$. Táto hodnota sa vypočíta ľahko, ak poznáme rozklad m na prvočinitele. Číslo m vyberieme práve tak aby sa tento rozklad hľadal "zložito". Ak p_1, p_2 sú prvočísla a $m = p_1 p_2$, tak $\varphi(m) = (p_1 - 1)(p_2 - 1)$. V tomto prípade je napríklad p_1 koreňom rovnice

$$\varphi(m) = \Big(\frac{m}{p_1} - 1\Big)\Big(p_1 - 1\Big).$$

Z tohoto vidíme, že vypočítať hodnotu $\varphi(m)$ je v tomto prípade rovnako "zložité", ako nájsť kánonický rozklad m.

Príklad 69. Aký je kánonický rozklad čísla $m = 11021$ ak vieme, že $\varphi(m) = 10812$? ∘

2.4 Polynomické kongruencie, Lagrangeova veta

Ak $f(x)$ je polynóm z celočíselnými koeficientami, tak kongruencia

$$f(x) \equiv 0 \pmod{m} \tag{20}$$

sa nazýva **polynomická kongruencia** modulo m, pre dané $m \in \mathbb{N}$. Celé číslo sa nazýva **riešenie** tejto kongruencie, ak jeho dosadením dostaneme platnú kongruenciu. Riešenie sa nazýva **primitívne** ak patrí do množiny $\{0, \ldots, m-1\}$.

Veta 19. Kongruencia (20) je riešiteľná práve vtedy, keď má aspoň jedno primitívne riešenie. Celé čísla tvaru $x'+tm$, kde x' je primitívne riešenie a $t \in \mathbb{Z}$ sú potom všetky jej riešenia.

Príklad 70. Uvažujme kongruenciu

$$7x + 6 \equiv 0 \pmod{12}.$$

Vieme, že $7^2 = 49 \equiv 1 \pmod{12}$. Keď túto kongruenciu vybásobíme 7 dostávame

$$x + 42 \equiv 0 \pmod{12},$$

čo znamená

$$x + 6 \equiv 0 \pmod{12} \Leftrightarrow x \equiv 6 \pmod{12}.$$

Preto primitívne riešenie je 6 a všetky riešenia sú $6 + 12t, t \in \mathbb{Z}$. ∘

Príklad 71. Ak $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ a $(a, m) = 1$, tak kongruencia

$$ax + b \equiv 0 \pmod{m} \tag{21}$$

má jediné primitívne riešenie. V tomto prípade

$$x \equiv -ba^{\varphi(m)-1} \pmod{m}.$$

∘

Príklad 72. Ak v predošlom príklade vynecháme podmienku $(a, m) = 1$, tak sa dá dokázať, že konngruencia (21) je riešiteľná práve vtedy, keď $(a, m)|b$ a v tom prípade má (a, m) primitívnych riešení . ∘

Veta 20. Nech $f(x)$ je polynóm z celočíselnými koeficientami. Ak p je prvočíslo a kongruencia

$$f(x) \equiv 0 \pmod{p}$$

má viac primitívnych riešení ako je stupeň polynómu $f(x)$, tak všetky koeficienty tohoto polynómu sú deliteľné p.

Dôkaz. Budeme postupovať indukciou podľa stupňa $f(x)$. Ak je to polynóm lineárny tak $f(x) = a_1x + a_0$. Nech $x_1 \neq x_2$ sú dve primitívne riešenia. Potom

$$a_1x_1 + a_0 \equiv 0 \pmod{p}$$

$$a_1x_2 + a_0 \equiv 0 \pmod{p}.$$

Ak odčítame prvú kongruenciu od druhej, dostávame

$$a_1(x_2 - x_1) \equiv 0 \pmod{p}.$$

Z toho, že $x_2 - x_1 \not\equiv 0 \pmod{p}$ vyplýva $a_1 \equiv 0 \pmod{p}$ a teda aj $a_0 \equiv 0 \pmod{p}$.

Predpokladajme, že veta platí pre polynómy stupňa $n-1$ a $f(x)$ je polynóm stupňa n a $x_1, \ldots, x_{n+1}$ sú primitívne riešenia uvažovanej kongruencie. Môžeme si vyjadriť

$$f(x) = g(x)(x - x_1) + c, \tag{22}$$

kde $g(x)$ je polynóm s čeločíselnými koeficietami. Ak dosadíme do tohoto vyjadrenia x_1, dostávame

$$f(x_1) = g(x_1)(x_1 - x_1) + c \equiv 0 \pmod{p},$$

a teda $c \equiv 0 \pmod{p}$. Inak povedané $p|c$. Z toho vyplýva

$$f(x) \equiv g(x)(x - x_1) \pmod{p}.$$

Postupným dosádzaním do tejto kongruencie dostávame $g(x_j) \equiv 0 \pmod{p}$ pre $j = 2, \ldots, n+1$. Teda kongruencia

$$g(x) \equiv 0 \pmod{p}$$

má aspoň n primitívnych riešení . Preto podľa indukčného predpokladu sú všetky koeficienty tohoto polynómu deliteľné p. Z vyjadrenia (22) vyplýva to isté pre polynóm $f(x)$. □

Príklad 73. Nech $p > 2$ je prvočíslo. Uvažujme polynóm

$$f(x) = (x+1)\dots(x+p-1) - x^{p-1} + 1.$$

Z malej Fermatovej vety vyplýva, že všetky $j = 0, \dots, p-1$ sú primitívne riešenia kongruencie

$$f(x) \equiv 0 \pmod{p}.$$

Ale stupeň tohoto polynómu je najviac $p-2$. Preto všetky jeho koeficienty sú deliteľné p a teda aj konštatný koeficient. Teda platí

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Táto kongruencia sa nazýva **Wilsonova veta**. ∘

Príklad 74. Pomocou rozvoja exponenciálnej funkcie do Taylorovho radu sa dá dokázať rovnosť

$$e^{ia} = \cos a + i \sin a, a \in \mathbb{R}.$$

Z tejto rovnosti vyplýva

$$e^{2\pi i a} = 1 \iff a \in \mathbb{Z}.$$

Teda ak p je prvočíslo a $c \in \mathbb{Z}$ tak

$$\sum_{j=0}^{p-1} e^{2\pi i \frac{jc}{p}} = 0,$$

ak $p \nmid c$ a

$$\sum_{j=0}^{p-1} e^{2\pi i \frac{jc}{p}} = p,$$

ak $p|c$. Z toho vyplýva, že pre polynóm z celočíselnými koeficientami $f(x)$ sa počet primitívnych riešení kongruencie

$$f(x) \equiv 0 \pmod{p}$$

rovná

$$\frac{1}{p} \sum_{x=0}^{p-1} \sum_{j=0}^{p-1} e^{2\pi i \frac{jf(x)}{p}}.$$

∘

Príklad 75. Ak si uvedomíme, že kongruencia

$$x^k \equiv 0 \pmod{p}$$

má jediné primitívne riešenie pre $k \in \mathbb{N}$, dostávame z predošlého prikladu rovnosť

$$\sum_{j=0}^{p-1} \sum_{x=0}^{p-1} e^{2\pi i \frac{jx^k}{p}} = p.$$

∘

2.5 Primitívne korene

Ak $m \in \mathbb{N}$ tak $a \in Z$ sa nazýva **primitívny koreň** modulo m ak pre každé $j \in \mathbb{Z}_m^*$ existuje $n \in \mathbb{N}$ také, že $a^n \equiv 1 \pmod{m}$. Inými slovami primitívny koreň je celé číslo nesúdeliteľné s m, ktoré má rád $\varphi(m)$ modulo m.

Príklad 76. 2 je primitívny koreň modulo 5. Alebo 3 je primitívny koreň modulo 7. ∘

Veta 21. Nech p je prvočíslo. Potom pre každé d, ktoré je deliteľom $p-1$, existuje práve $\varphi(d)$ prvkov $\mathbb{Z}_p^*$ rádu d.

Dôkaz. Kongruencia

$$x^d \equiv 1 \pmod{p} \tag{23}$$

má najviac d riešení . Predpokladajme, že existuje $a \in \mathbb{Z}_m^*$ také, že $\mathbf{ord}(a) = d$. Potom zvyšky $1, a, \ldots, a^{d-1}$ po delení p sú všetky rôzne a sú primitívnymi riešeniami kongruencie (23). Preto sú to všetky primitívne riešenia tejto kongruencie. Teda každý prvok rádu d z $\mathbb{Z}_m^*$ je v tvare $a^k, (k,d) = 1$. Označme $\lambda(d)$ počet prvkov rádu d v v $\mathbb{Z}_m^*$. Z predšlého vyplýva, že $\lambda(d) = 0$ alebo $\lambda(d) = \varphi(d)$. Nech $d_1, \ldots, d_\ell$ sú všetky delitele $p-1$. Potom

$$\lambda(d_1) + \cdots + \lambda(d_\ell) = p - 1.$$

Vieme však, že

$$\varphi(d_1) + \cdots + \varphi(d_\ell) = p - 1.$$

Preto musí platiť $\lambda(d_j) = \varphi(d_j)$ pre $j = 1, \ldots, \ell$. □

Z tejto vety vyplźva, že existuje $\varphi(p-1)$ primitívnych koreňov modulo p.

Príklad 77. Existencia primitívneho koreňa modulo p vyplýva aj z príkladu 54 a Lagrangeovej vety. Ak R je maximálny rád prvkov modulo p, tak každé $a \in \mathbb{Z}_p^*$ je primitívnym riešením kongruencie $x^R - 1 \equiv 0 \pmod{p}$. Podľa Lagrangeovej vety je to možné iba v prípade $R = p - 1$. ∘

Vďaka existencii primitívneho koreňa modulo p môžeme definovať istú obdobu logaritmu. Ak $a \in \mathbb{Z}$,$(a, p) = 1$ a g je primitívny koreň modulo p, tak existuje jediné číslo $n \in \{0, \ldots, p-2\}$ také, že

$$a \equiv g^n \pmod{p}. \tag{24}$$

Túto hodnotu n nazývame **index** a modulo p pri základe g. Označujeme ju $\mathbf{ind}_g(a)$. Z toho, že g je rádu $p-1$ modulo p, dostávame

$$\mathbf{ind}_g(ab) \equiv \mathbf{ind}_g(a) + \mathbf{ind}_g(b) \pmod{p-1}, \tag{25}$$

pre $a, b \in \mathbb{Z}$, $(a, p) = (b, p) = 1$.

Index sa dá použiť hľadaní riešenia exponenciálnych kongruencií .

Príklad 78. Ktoré $x \in \mathbb{N}$ vyhovujú kongruencii $3^x + 4^x \equiv 1 \pmod{5}$? Číslo 2 je primitívny koreň modulo 5 a

$$3 \equiv 2^3 \pmod{5}, 4 \equiv 2^2 \pmod{5}.$$

Kongruenciu, ktorú riešime, dostávame takto do tvaru

$$2^{3x} + 2^{2x} \equiv 1 \pmod{5}.$$

Ak si označíme $t = 2^x$, tak musí platiť

$$t^3 + t^2 \equiv 1 \pmod{5}.$$

Teda sme dostali polynomickú kongruenciu. Jej primitívne riešenie je $t = 3$. Teda $2^x \equiv 3 \pmod{5}$ a preto $x \equiv 3 \pmod{4}$.

Príklad 79. Nech $p > 2$ je prvočíslo a $s_1, \ldots, s_p$ je úplný zvyškový systém modulo p. Dá sa dokázať, že v prípade $m \in \mathbb{N}$ $p - 1 \nmid m$ platí

$$\sum_{j=1}^{p} s_j^m \equiv 0 \pmod{p}.$$

Ak g je primitívny koreň modulo p, tak

$$g^m \not\equiv 1 \pmod{p}. \tag{26}$$

Z druhej strany aj $gs_1, \ldots, gs_p$ úplný zvyškový systém modulo p a teda

$$\sum_{j=1}^{p} s_j^m \equiv \sum_{j=1}^{p} (gs_j)^m \pmod{p},$$

čo znamená

$$\sum_{j=1}^{p} s_j^m \equiv g^m \sum_{j=1}^{p} s_j^m \pmod{p}.$$

Z vlastnosti (26) vyplýva dokazovaná kongruencia.

Príklad 80. Pomocou predchádzajúceho príkladu sa dá dokázať: Ak $f(x)$ je polynóm z celočíselnými koeficientami stupňa menšieho ako $p-1$, tak

$$\sum_{j=1}^{p} f(s_j) \equiv 0 \pmod{p}.$$

Príklad 81. Pomocou príkladu 67 sa dá dokázať trochu všoebecnejšie tvrdenie : Ak $f(x) = a_n x^n + \cdots + a_0, a_\ell \in \mathbb{Z}$, tak

$$\sum_{j=1}^{p} f(s_j) \equiv -\sum_{\substack{\ell \le n \\ p-1 | \ell}} a_\ell \pmod{p}.$$

Z príkladu 68 vidíme že, ak $m \in \mathbb{N}$ má aspoň dva nepárne prvočíselné delitele, tak neexistuje primitívny koreň modulo m. Teraz vyjasníme, ako to vyzerá v ostatných prípadoch.

Príklad 82. Nech p je prvočíslo. Ak $a \in \mathbb{N}, (a,p) = 1$, je taký primitívny koreň modulo p, že $a^{p-1} \not\equiv 1 \pmod{p^2}$, tak sa dá dokázať, že a je primitívny koreň modulo p^2. Vyplýva to z toho, že rád čísla a^{p-1} modulo p^2 môže byť $p-1$ alebo $(p-1)p = \varphi(p^2)$.

Veta 22. Nech p je prvočíslo. Ak g je taký primitívny koreň modulo p, že

$$g^{p-1} \not\equiv 1 \pmod{p^2}, \tag{27}$$

tak g je primitívny koreň modulo p^α pre $\alpha = 2, 3, 4, \ldots$.

Dôkaz. Stačí dokázať, že rád prvku g modulo p^α je $\varphi(p^\alpha)$. Vieme, že $g^{(p-1)p^{\alpha-1}} \equiv 1 \pmod{p^\alpha}$. Z toho vyplýva, že rád prvku g^{p-1} je p^β, pre vhodné $\beta \le \alpha$. Predpokladajme

$$g^{(p-1)p^{\alpha-2}} \equiv 1 \pmod{p^\alpha}. \tag{28}$$

Hodnotu g^{p-1} si môžeme vyjadriť v tvare

$$g^{p-1} = 1 + kp,$$

pre vhodné celé číslo k. Podľa binomickej vety si preto môžeme vyjadriť

$$g^{(p-1)p^{\alpha-2}} = (1+kp)^{p^{\alpha-2}} \equiv 1 + kp^{\alpha-1} \pmod{p^\alpha}.$$

Ak to porovnáme s (28), dostávame

$$kp^{\alpha-1} \equiv 0 \pmod{p^\alpha}.$$

Z toho vyplýva $p|k$ a teda

$$g^{p-1} \equiv 1 \pmod{p^2},$$

a dostávame spor s (27). □

Príklad 83. Napríklad 2 je primitívny koreň modulo 5^α pre $\alpha = 1, 2, 3, \ldots$. Rovnako tak je 2 aj primitívny koreň modulo 7^α.

Ak g je primitívny koreň modulo p, ktorý nespĺňa podmienku (27) a $p \neq 2$, tak jednoduchou úpravou podľa binomickej vety sa dá dokázať, že $a+p$ je primitívny koreň modulo p, ktorý túto podmienku spĺňa. Preto platí

Veta 23. Ak $p \neq 2$ je prvočíslo a $\alpha \in \mathbb{N}$, tak existuje primitívny koreň modulo p^α.

Iná situácia je pri prvočísle 2.

Príklad 84. Matematickou indukciou sa dá dokázať, že pre každé nepárne prirodzené číslo a platí

$$a^{\frac{\varphi(2^\alpha)}{2}} = a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}.$$

pre $\alpha = 3, 4, 5 \ldots$. Teda ani v týchto prípadoch primitívny koreň neexistuje.

Veta 24. Ak $\alpha = 3, 4, 5, \ldots$, tak pre každé nepárne číslo a existujú jedonoznačne určené $j_1 \in \{0, \ldots, 2^{\alpha-2} - 1\}$ a $j_2 \in \{0.1\}$ také, že

$$a \equiv 5^{j_1}(2^\alpha - 1)^{j_2} \pmod{2^\alpha}.$$

Dôkaz. Stačí dokázať, že 5 je rádu $2^{\alpha-2} = \frac{\varphi(2^\alpha)}{2}$. Z predošlého príkladu dostáveme

$$5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}.$$

Ak by 5 mala nižší rád ako chceme dokázať, muselo by platiť

$$5^{2^{\alpha-3}} \equiv 1 \pmod{2^\alpha}. \tag{29}$$

Vieme, že $5 = 1 + 4$, a preto podľa binomickej vety dostávame

$$5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha}.$$

Porovnaním s (29) dostávame spor. □

Príklad 85. Podobným spôsobom sa dá dokázať, že

$$9^{2^{\alpha-4}} \equiv 1 + 2^{\alpha-2} \pmod{2^\alpha}$$

pre $\alpha \geq 4$.

2.6 Kvadratické zvyšky

Prdpokladajme, že p je nepárne prvočíslo. Celé číslo a, $(a, p) = 1$, sa nazýva **kvadratický zvyšok** modulo p práve vtedy, keď je riešiteľná kongruencia

$$x^2 \equiv a \pmod{p}. \tag{30}$$

Dosadím do Eulerovej vety vidíme, že ak a je kvadratický zvyšok, tak a je koreňom kongruencie

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \tag{31}$$

Nech g je primitívny koreň modulo p. Dané číslo a možeme vyjadriť v tvare

$$a \equiv g^k \pmod{p},\ k = 1, \ldots, p-1.$$

Pri tomto vyjadrení vidíme, že a je kvadratický zvyšok práve vtedy, keď k je párne číslo. Teda existuje presne $\frac{p-1}{2}$ kvadratických zvyškov modulo p. Kongruencia (31) môže mať najviac $\frac{p-1}{2}$ riešení modulo p. Preto a je kvadratický zvyšok práve vtedy, keď spĺňa túto túto kongruenciu.

Číslo $a \in \mathbb{Z}, (a, p) = 1$, ktoré nie je kvadratickým zvyškom modulo p sa nazýva **kvadratický nezvyšok** modulo p.

Ak si spomenieme na rozklad polynómu $t^2 - 1 = (t-1)(t_1)$, tak z Eulerovej vety dostávame

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

pre $a \in \mathbb{Z}$, $(a,p) = 1$. Teda pre každé $a \in \mathbb{Z}, (a,p) = 1$ platí $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Pretože kongruencia (31) nemá viac ako $\frac{p-1}{2}$ riešení modulo p, vyplýva z toho nasledujúce kritérium:

Veta 25. Ak $p \neq 2$ je prvočíslo a $a \in \mathbb{Z}, (a,p) = 1$, tak
a) a je kvadratický zvyšok modulo p práve vtedy, keď

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

b) a je kvadratický nezvyšok modulo p práve vtedy, keď

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

Príklad 86. Z predošlej vidíme, že $p-1$ je kvadratický zvyšok modulo p práve vtedy, keď $p \equiv 1 \pmod{4}$.

Príklad 87. Z vety 25, vyplýva aj to, že ak a_1, a_2 sú kvadratické nezvyšky modulo p, tak $a_1 a_2$ je kvadratický zvyšok modulo p. Samozrejme aj iné kombinácie.

Príklad 88. Veta 25 sa dá niekedy použiť na rýchle zistenie či dané a je kvadratický zvyšok modulo p. Napríklad pri násobení modulo 7 vidíme, že $5^3 \equiv -1 \pmod{7}$ a teda 5 je kvadratický nezvyšok. Ale $5^4 \equiv 1 \pmod{13}$ - 5 je kvadratický zvyšok modulo 13. Pri väčších prvočíslach je to už výpočtovo náročnejšie.

Príklad 89. Ak $p = 4k+3$ a $(a,p) = 1$, tak podľa vety 25 platí $a^{2k+2} \equiv \pm a \pmod{p}$. Teda a je kvadratický zvyšok modulo p práve vtedy, keď

$$a^{2k+2} \equiv a \pmod{p}.$$

V tomto prípade $\pm a^{k+1}$ modulo p sú všetky riešenia kongruencie (30) modulo p.

V prípade, že prvočíslo p je veľké, sú hore uvedené postupy výpočtovo náročné a teda pomalé. Odvodíme si rovnosti, resp. kongruencie, ktoré tieto postupy nahradia oveľa rýchlejšími.

Veta 26. Nech $p \neq 2$ je prvočíslo a $a \in \mathbb{Z}, (a,p) = 1$. Označme symbolom S počet takých $j \in \{1, \ldots, \frac{p-1}{2}\}$, pre ktoré zvyšok čísla aj po delení p prevyšuje $\frac{p-1}{2}$. Potom

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

Dôkaz. Množina, čísel

$$\Big\{ -\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots \frac{p-1}{2} \Big\}$$

Tvorí úplný zvyškový systém modulo p. Preto ak číslo $aj, j = 1, \ldots, \frac{p-1}{2}$ má zvyšok po delení p, ktorý neprevyšuje $\frac{p-1}{2}$, tak je kongruentné s nejakým $k_j . 1 \leq k_j \leq \frac{p-1}{2}$.

Ak daný zvyšok prevyšuje $\frac{p-1}{2}$ tak aj je kongruentné s $-k_j$. Takýchto zvyškov je práve S a teda $aj \equiv \pm k_j \pmod{p}$. Znamienko $-$ je práve pri S prvkov j. Ak tieto kongruancie vynásobíme, dostávame

$$a^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot \ldots \frac{p-1}{2} \equiv (-1)^S k_1 k_2 \ldots k_{\frac{p-1}{2}} \pmod{p}. \tag{32}$$

Ak sa nám podarí dokázať

$$j \neq \ell \Longrightarrow k_j \neq k_\ell, \tag{33}$$

tak $\{k_1, \ldots, k_{\frac{p-1}{2}}\} = \{1, \ldots, \frac{p-1}{2}\}$. Z kongruencie (32) preto vyplýva

$$a^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot \ldots \frac{p-1}{2} \equiv (-1)^S \cdot 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \pmod{p}.$$

Z čoho po vykrátení dostávame tvrdenie vety. Aby sme dokázali (33), uvažujme $k_j = k_\ell$, Potom

$$aj \equiv \pm a\ell \pmod{p},$$

teda

$$j \equiv \pm \ell \pmod{p}.$$

To je možné iba ak $j = \ell$, pretože $1 \leq k, \ell, \leq \frac{p-1}{2}$. □

Z tejto vety vidíme, že a je kvadratický zvyšok práve vtedy, keď S je párne číslo.

Veta 27. Pre S z vety 26 platí

$$S \equiv \sum_{j=1}^{\frac{p-1}{2}} \Big[\frac{2aj}{p} \Big] \pmod{2}.$$

Dôkaz Hodnotu aj si môžeme vyjadriť

$$aj = kp + r, r \in \left\{1, \ldots, \frac{p-1}{2}\right\}.$$

Preto

$$\left[\frac{2aj}{p}\right] = \left[2k + \frac{2r}{p}\right].$$

Z tohoto vyjadrenia vidíme, že ak $r \leq \frac{p-1}{2}$, tak

$$\left[\frac{2aj}{p}\right] = 2k.$$

A ak $r > \frac{p-1}{2}$, tak

$$\left[\frac{2aj}{p}\right] = 2k + 1.$$

Z toho vyplýva tvrdenie. □

Aby sme si situáciu zjednodušili zavedieme tzv. **Legendreov symbol** $(\frac{a}{p})$. Ak p je prvočíslo a $(a, p) = 1$, tak v prípade, že a je kvadratický zvyšok modulo p kladieme

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

V opačnom prípade

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

Práve tento symbol, respektíve jeho vlastnosti umožnia rýchlo zistiť, či dané číslo je kvadratický zvyšok alebo nezvyšok. Treba zdôrazniť, že **v tomto prípade nejde o zlomok.**

Podľa vety 25 dostávame

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}, \tag{34}$$

ak p je nepárne prvočíslo a $(a, p) = 1$. Z toho ďalej vyplýva

$$\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right), \tag{35}$$

$$\left(\frac{a^2}{p}\right) = 1, \tag{36}$$

$$\left(\frac{a_1 a_2}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right), \tag{37}$$

pre $(a_1 a_2, p) = 1$.

Teraz sformulujeme vetu, ktorá nám umožní jednoducho zisťovať kvadratické zvyšky alebo nezvyšky, ako sme to sľubovali vyššie.

Veta 28. Nech p a q sú rôzna nepárne prvočísla. Potom

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

Príklad 90. Napriklad chceme zistiť, či 5 je kvadratický zvyšok modulo 29. Podľa predošlej vety platí

$$\left(\frac{5}{29}\right) = \left(\frac{29}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

Teda 5 je kvadratický zvyšok modulo 29. Podobne dostávame

$$\left(\frac{7}{31}\right) = -\left(\frac{31}{7}\right) = -\left(\frac{3}{7}\right) = 1.$$

Príklad 91. Ak aspoň jedno z nepárnych prvočísel p, q je tvaru $4k+1$, tak

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

V opačnom prípade platí

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

Príklad 92.

$$\left(\frac{21}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{7}{101}\right) = \left(\frac{2}{3}\right)\left(\frac{3}{7}\right) = (-1)(-1) = 1.$$

Historický názov Vety 28 je **Gaussov kvadratický zákon reciprocity**. V nasledujúcom texte budeme robiť úvahy, ktoré vyústia do dôkazu tohoto tvrdenia.

Veta 29. Pre každé nepárne prvočíslo p platí

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

a pre nepárne celé číslo a, $(a,p) = 1$ platí

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{aj}{p}\right]}.$$

Dôkaz. Podľa (35) a (37) dostávame

$$\left(\frac{2}{p}\right) = \left(\frac{2+2p}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{\frac{1+p}{2}}{p}\right) = \left(\frac{\frac{1+p}{2}}{p}\right).$$

Pre exponent S z viet 26, 27 preto platí

$$S \equiv \sum_{j=1}^{\frac{p-1}{2}} \Big[\frac{(p+1)j}{p}\Big] \pmod 2.$$

Suma na pravej strane sa po vykrátení rovná

$$\sum_{j=1}^{\frac{p-1}{2}} \Big[j + \frac{j}{p}\Big] = \sum_{j=1}^{\frac{p-1}{2}} j = \frac{p^2-1}{8}.$$

Ideme dokazovať druhú rovnosť. Podobne ako v predošlom prípade dostávame

$$\Big(\frac{a}{p}\Big) = \Big(\frac{a+p}{p}\Big) = \Big(\frac{2}{p}\Big)\Big(\frac{\frac{a+p}{2}}{p}\Big). \tag{38}$$

Pre spomínaný exponent S v tomto prípade platí

$$S \equiv \sum_{j=1}^{\frac{p-1}{2}} \Big[\frac{(a+p)j}{p}\Big] \pmod 2.$$

Opäť vidíme, že suma na pravej strane sa rovná

$$\sum_{j=1}^{\frac{p-1}{2}} \Big[\frac{aj}{p} + j\Big] = \sum_{j=1}^{\frac{p-1}{2}} \Big[\frac{aj}{p}\Big] + \frac{p^2-1}{8}.$$

Po dosadení do (38) dostávame druhú rovnosť. □

Príklad 93. Ak $p = 4k+1$, tak 2 je kvadratický zvyšok modulo p práve vtedy, keď $2|k$.

Ak p je prvočíslo tvaru $4k+3$, tak 2 je kvadratický zvyšok modulo p práve vtedy, keď $2 \nmid k$.

Dôkaz vety 28. Podľa predošlej vety platí

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^E,$$

pričom

$$E = \sum_{j=1}^{\frac{p-1}{2}} \Big[\frac{qj}{p}\Big] + \sum_{k=1}^{\frac{q-1}{2}} \Big[\frac{pk}{q}\Big].$$

Stačí dokázať

$$E = \frac{p-1}{2}\frac{q-1}{2}. \tag{39}$$

Uvažujme množinu usporiadaných dvojíc

$$M = \Big\{(pk, qj); k = 1, \ldots, \frac{q-1}{2}, j = \frac{p-1}{2}\Big\}.$$

V tomto prípade nemôže nastať $pk = qj$. Preto množinu M môžeme rozdeliť na dve dizjunktné podmožiny

$$M = M_1 \cup M_2.$$

Kde $M_1 = \{(pk, qj) \in M; pk < qj\}$ a $M_2 = \{(pk, qj) \in M; pk > qj\}$. Keď si predstavíme ako vyzerajú prvky týchto množín, vidíme, že M_1 obsahuje $\sum_{j=1}^{\frac{p-1}{2}}[qj/p]$ prvkov a M_2 obsahuje $\sum_{k=1}^{\frac{q-1}{2}}[pk/q]$ prvkov. Z toho vyplýva rovnosť (39). □

2.7 Čínska veta o zvyškoch

Predpokladajme, že sú dané prirodzené čísla $m_1, \ldots, m_k$, ktoré sú navzájom nesúdelné, t. j. $(m_i, m_j) = 1$ pre $i \neq j$.

Označme

$$M = m_1 \ldots m_k$$

a

$$M_i = \frac{M}{m_i},\ i = 1, \ldots, k.$$

Číslo M_i je súčinom všetkých m_j kde $j \neq i$ a teda

$$(M_i, m_i) = 1, i = 1, \ldots, k.$$

Preto podľa Eulerovej vety , vety 16, dostávame

$$M_i^{\varphi(m_i)} \equiv 1 \pmod{m_i},\ i = 1, \ldots, k. \tag{40}$$

Veta 30. Ak $r_1, \ldots, r_k$ sú celé čísla a

$$R = r_1 M_i^{\varphi(m_1)} + \cdots + r_k M_k^{\varphi(m_k)} \tag{41}$$

tak

$$R \equiv r_i \pmod{m_i}, i = 1, \ldots k, \tag{42}$$

a každé celé číslo r vyhovuje (42) práve vtedy, keď

$$r \equiv R \pmod{m_1 \ldots m_k}.$$

Dôkaz. Ak si vyberieme nejaké konkrétne $i \leq k$ tak, ako sme už spomínali, číslo M_i je súčinom všetkých m_j pre $j \neq i$ a teda $m_j | M_i$ čo znamená

$$M_i^{\varphi(m_i)} \equiv 0 \pmod{m_j}, j \neq i.$$

Z kongruencie (40) teda vyplýva $R \equiv r_i \pmod{m_i}$.

Nech r je celé číslo. Toto číslo spĺňa kongruencie (42) práve vtedy, keď $R \equiv r \pmod{m_i}$ pre $i = 1, \ldots, k$. Čísla $m_i, i = 1, \ldots, k$ sú navzájom nesúdeliteľné preto tento prípad nastáva práve vtedy keď $R \equiv r \pmod{M}$. □

Číslo R z predošlej vety môže byť veľmi veľké, stačí uvažovať jeho zvyšok po delení M, teda pri výpočte môžeme použiť operácie modulo M.

Príklad 94. Pre každé $r \in \mathbb{Z}$ platí $r \equiv 2 \pmod{5}$ a $r \equiv 3 \pmod{7}$ práve vtedy keď $r \equiv 17 \pmod{35}$. ∘

Príklad 95. Pre každé $r \in \mathbb{Z}$ platí $r \equiv 9 \pmod{11}$ a $r \equiv 6 \pmod{15}$ a $r \equiv 5 \pmod{17}$ práve vtedy keď $r \equiv 141 \pmod{2805}$. ∘

Príklad 96. Ak $m_1, m_2 \in \mathbb{N}$ sú nesúdeliteľné, tak každému $a \in \mathbb{Z}^*_{m_1 m_2}$ môžeme priradiť usporiadanú dvojicu $[a_1, a_2] \in \mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2}$, pričom a_1 je zvyšok a po delení m_1 a a_2 je zvyšok po delení m_2. Podľa Čínskej zvyškovej je toto zobrazenie bijekcia a preto $|\mathbb{Z}_{m_1 m_2}| = |\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}|$. To znamená, že $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$. ∘

3 Čebyševove nerovnosti

Symbolom $\pi(x)$ budene označovať počet prvočísel, ktoré neprevyšujú reálne číslo x. Táto funkcia sa nazýva **prvočíselná funkcia**. Napríklad $\pi(1) = 0, \pi(2) = 1, \pi(5) = 3$. Na prvý pohľad je zrejmé, že platí

$$\pi(x) \leq [x] \tag{43}$$

pre $x \geq 1$. Z nekonečnosti množiny prvočísel vyplýva

$$\lim_{x \to \infty} \pi(x) = \infty.$$

Pri štúdiu prvočíselnej funkcie je dobré si uvedomiť nasledujúce skutočnosti. Množinu $\mathbb{N}$ môžeme vytvoriť dvomi spôsobmi. Prvý je ten, že začneme 1-kou a postupne pričítame 1 - ku. Tak dostávame usporiadanie tejto množiny podľa veľkosti. Iný spôsob je taký, že máme všetky prvočísla a tie násobíme.

Tento spôsob vedie na čiastočné usporiadanie podľa deliteľnosti. Hasseho diagram prvého usporiadania je jednoduchý zvislá čiara. Ak si načrtneme Hasseho diagram deliteľnosti, vidíme pomerne komplikovaný graf. To naznačuje, že popísať pojmy pochádzajúce z deliteľnosti pomocou veľkosti môže byť zložité. Isté jasno môžu do veci vniesť úvahy o veľkých číslach, ktoré majú zároveň veľa deliteľov. Teda sú dostatočne vysoko v oboch grafoch. Jedným z takýchto typov čísel sú faktoriály.

Ďalšiu dôležitú úlohu bude zohrávať logaritmická funkcia. Jej význam spočíva v tom, že prevádza súčin na súčet.

Začneme kombinačným číslom $\binom{2k+1}{k+1}$, $k \in \mathbb{N}$. Keď ho vyjadríme v tvare zlomku, dostávame

$$\binom{2k+1}{k+1} = \frac{(2k+1)!}{k!(k+1)!}.$$

Ak zmeníme poradie činiteľov v čitateli tak, že najprv napíšeme všetky párne a potom nepárne, tak dostávame čitateľ v tvare

$$(2k+1)! = 2 \cdot \dots \cdot (2k) \cdot 1 \cdot 3 \cdot \dots \cdot (2k+1) = 2^k k! \cdot 1 \cdot 3 \cdot \dots \cdot 2k+1.$$

Každý nepárny činiteľ druhej časti tohoto súčinu môžeme zhora odhadnúť najbližším párnym číslom a dostávame

$$(2k+1)! \leq 2^k k! \cdot 2^k (k+1)!,$$

z čoho vyplýva nerovnosť

$$\binom{2k+1}{k+1} \leq 4^k. \tag{44}$$

Každé prvočíslo, ktoré patrí do intervalu $[k+2, 2k+1]$ sa vyskytuje v čitateli $\binom{2k+1}{k+1}$, ale sa nevyskytuje v menovateli tohoto zlomku. Preto je daný binomický koeficient týmto prvočíslom deliteľný. Z toho vyplýva

$$\prod_{k+1<p\leq 2k+1} p \Big| \binom{2k+1}{k+1},$$

a teda podľa (44) dostávame

$$\prod_{k+1<p\leq 2k+1} p \leq 4^k. \tag{45}$$

Veta 31. Pre každé prirodzené číslo n platí

$$\prod_{p\leq n} p \leq 4^n.$$

Dôkaz. Budeme postupovať indukciou. Pre $n = 1, 2$ tvrdenie platí . Predpokladajme, že platí pre vsetky $n' \leq n$. Ak $n+1$ je párne číslo, tak $\prod_{p\leq n} p = \prod_{p\leq n+1} p$ a teda veta platí aj v tomto prípade. Nech $n+1$ je nepárne číslo. Teda $n+1 = 2k+1$. Potom

$$\prod_{p\leq n+1} p = \prod_{p\leq k+1} p \cdot \prod_{k+1<p\leq 2k+1} p.$$

Je zrejmé, že $k+1 \leq n$ a teda podľa indukčného predpokladu máme

$$\prod_{p\leq k+1} p \leq 4^{k+1}.$$

Preto podľa (45) dostávame

$$\prod_{p\leq 2k+1} p \leq 4^{2k+1}.$$

□

Príklad 97. Ak v predošlej vete zlogaritmujeme obidve strany nerovnosti, dostávame

$$\sum_{p\leq n} \ln p \leq n \ln 4.$$

Môžeme to vyjadriť aj

$$\sum_{p\leq n} \ln p = \mathcal{O}(n).$$

∘

Tento výsledok nám umožní dokázať horný odhad prvočíselnej funkcie. Z príkladu 97 dostávame

$$\sum_{\sqrt{n}<p\leq n} \ln p \leq n \ln 4.$$

Ak každý sčítanec poslednej sumy odhadneme zdola hodnotou $\ln \sqrt{n}$, dostávame nerovnosť

$$(\pi(n) - \pi(\sqrt{n})) \ln \sqrt{n} \leq n \ln 4.$$

To znamená

$$\pi(n) \leq \frac{2n \ln 4}{\ln n} + \pi(\sqrt{n}) \leq \frac{2n \ln 4}{\ln n} + \sqrt{n}.$$

Ak zoberieme do úvahy nerovnosť

$$\sqrt{x} \leq \frac{x}{\ln x}$$

pre $x \geq 2$, dostávame

$$\pi(n) \leq \frac{2n \ln 4}{\ln n} + \frac{n}{\ln n} = (2 \ln 4 + 1)\frac{n}{\ln n}, n \geq 2. \tag{46}$$

Aby sme odvodili dolný odhad pre prvočíselnú funkciu, využijeme vlastnosti binomického koeficientu $\binom{2n}{n}$. Dôležitú úlohu bude hrať vyjadrenie faktoriálov v tvare kanonického rozkladu. Začneme preto takto:

Veta 32. Ak p je prvočíslo a $n \in \mathbb{N}$, tak p sa vyskytuje v kánonickom rozklade $n!$ s exponentom

$$\alpha(p, n) = \sum_{j \leq \frac{\ln n}{\ln p}} \left[\frac{n}{p^j}\right].$$

Dôkaz. Ak $j \leq \frac{\ln n}{\ln p}$, tak množina $\{1, \ldots, n\}$ obsahuje práve $[\frac{n}{p^j}] - [\frac{n}{p^{j+1}}]$ čísel, ktoré majú v kánonickom rozklade prvočíslo p s exponentom j. Preto p bude v kánonickom rozklade $n!$ vystupovať s exponentom

$$\sum_{j \leq \frac{\ln n}{\ln p}} j\left(\left[\frac{n}{p^j}\right] - \left[\frac{n}{p^{j+1}}\right]\right) = \sum_{j \leq \frac{\ln n}{\ln p}} j\left[\frac{n}{p^j}\right] - \sum_{j \leq \frac{\ln n}{\ln p}} j\left[\frac{n}{p^{j+1}}\right] =$$

$$= \sum_{j \leq \frac{\ln n}{\ln p}} j\left[\frac{n}{p^j}\right] - \sum_{i \leq \frac{\ln n}{\ln p}+1} (i-1)\left[\frac{n}{p^i}\right] =$$

$$= \sum_{j \leq \frac{\ln n}{\ln p}} \left[\frac{n}{p^j}\right].$$

□

Príklad 98. Môžeme si vyjadriť $\ln n! = n \ln n - n + \mathcal{O}(\ln n)$. Podľa predošlej vety platí

$$\ln n! = \sum_{p \leq n} \left[\frac{n}{p}\right] \ln p + \sum_{p \leq n} \sum_{j=2}^{\frac{\ln n}{\ln p}} \left[\frac{n}{p^j}\right] \ln p = n \sum_{p \leq n} \frac{\ln p}{p} + \mathcal{O}(n).$$

Preto

$$n \ln n - n + \mathcal{O}(\ln n) = n \sum_{p \leq n} \frac{\ln p}{p} + \mathcal{O}(n).$$

Z toho po úpravách vyplýva

$$\sum_{p\leq n}\frac{\ln p}{p}=\ln n+\mathcal{O}(1).$$

∘

Z predošlej vety vidíme, že prvočíslo $p\leq 2n$ vystupuje v kánonickom rozklade binomického koeficientu $\binom{2n}{n}$, $n\in\mathbb{N}$ s exponentom

$$\sum_{j\leq\frac{\ln 2n}{\ln p}}\left[\frac{2n}{p^j}\right]-2\left[\frac{n}{p^j}\right].$$

Z toho vyplýva, že

$$\ln\binom{2n}{n}=\sum_{p\leq 2n}\ln p\sum_{j\leq\frac{\ln 2n}{\ln p}}\left[\frac{2n}{p^j}\right]-2\left[\frac{n}{p^j}\right]. \tag{47}$$

Odvodíme si zase nerovnosti pre daný binomický koeficient, ktoré využijeme pri štúdiu tejto rovnosti. Platí

$$\binom{2n}{n}=\frac{(2n)!}{n!^2}=\frac{2^n n!\cdot 1\cdot 3\cdot\dots\cdot 2n-1}{n!^2}=\frac{2^n\cdot 1\cdot 3\cdot\dots\cdot 2n-1}{n!}.$$

Ak odhadneme každý nepárny činiteľ čitateľa posledného zlomku najbližším párnym číslom zdola, dostávame nerovnosť

$$\binom{2n}{n}\geq\frac{2^n\cdot 2\cdot 4\cdot\dots\cdot 2(n-1)}{n!}=\frac{2^{2n-1}}{n}.$$

Príklad 99. Podobným spôsobom sa dá dokázať

$$\binom{2n}{n}\leq 4^n, n\geq 2.$$

∘

Z rovnosti (47) teda vyplýva

$$\sum_{p\leq 2n}\ln p\sum_{j\leq\frac{\ln 2n}{\ln p}}\left[\frac{2n}{p^j}\right]-2\left[\frac{n}{p^j}\right]\geq(2n-1)\ln 2-\ln n. \tag{48}$$

Hodnota $[2x] - 2[x]$ sa rovná 0 alebo 1. Z toho vyplýva

$$\Big[\frac{\ln 2n}{\ln p}\Big] \geq \sum_{j \leq \frac{\ln 2n}{\ln p}} \Big[\frac{2n}{p^j}\Big] - 2\Big[\frac{n}{p^j}\Big].$$

Preto z (48) vyplýva

$$\sum_{p \leq 2n} \Big[\frac{\ln 2n}{\ln p}\Big] \ln p \geq (2n-1)\ln 2 - \ln n.$$

Z nerovnosti

$$\Big[\frac{\ln 2n}{\ln p}\Big] \ln p \geq \ln 2n - \ln p$$

preto dostávame

$$\pi(2n)\ln 2n - \sum_{p \leq 2n} \ln p \geq (2n-1)\ln 2 - \ln n.$$

A teda

$$\pi(2n)\ln 2n \geq (2n-1)\ln 2 - \ln n + 2n\ln 4 = 2n\ln 8 - \ln 2n.$$

Z toho vyplýva

$$\pi(2n) \geq \frac{2n\ln 8 - \ln 2n}{\ln 2n} = \ln 8 \frac{2n}{\ln 2n} - 1.$$

Dokázali sme výsledok, ktorý sa v literatúre býva nazývaný **Čebyševove nerovnosti**:

Veta 33. Existujú také kladné konštanty c_1, c_2, že pre každé reálne číslo $x > 2$ platí

$$c_1 \frac{x}{\ln x} \leq \pi(x) \leq c_2 \frac{x}{\ln x}$$

Príklad 100. Teraz môžeme odhadnúť zdola

$$\sum_{p \leq n} \ln p \geq \sum_{\sqrt{n} < p \leq n} \ln p \geq \frac{\ln n}{2}(\pi(n) - \pi(\sqrt{n})).$$

Podľa Čebyševovych nerovností dostávame

$$\pi(n) - \pi(\sqrt{n}) \geq c_2 \frac{n}{\ln n} - c_1 \frac{2\sqrt{n}}{\ln n}, n \geq 2.$$

Z toho po úpravách vyplynie

$$\sum_{p \leq n} \ln p \geq c_3 n, n \in \mathbb{N}. \tag{49}$$

pre vhodnú konštantu $c_3 > 0$. ∘

Príklad 101. Nech $2 = p_1 < p_2 < \cdots < p_n \ldots$ je postupnosť všetkých prvočísel usporiadaná podľa veľkosti. Pomocou Čebyševovych nerovností sa dá dokázať ,že

$$\kappa_1 n \ln n \leq p_n \leq \kappa_2 n \ln n,$$

pre vhodné $\kappa_1, \kappa_2 > 0$. Ak totiž dosadíme do Čebyševovych nerovností $x = p_n$, tak dostávame

$$c_1 \frac{p_n}{\ln p_n} \leq n \leq c_2 \frac{p_n}{\ln p_n}.$$

Z toho vyplýva okrem iného

$$n \ln p_n \leq c_2 p_n.$$

Určite platí $n \leq p_n$ a teda

$$n \ln n \leq c_2 p_n.$$

Z druhej strany dostávame, že

$$n \ln p_n \geq c_1 p_n. \tag{50}$$

Ak si uvedimíme, že $\sqrt{x} \leq \frac{x}{\ln x}, x \geq 2$

$$c_1 \sqrt{p_n} \leq n$$

a teda

$$p_n \leq c_4 n^2$$

pre vhodnú konštantu $c_4 > 0$. Ak z tejto nerovnosti dosadíme do (50) dostávame

$$n(2 \ln n + \ln c_4) \geq p_n.$$

Z toho po drobných úpravách dostávame

$$p_n \leq \kappa_2 n \ln n,$$

pre nejakú kladnú konštantu κ_2. ∘

Príklad 102. Z predošlého príkladu vyplýva

$$\sum_p \frac{1}{p} = \infty.$$

∘

4 Eulerova sumačná formula

Veta 34. Ak f je reálna funkcia definovaná na intervale $[1,\infty)$, ktorá tam má spojitú deriváciu, tak pre každé $n \in \mathbb{N}$ platí

$$f(n+1) = \int_n^{n+1} f(x)dx + \int_n^{n+1} \{x\}f'(x)dx.$$

Dôkaz. Začneme rovnosťou

$$\int_n^{n+1} \{x\}f'(x)dx = \int_n^{n+1} (x-n)f'(x)dx =$$

$$-n\int_n^{n+1} f'(x)dx + \int_n^{n+1} xf'(x)dx =$$

$$-n(f(n+1)-f(n)) + \int_n^{n+1} xf'(x)dx.$$

Použitím metódy per partes na druhý sčítanec dostávame

$$\int_n^{n+1} xf'(x)dx = [xf(x)]_n^{n+1} - \int_n^{n+1} f(x)dx =$$

$$= nf(n) - (n+1)f(n+1) - \int_n^{n+1} f(x)dx.$$

Ďalej platí

$$nf(n) - (n+1)f(n+1) + n(f(n+1)-f(n)) = f(n+1).$$

Preto

$$\int_n^{n+1} xf'(x)dx = f(n+1) - \int_n^{n+1} f(x)dx.$$

□

Z toho hneď vyplýva:

Veta 35. Ak f je reálna funkcia definovaná na intervale $[1,\infty)$ a má tam spojitú deriváciu, tak

$$\sum_{n=1}^{N} f(n) = f(1) + \int_1^N f(x)dx + \int_1^N \{x\}f'(x)dx.$$

V ďalšom zavedieme jedno označenie, ktoré nám umožní vyhnúť sa komplikovaným výrazom, ktorých detaily nie sú dôležité. Bude nás zaujímať iba to, ako rýchlo rastú, prípadne klesajú. Ak f, g sú funkcie definované na nejakej množine, tak píšeme $f(x) = \mathcal{O}(g(x))$, ak existuje kladná konštanta κ taká, že

$$|f(x)| \leq \kappa g(x) \tag{51}$$

pre každé x z danej množiny. Treba upozorniť , že nejde o klasickú rovnosť ale odhad. Napríklad ak, $f(x)$ je polynóm n - tého stupňa, tak na interevale $[1, \infty)$ platí

$$f(x) = \mathcal{O}(x^n).$$

Tento symbol sa nazýva **veľké O**. Rovnosť (4) môžeme vyjadriť

$$\sum_{n=1}^{N} \frac{1}{n^2} = \frac{\pi^2}{6} + \mathcal{O}\Big(\frac{1}{N}\Big). \tag{52}$$

Príklad 103. Ak použijeme predošlú vetu na harmonický rad, dostávame

$$\sum_{n=1}^{N} \frac{1}{n} = 1 + \int_1^N \frac{dx}{x} - \int_1^N \frac{\{x\}dx}{x^2} = 1 + \ln N + \int_1^N \frac{\{x\}dx}{x^2}.$$

Inak napísané

$$\sum_{n=2}^{N} \frac{1}{n} - \ln N = \int_1^N \frac{\{x\}dx}{x^2}.$$

Integrál na pravej strane konverguje, preto existuje vlastná limita

$$C = \lim_{N\to\infty} \sum_{n=1}^{N} \frac{1}{n} - \ln N = \int_1^\infty \frac{\{x\}dx}{x^2}.$$

Nevlastný integrál na pravej strane si môžeme rozpísať

$$C = \int_1^\infty \frac{\{x\}dx}{x^2} = \int_1^N \frac{\{x\}dx}{x^2} + \int_N^\infty \frac{\{x\}dx}{x^2}.$$

Ďalej platí

$$0 \leq \int_N^\infty \frac{\{x\}dx}{x^2} \leq \int_N^\infty \frac{dx}{x^2} = \frac{1}{N}.$$

Preto

$$\int_1^N \frac{\{x\}dx}{x^2} = C - 1 + \mathcal{O}\Big(\frac{1}{N}\Big).$$

Tým sme dokázali odhad

$$\sum_{n=1}^{N} \frac{1}{n} = \ln N + C + \mathcal{O}\Big(\frac{1}{N}\Big). \tag{53}$$

Hodnota C ktorá vystupuje v rovnosti (53) sa nazýva **Eulerova konštanta**. Treba upozorniť čitateľa, aby si ju neplietol so Eulerovým číslom e.

Príklad 104. Podobným spôsobom sa dá odvodiť

$$\sum_{n=1}^{N} \ln n = N \ln N - N + \mathcal{O}(\ln N). \tag{54}$$

∘

Príklad 105. Dá sa odvodiť aj

$$\sum_{n \le N} \ln \frac{N}{n} = \mathcal{O}(N).$$

Príklad 106. Podobne sa dajú sa odvodiť odhady

$$\sum_{n=1}^{N} \frac{1}{\sqrt{n}} = 2\sqrt{N} + K + \mathcal{O}\Big(\frac{1}{\sqrt{N}}\Big), \tag{55}$$

$$\sum_{n=2}^{N} \frac{1}{n \ln n} = \ln \ln N + K_1 + \mathcal{O}\Big(\frac{1}{N \ln N}\Big), \tag{56}$$

$$\sum_{n=2}^{N} \frac{1}{\ln n} = \int_2^N \frac{dt}{\ln t} + K_2 + \mathcal{O}\Big(\frac{1}{\ln N}\Big). \tag{57}$$

Z posledného odhadu sa dá pomocou l'Hospitalovho pravidla dokázať

$$\lim_{N \to \infty} \frac{\ln N}{N} \sum_{n=2}^{N} \frac{1}{\ln n} = 1.$$

∘

Príklad 107. Dá sa dokázať všeobecnejšie: Ak f je nezáporná nerastúca reálna funkcia definovaná na intervale $[a, \infty), a \in \mathbb{N}$, $\lim_{x \to \infty} f(x) = 0$ a má tam spojitú deriváciu, tak

$$\sum_{n=a}^{N} f(n) = \int_a^N f(t)dt + K + \mathcal{O}(f(N)),$$

kde $K = \int_a^\infty \{t\} f'(t)dt$.

5 Dirichletova konvolúcia

Pod pojmom **aritmetická funkcia** budeme myslieť postupnosť reálnych alebo komplexných čísel. Ak f, g sú dve aritmetické funkcie, tak aritmetická funkcia $f * g$ definovaná rovnosťou

$$(f * g)(n) = \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big) \tag{58}$$

sa nazýva **Dirichletova konvolúcia** f a g.

Ak f, g sú aritmerické funkcie a $h = g * f$, tak pre sumáciu h platí

$$\sum_{n\le x} h(n) = \sum_{n\le x} \sum_{d|n} f(d) h\Big(\frac{n}{d}\Big).$$

V poslednej sume môžeme vyjadriť $n = kd \le x$ a dostávame

$$\sum_{n\le x} h(n) = \sum_{kd\le x} f(d)h(k) = \sum_{d\le x} f(d) \sum_{k\le \frac{x}{d}} h(k). \tag{59}$$

Označme $i(n) = 1, n \in \mathbb{N}$. Túto aritmetickú funkciu budeme nazývať **jednotková funkcia**.

Príklad 108. Dá sa dokázať, že $i * i$ je aritmetická funkcia, ktorá každému prirodzenému číslu priraďuje počet jeho deliteľov. ∘

Počet deliteľov prirodzeného čísla n budeme označovať $\tau(n)$. Teda $\tau = i * i$.

Príklad 109. Pre sumačnú funkciu funkcie τ patí

$$\sum_{n\le x} \tau(n) = \sum_{n\le x} \sum_{d|n} 1 = \sum_{kd\le x} 1 = \sum_{d\le x} \sum_{k\le \frac{x}{d}} 1 = \sum_{d\le x} \Big[\frac{x}{d}\Big].$$

A teda

$$\sum_{n\le x} \tau(n) = x \sum_{d\le x} \frac{1}{d} + \mathcal{O}(x).$$

Z tejto rovnosti sa dá pomocou príkladu 103 odvodiť

$$\lim_{x\to\infty} \frac{1}{x \ln x} \sum_{n\le x} \tau(n) = 1.$$

∘

Tento príklad ukazuje, že aj keď sa funkcia τ správa na číselnej osi nepravidelne, tak jej sumačná funkcia má pravidelný rast.

Príklad 110. Odhad sumačnej funkcie τ z príkladu 109 sa dá zlepšiť. Podstatnú úlohu tam hral odhad hodnoty $\sum_{kd\leq n} 1$. Je to počet prvkov množiny

$$I = \{[k,d]; kd \leq n\}.$$

Ak $kd \leq n$ tak $k \leq \sqrt{n}$ alebo $d \leq \sqrt{n}$. Preto

$$I = \{[k,d]; kd \leq n, k \leq \sqrt{n}\} \cup \{[k,d]; kd \leq n, d \leq \sqrt{n}\}.$$

To znamená

$$\sum_{kd\leq n} 1 = \sum_{\substack{kd\leq n\\ k\leq\sqrt{n}}} 1 + \sum_{\substack{kd\leq n\\ d\leq\sqrt{n}}} 1 - \sum_{\substack{k\leq\sqrt{n}\\ d\leq\sqrt{n}}} 1 =$$

$$\sum_{d\leq\sqrt{n}} \Big[\frac{n}{d}\Big] + \sum_{k\leq\sqrt{n}} \Big[\frac{n}{k}\Big] - [\sqrt{n}]^2 = 2\sum_{d\leq\sqrt{n}} \Big[\frac{n}{d}\Big] - [\sqrt{n}]^2 =$$

$$2n\sum_{d\leq\sqrt{n}} \frac{1}{d} + \mathcal{O}(\sqrt{n}) - (\sqrt{n} - \{\sqrt{n}\})^2.$$

Ak použijeme vyjadrenie čiastočného súčtu harmonického radu podľa príkladu 103, dostávame

$$\sum_{j\leq n} \tau(j) = 2n\Big(\ln\sqrt{n} + 2C + \mathcal{O}\Big(\frac{1}{\sqrt{n}}\Big)\Big) - n + \mathcal{O}(\sqrt{n}) =$$

$$= n\ln n + (2C-1)n + \mathcal{O}(\sqrt{n}).$$

Teda sa nám podarilo odhad $\mathcal{O}(n)$ nahradiť presnejším odhadom $\mathcal{O}(\sqrt{n})$. ∘

Istý význam má Dirichletova konvolúcia aj pri ščítaní nekonečných radov.

Príklad 111. Ak pre dané aritmetické funkcie f, g a reálne číslo s nekonečné rady

$$\sum_{n=1}^{\infty} \frac{(f*g)(n)}{n^s}, \Big(\sum_{n=1}^{\infty} \frac{f(n)}{n^s}\Big), \Big(\sum_{n=1}^{\infty} \frac{g(n)}{n^s}\Big)$$

absolútne konvergujú, tak

$$\sum_{n=1}^{\infty} \frac{(f*g)(n)}{n^s} = \Big(\sum_{n=1}^{\infty} \frac{f(n)}{n^s}\Big)\Big(\sum_{n=1}^{\infty} \frac{g(n)}{n^s}\Big).$$

∘

Veta 36. Ak f, g, h sú aritmetické funkcie, tak

$$f * g = g * f \tag{60}$$

$$(f * g) * h = f * (g * h). \tag{61}$$

Dôkaz. Rovnosť (60) vyplýva z toho, že ak d prebieha všetky delitele daného $n \in \mathbb{N}$, tak aj $\frac{n}{d}$ prebieha všetky delitele daného prirodzeného čísla. Rovnosť (61) dostaneme tak, že jej obidve strany upravíme na hodnotu

$$\sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3).$$

□

Aritmetická funkcia I definovaná, tak že $I(1) = 1$ a $I(n) = 0, n \geq 2$ spĺňa rovnosť

$$f * I = f,$$

čo ľahko preveríme dosadením. Je to teda neutrálny prvok vzhľadom na Dirichletovu konvolúciu. Tu sa samozrejme ponúka otázka inverzného prvku. Takáto funkcia sa nazýva **Dirichletova inverzia** k danej aritmetickej funkcii. Dá sa zostrojiť takto:
Z rovnosti $f * g = I$ vyplýva $g(1) = \frac{1}{f(1)}$. Ak je funkcia g definovaná pre všetky prirodzené čísla menšie ako dané $n \in \mathbb{N}, n > 1$, tak

$$f(1)g(n) = -\sum_{\substack{d|n \\ d<n}} g(d) f\Big(\frac{n}{d}\Big). \tag{62}$$

Dokázali sme

Veta 37. Ak f je taká aritmetická funkcia, že $f(1) \neq 0$, tak existuje jediná aritmetická funkcia g taká, že $f * g = I$. Ak $f(1) = 0$, tak taká funkcia neexistuje.

Dirichletovu inverziu k aritmerickej funkcii f budeme označovať f^{-1}.

Príklad 112. Ak $f(1) \neq 0$ a p je prvočíslo, tak podľa (62) dostávame

$$f^{-1}(p) = -\frac{f^{-1}(1) f(p)}{f(1)} = -\frac{f(p)}{f^2(1)},$$

ak p je prvočíslo. Potom

$$f^{-1}(p^2) = -\frac{1}{f(1)}(f^{-1}(p) f(p) + f^{-1}(1) f(p^2)).$$

Pre ľubovoľné $\alpha \in \mathbb{N}$ platí

$$f^{-1}(p^\alpha) = -\frac{1}{f(1)}(f^{-1}(p^{\alpha-1})f(p) + \cdots + f^{-1}(1)f(p^\alpha)).$$

∘

Aritmetická funkcia f sa nazýva **multiplikatívna**, ak

$$(n_1, n_2) = 1 \Longrightarrow f(n_1 n_2) = f(n_1)f(n_2),$$

pre $n_1, n_2 \in \mathbb{N}$. Štúdium multiplikatívnych funkcií uľahčuje fakt, že ich hodnoty sú dané hodnotami v číslach tvaru p^α, kde p je prvočíslo a $\alpha \in \mathbb{N}$. Inak povedané pre multiplikatívnu aritmetickú funkciu f platí

$$f(n) = f(p_1^{\alpha_1}) \dots f(p_k^{\alpha_k}), \tag{63}$$

pričom $n = p_1^{\alpha_1} \dots p_1^{\alpha_1}$ je kánonický rozklad n. Jednoduchým príkladom multiplikatívnych aritmetických funkcií sú identická funkcia $id(n) = n$ a jednotková funkcia $i(n) = 1$, pre $n \in \mathbb{N}$. Ak multiplikatívna aritmetická funkcia f nadobúda aspoň jednu nenulovú hodnotu, napríklad $f(n) \neq 0$, tak $f(n) = f(n \cdot 1) = f(n)f(1)$ a teda po vykrátení dostávame

$$f(1) = 1. \tag{64}$$

Veta 38. Ak f, g sú multiplikatívne aritmetické funkcie, tak ak $f * g$ je multiplikatívna aritmetická funkcia.

Dôkaz. Ak $(n_1, n_2) = 1$ tak podľa Hlavnej vety aritmetiky sa každý deliteľ $d|n_1 n_2$ dá jednoznačne vyjadriť v tvare $d = d_1 d_2$, pričom $d_1|n_1$ a $d_2|n_2$ a teda aj $(d_1, d_2) = 1$. Preto

$$(f * g)(n_1 n_2) = \sum_{d|n_1 n_2} f(d)g\Big(\frac{n_1 n_2}{d}\Big) = \sum_{\substack{d_1|n_1 \\ d_2|n_2}} f(d_1 d_2)g\Big(\frac{n_1}{d_1}\frac{n_2}{d_2}\Big) =$$

$$= \sum_{\substack{d_1|n_1 \\ d_2|n_2}} f(d_1)f(d_2)g\Big(\frac{n_1}{d_1}\Big)g\Big(\frac{n_2}{d_2}\Big) = \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1)f(d_2)g\Big(\frac{n_1}{d_1}\Big)g\Big(\frac{n_2}{d_2}\Big) =$$

$$\sum_{d_1|n_1} f(d_1)g\Big(\frac{n_1}{d_1}\Big) \sum_{d_2|n_2} f(d_2)g\Big(\frac{n_2}{d_2}\Big) = (f * g)(n_1)(f * g)(n_2).$$

□

Príklad 113. Súčet deliteľov $\sigma(n) = \sum_{d|n} d$ je multiplikatívna aritmetická funkcia. Preto pre $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ - kánonický rozklad, platí

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

Podobne sa dá odvodiť formula pre $\tau(n)$, ktorá znamená počet delteľov n. Platí

$$\tau(n) = (\alpha_1 + 1) \dots (\alpha_k + 1),$$

pri danom kánonickom rozklade n. ∘

Aritmetická funkcia f sa nazýva **úplne multiplikatívna**, ak $f(n_1 n_2) = f(n_1)f(n_2), n_1, n_2 \in \mathbb{N}$. Dirichletova inverzia k takejto funkcii sa dá nájsť jednoducho.

Veta 39. Ak f je úplne multiplikatívna nenulová aritmetická funkcia, tak jej Dirichletova inverzia je aritmetická funkcia h definovaná $h(1) = 1$, ak $n = p_1 \dots p_k$ je kánonický rozklad, tak

$$h(n) = (-1)^k f(p_1) \dots f(p_k)$$

a $h(n) = 0$, ak existuje $a \in \mathbb{N}, a > 1$ také, že $a^2|n$.

Dôkaz. Výpočtom sa dá overiť, že aritmetická funkcia h je multiplikatívna. Preto podľa vety 38 je aj $f * h$ multiplikatívna. Aby sme dokázali rovnosť $f * h = I$, teda $(f * h)(n) = 0$ pre $n > 1$, stačí túto rovnosť dokázať pre $n = p^\alpha$, p je prvočíslo a $\alpha \geq 1$. V tomto prípade platí

$$(f * h)(p^\alpha) = f(p^\alpha) - f(p)f(p^{\alpha-1}) = 0.$$

□

Dirichletova inverzia k jednotkovej funkcii i, je preto aritmetická funkcia μ daná: $\mu(1) = 1$,

$$\mu(n) = (-1)^k$$

ak $n = p_1 \dots p_k$ je kánonický rozklad, a $\mu(n) = 0$ ak existuje také $a \in \mathbb{N}$, $a > 1$, že $a^2|n$. Táto funkcia sa nazýva **Möbiova funkcia**.

Príklad 114. Möbiova funkcia je multiplikatívna, teda môžeme dokázať

$$\sum_{d|n} \frac{\mu(d)}{d^s} = \prod_{p|n} \Big(1 - \frac{1}{p^s}\Big).$$

∘

Príklad 115. Pomocou toho, že nekonečný rad $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ absolutne konverguje pre $s > 1$, sa dá dokázať

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p \Big(1 - \frac{1}{p^s}\Big).$$

∘

Príklad 116. Ak si uvedomíme, že

$$\sum_{n=1}^{\infty} \frac{I(n)}{n^s} = 1,$$

tak podľa príkladu 111 dostávame pre $s > 1$

$$\Big(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\Big)\Big(\sum_{n=1}^{\infty} \frac{1}{n^s}\Big) = 1.$$

∘

Príklad 117. Dokážeme, že Möbiovu funkciu môžeme vyjadriť v tvare

$$\mu(m) = \sum_{j=1}^{\varphi(m)} e^{2\pi i \frac{r_j}{m}}, \tag{65}$$

kde $r_j, j = 1, \ldots, \varphi(m)$, je redukovaný zvyškový systém modulo m.

Začneme tak, že dokážeme, že aritmetická funkcia definovaná sumou na pravej strane (65), teda

$$f(m) = \sum_{j=1}^{\varphi(m)} e^{2\pi i \frac{r_j}{m}}, m \in \mathbb{N},$$

je multiplikatívna. Predpokladajme, že m_1, m_2 sú nesúdeliteľné prirodzené čísla a $r_j, j = 1, \ldots, \varphi(m_1)$, je redukovaný zvyškový systém modulo m_1, $s_k, k = 1, \ldots, \varphi(m_2)$, je redukovaný zvyškový systém modulo m_2. Podľa príkladu 57 je

$$r_j m_2 + s_k m_1, j = 1, \ldots, \varphi(m_1), k = 1, \ldots, \varphi(m_2)$$

redukovaný zvyškový systém modulo $m_1 m_2$. Preto

$$f(m_1 m_2) = \sum_{j=1}^{\varphi(m_1)} \sum_{k=1}^{\varphi(m_2)} e^{2\pi i \frac{r_j m_2 + s_k m_1}{m_1 m_2}} = \sum_{j=1}^{\varphi(m_1)} \sum_{k=1}^{\varphi(m_2)} e^{2\pi i \Big(\frac{r_j}{m_1} + \frac{s_k}{m_2}\Big)} =$$

$$= \sum_{j=1}^{\varphi(m_1)} e^{2\pi i \frac{r_j}{m_1}} \sum_{k=1}^{\varphi(m_2)} e^{2\pi i \frac{s_k}{m_2}} = f(m_1)f(m_2).$$

Teraz stačí dokázať iba to, že tieto dve aritmetické funkcie nadobúdajú rovnaké hodnoty v mocninách prvočísel. Ak p je prvočíslo, tak

$$f(p) = \sum_{j=1}^{p-1} e^{2\pi i \frac{j}{p}} = \sum_{j=0}^{p-1} e^{2\pi i \frac{j}{p}} - 1 = -1 = \mu(p).$$

Pre prirodzené číslo $\alpha > 1$ platí

$$f(p^\alpha) = \sum_{j=0}^{p^\alpha - 1} e^{2\pi i \frac{j}{p^\alpha}} - \sum_{k=0}^{p^{\alpha-1}-1} e^{2\pi i \frac{pk}{p^\alpha}} = \sum_{j=0}^{p^\alpha - 1} e^{2\pi i \frac{j}{p^\alpha}} - \sum_{k=0}^{p^{\alpha-1}-1} e^{2\pi i \frac{k}{p^{\alpha-1}}} =$$

$$= 0 - 0 = \mu(p^\alpha).$$

∘

Iné použitie Möbiovej funkcie vidíme v nasledujúcej vete, ktorá nesie názov **Möbiova inverzná formula**.

Veta 40. Ak f je aritmetická funkcia a

$$g(n) = \sum_{d|n} f(d),$$

tak

$$f(n) = \sum_{d|n} \mu(d) g\Big(\frac{n}{d}\Big).$$

Dôkaz. Podľa prvej rovnosti platí $g = i * f$. Preto $\mu * g = \mu * (i * f) = (\mu * i) * f = I * f = f$. □

Príklad 118. Dá sa dokázať, že $\sum_{d|n} \varphi(d) = n$. Z toho podľa predošlej vety dostávame $\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$. ∘

Príklad 119. Niektoré aritmetické funkcie sa správajú dosť nepravidelne, keď ich argument prebieha množinu prirodzených čísel v poradí podľa veľkosti. Niekedy sa pomocou Möbiovej inverznej formule dá odhadnúť ich sumačná funkcia. Napríklad

$$\sum_{n\le x} \frac{\varphi(n)}{n} = \sum_{n\le x} \sum_{d|n} \frac{\mu(d)}{d} = \sum_{kd\le x} \frac{\mu(d)}{d} = \sum_{d\le x} \sum_{k\le \frac{x}{d}} \frac{\mu(d)}{d} =$$

$$= \sum_{d\le x} \frac{\mu(d)}{d}\Big[\frac{x}{d}\Big] = x\sum_{d\le x}\frac{\mu(d)}{d^2} + \mathcal{O}\Big(\sum_{d\le x}\frac{\mu(d)}{d}\Big).$$

Z tejto rovnosti sa dá dokázať

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n\le x}\frac{\varphi(n)}{n} = \frac{6}{\pi^2}.$$

Dirichletova konvolúcia nám dáva možnosť spojiť logaritmickú funkciu a prvočísla spôsobom, ktorý ďalej ukáže ako vniesť jasno do rozdelenie prvočísel na rálnej osi. Je to aritmetická funkcia

$$\Lambda = \mu * \ln, \tag{66}$$

(Pričom symbolom ln označujeme klasicky postupnosť $\{\ln n\}$.) Táto aritmetická funkcia sa nazýva **von Mangoltova** funkcia. Z definície vyplýva

$$\sum_{d|n}\Lambda(d) = \ln n,\ n\in\mathbb{N}. \tag{67}$$

Pre prvočíslo p a $j\in\mathbb{N}$ dostávame

$$\Lambda(p^j) = \ln p^j - \ln p^{j-1} = \ln p.$$

Kompletne popisuje hodnoty Λ nasledujúca veta.

Veta 41. Pre von Mangoltovu funkciu platí $\Lambda(n) = \ln p$ v prípade, že n má jediného prvočíselného deliteľa a to p a $\Lambda(n) = 0$ v opačnom prípade.

Dôkaz. Nech f je aritmetická funkcia definovaná $f(n) = \ln p$, ak $n = p^\alpha$ a $f(n) = 0$ inak. Ak máme nejaké prirodzené číslo $n = p_1^{\alpha_1}\dots p_k^{\alpha_k}$ s kánonickým rozkladom, dostávame

$$\sum_{d|n} f(d) = \alpha_1\ln p_1 + \dots + \alpha_k \ln p_k$$

a teda

$$\sum_{d|n} f(d) = \ln n. \tag{68}$$

Dokázali sme $f * i = \ln$ a teda $f = \mu * \ln = \Lambda$. □

Príklad 120. Dá sa dokázať : ak $p_1,\dots,p_k$ sú rôzne prvočísla, tak hodnoty $\ln p_1,\dots,\ln p_k$ sú lineárne nezávislé nad poľom racionálnych čísel. ∘

Príklad 121. Dôležitá bude nasledujúca rovnosť

$$(\mu * \Lambda)(n) = -\mu(n) \ln n \tag{69}$$

pre $n \in \mathbb{N}$. Táto rovnosť vyplýva z Mobiovej inverznej formule, ak si vyjadríme

$$\Lambda(n) = \sum_{d|n} \mu(d) \ln\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \ln n - \sum_{d|n} \mu(d) \ln d =$$

$$= \ln n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \ln d = -\sum_{d|n} \mu(d) \ln d.$$

6 Parciálna sumácia

Veta 42. Nech f, g sú reálne funkcie definované na intervale (x_0, x_1), $x_0 \geq 0$ a funkcia f tam má spojitú deriváciu a $g(x) = g([x])$. Potom pre každé prirodzené čísla $k_1 < k_2$,$k_1 \geq x_0 + 1$, platí

$$\sum_{n=k_1}^{k_2} f(n)(g(n) - g(n-1)) = f(k_2)g(k_2) - f(k_1)g(k_1) + \int_{k_1}^{k_2} g(t)f'(t)dt.$$

Dôkaz. Začneme upravovať ľavú stranu

$$\sum_{n=k_1}^{k_2} f(n)(g(n) - g(n-1)) = \sum_{n=k_1}^{k_2} f(n)g(n) - \sum_{n=k_1}^{k_2} f(n)g(n-1) =$$

$$= \sum_{n=k_1}^{k_2} f(n)g(n) - \sum_{n=k_1-1}^{k_2-1} f(n+1)g(n) =$$

$$= \sum_{n=k_1}^{k_2-1} g(n)(f(n) - f(n+1)) + f(k_2)g(k_2) - f(k_1)g(k_2).$$

Z predpokladov vyplýva

$$g(n)(f(n) - f(n+1)) = \int_n^{n+1} g(t)f'(t)dt.$$

Z toho po dosadení vyplýva tvrdenie. □

Príklad 122. Ukážeme použitie predošlej vety na dôkaz

$$\sum_{p\le N}\frac{1}{p}=\ln\ln N+C_1+\mathcal{O}\Big(\frac{1}{\ln N}\Big). \tag{70}$$

Pripomenieme si odhad z príkladu 98. Definujme si funkciu

$$\gamma(x)=\sum_{p\le N}\frac{\ln p}{p}.$$

Podľa spomínaného príkladu platí

$$\gamma(N)=\ln N+c(N), \tag{71}$$

pričom $c(N)=\mathcal{O}(1)$. Definujeme si funkciu $\delta(n)=\frac{\ln p}{p}$, ak $n=p$ je prvočíslo a $\delta(n)=0$ v inom prípade. Potom môžeme vyjadriť

$$\sum_{p\le N}\frac{1}{p}=\sum_{n\le N}\frac{\delta(n)}{\ln n}.$$

Preto

$$\sum_{p\le N}\frac{1}{p}=\sum_{n\le N}\frac{\gamma(n)-\gamma(n-1)}{\ln n}=\sum_{n\le N}\frac{\gamma(n)}{\ln n}-\sum_{n\le N}\frac{\gamma(n-1)}{\ln n}=$$

$$\frac{\gamma(N)}{\ln N}+\sum_{n\le N-1}\frac{\gamma(n)}{\ln n}-\sum_{n\le N-1}\frac{\gamma(n)}{\ln(n+1)}=$$

$$=\frac{\gamma(N)}{\ln N}+\sum_{n\le N-1}\gamma(n)\Big(\frac{1}{\ln n}-\frac{1}{\ln(n+1)}\Big).$$

Teraz môžeme použiť vetu 42. Derivovaním dostávame $(\frac{1}{\ln x})'=\frac{-1}{x\ln^2 x}$. Z tejto vety vyplýva

$$\sum_{n\le N-1}\gamma(n)\Big(\frac{1}{\ln n}-\frac{1}{\ln(n+1)}\Big)=$$

$$=\sum_{n\le N-1}\gamma(n)\Big(\frac{1}{\ln n}-\frac{1}{\ln(n+1)}\Big)=\int_2^N\frac{\gamma(t)dt}{t\ln^2 t}.$$

Ak dosadíme za γ podľa (71), dostávame

$$\sum_{n\le N-1}\gamma(n)\Big(\frac{1}{\ln n}-\frac{1}{\ln(n+1)}\Big)=\int_2^N\frac{dt}{t\ln t}+\int_2^N\frac{c(t)dt}{t\ln^2 t}.$$

Prvý integrál na pravej strane sa rovná $\ln\ln N - \ln\ln 2$. Nevlastný integrál $\int_2^\infty \frac{dt}{t\ln^2 t}$ absolútne konverguje a teda aj nevlastný integrál $\int_2^\infty \frac{c(t)dt}{t\ln^2 t}$ konverguje. Označme

$$\kappa = \int_2^\infty \frac{c(t)dt}{t\ln^2 t}.$$

Potom

$$\int_2^N \frac{c(t)dt}{t\ln^2 t} = \kappa - \int_N^\infty \frac{c(t)dt}{t\ln^2 t} = \kappa + \mathcal{O}\Big(\frac{1}{\ln N}\Big).$$

Po dosadení do príslušných rovností dostávame (70).

7 Čebyševove funkcie

Definujeme si teraz funkcie

$$\psi(x) = \sum_{n\le x} \Lambda(n) \tag{72}$$

$$\theta(x) = \sum_{p\le x} \ln p. \tag{73}$$

Tieto funkcie sa nazývajú **Čebyševove funkcie**. Ich význam spočíva v tom, že sa pomocou nich dá vhodne vyjadriť prvočíselná funkcia. S funkciou θ sme sa už viackrát stretli, ale ešte nebolo potrebné ju definovať.

Funkciu θ si môžeme vyjadriť

$$\theta(N) = \sum_{n=2}^{N} (\pi(n) - \pi(n-1))\ln n.$$

A teda podľa vety 42 dostávame

$$\theta(N) = \ln N\pi(N) + \int_2^N \frac{\pi(t)}{t}dt. \tag{74}$$

Z druhej strany platí

$$\pi(N) = \sum_{n\le N} \frac{\theta(n) - \theta(n-1)}{\ln n}.$$

Z vety 42 dostávame

$$\pi(N) = \frac{\theta(N)}{\ln N} - \int_2^N \frac{\theta(t)}{t\ln t}dt. \tag{75}$$

Medzi funkciami ψ a θ môžeme odvodiť vzťah nasledujúcim spôsobom

$$\psi(x) = \theta(x) + \sum_{k\geq 2, p^k \leq x} \ln p.$$

Druhý ščítanec rozpíšeme

$$\sum_{k\geq 2, p^k \leq x} \ln p = \sum_{2\leq k\leq \frac{\ln x}{\ln 2}} \sum_{p\leq \sqrt[k]{x}} \ln p.$$

Všetky ščítance v druhej sume sú zhora ohraničené prvým ščítancom a teda

$$\sum_{\substack{k\geq 2\\ p^k\leq x}} \ln p \leq \frac{\ln x}{\ln 2} \sum_{p\leq \sqrt{x}} \ln p \leq \frac{\ln x}{\ln 2} \ln \sqrt{x}\pi(\sqrt{x}) \leq c_2\sqrt{x}\ln x.$$

Preto

$$\psi(x) = \theta(x) + \mathcal{O}(\sqrt{x}\ln x). \tag{76}$$

Príklad 123. Dá sa dokázať, že pre nerastúcu nezápornú funkciu f definovanú na $(1,\infty)$ takú, že $\lim_{x\to\infty} f(x) = 0$, platí

$$\lim_{N\to\infty} \frac{1}{N}\int_1^N f(t)dt = 0.$$

∘

Z tohoto príkladu a rovností (74), (75) a (76) vyplýva

Veta 43. Nasledujúce rovnosti sú ekvivalentné

$$\lim_{N\to\infty} \frac{\pi(N)\ln N}{N} = 1,$$

$$\lim_{N\to\infty} \frac{\psi(N)}{N} = 1,$$

$$\lim_{N\to\infty} \frac{\theta(N)}{N} = 1.$$

Príklad 124. Označme symbolom $[1,\ldots,N]$ najmenší spoločný násobok čísel $1,\ldots,N$, $N\in\mathbb{N}$. Z predošlej vety vyplýva, že rovnosť

$$\lim_{N\to\infty} \frac{\pi(N)\ln N}{N} = 1$$

je ekvivalentná rovnosti

$$\lim_{N\to\infty} \sqrt[N]{[1,\ldots,N]} = e.$$

Najmenší spoločný násobok si totiž môžeme vyjadriť

$$[1,\ldots,N] = \prod_{p\le N} p^{\left[\frac{\ln N}{\ln p}\right]}.$$

Preto

$$\ln \sqrt[N]{[1,\ldots,N]} = \frac{1}{N}\sum_{p\le N}\Big[\frac{\ln N}{\ln p}\Big]\ln p = \frac{\psi(N)}{N}.$$

∘

Príklad 125. Z rovnosti (69) dostávame

$$\sum_{n\le x}\mu(n)\ln n = -\sum_{n\le x}\sum_{d|n}\mu(d)\Lambda\Big(\frac{n}{d}\Big) = -\sum_{kd\le x}\mu(d)\Lambda(k) =$$

$$-\sum_{d\le x}\mu(d)\sum_{k\le\frac{x}{d}}\Lambda(k).$$

To znamená

$$\sum_{n\le x}\mu(n)\ln n = -\sum_{d\le x}\mu(d)\psi\Big(\frac{x}{d}\Big). \tag{77}$$

∘

Veta 44. Existujú kladné konštanty c_3, c_2, pre ktoré

$$c_3 x \le \theta(x) \le \psi(x) \le c_4 x,$$

pre $x \ge 2$.

Dôkaz. Prvá nerovnosť vyplýva z príkladu 49. Druhú nerovnosť dostaneme, keď si uvedomíme podľa vety 41, že každý šťítanec, ktorý vystupuje v sume pre θ, vystupuje aj v sume pre ψ.

Funkciu ψ si môžeme vyjadriť v tvare

$$\psi(x) = \sum_{p^j\le x}\ln p = \sum_{p\le x}\sum_{j=1}^{[\frac{\ln x}{\ln p}]}\ln p = \sum_{p\le x}\Big[\frac{\ln x}{\ln p}\Big]\ln p. \tag{78}$$

Z tejto rovnosti dostávame

$$\psi(x) \leq \sum_{p \leq x} \frac{\ln x}{\ln p} \ln p = \pi(x) \ln x.$$

Preto, keď použijeme horný odhad prvočíselnej funkcie z vety 33, dostávame

$$\psi(x) \leq c_2 x.$$

□

Príklad 126. Dokážeme odhad

$$\sum_{p \leq N} \ln^2 p = \theta(N) \ln N + \mathcal{O}(N).$$

Sumu na ľavej strane si môžeme vyjadriť

$$\sum_{n \leq N} (\theta(n) - \theta(n-1)) \ln n = \sum_{n \leq N} \theta(n) \ln n - \sum_{n \leq N} \theta(n-1) \ln n =$$

$$= \ln N \theta(N) + \sum_{n \leq N-1} \theta(n) \ln n - \sum_{n \leq N} \theta(n-1) \ln n$$

$$\theta(N) \ln N + \sum_{n \leq N-1} \theta(n) \ln n - \sum_{n \leq N-1} \theta(n)) \ln(n+1)$$

$$\theta(N) \ln N + \int_1^N \frac{\theta(t)}{t} dt = \ln N \theta(N) + \mathcal{O}(N).$$

∘

Príklad 127. Podľa rovnosti (68) dostávame

$$\sum_{n \leq x} \ln n = \sum_{n \leq x} \sum_{d|n} \Lambda(d) = \sum_{kd \leq x} \Lambda(d) = \sum_{d \leq x} \sum_{k \leq \frac{x}{d}} \Lambda(d) =$$

$$= \sum_{d \leq x} \Lambda(d) \sum_{k \leq \frac{x}{d}} 1 = \sum_{d \leq x} \Lambda(d) \left[\frac{x}{d}\right] = x \sum_{d \leq x} \frac{\Lambda(d)}{d} + \mathcal{O}(\psi(x)) =$$

$$= x \sum_{d \leq x} \frac{\Lambda(d)}{d} + \mathcal{O}(x).$$

Z príkladu 54 teda vyplýva

$$x \ln x - x + \mathcal{O}(\ln x) = x \sum_{d \leq x} \frac{\Lambda(d)}{d} + \mathcal{O}(x).$$

Po vydelení x -om a istých úpravách dostávame

$$\sum_{d\le x}\frac{\Lambda(d)}{d}=\ln x+\mathcal{O}(1). \tag{79}$$

∘

Veta 45. Ak F a f sú reálne funkcie definované na intervale $[1,\infty)$, tak nasledujúce rovnosti sú ekvivalentné

$$F(x)=\sum_{n\le x}f\Big(\frac{x}{n}\Big),$$

$$f(x)=\sum_{d\le x}\mu(d)F\Big(\frac{x}{d}\Big).$$

Dôkaz. Predpokladajme, že platí prvá rovnosť. Potom

$$\sum_{d\le x}\mu(d)F\Big(\frac{x}{d}\Big)=\sum_{d\le x}\mu(d)\sum_{n\le\frac{x}{d}}f\Big(\frac{x}{dn}\Big)=\sum_{nd\le x}\mu(d)f\Big(\frac{x}{dn}\Big).$$

Ak označíme $m=nd$ v poslednej sume, tak z predošlého vyplývau

$$\sum_{d\le x}\mu(d)F\Big(\frac{x}{d}\Big)=\sum_{\substack{m\le x\\ d|m}}\mu(d)f\Big(\frac{x}{m}\Big)=\sum_{m\le x}f\Big(\frac{x}{m}\Big)\sum_{d|m}\mu(d)=f(x).$$

Opačnú implikáciu dokážeme rovnako. □

Príklad 128. Pre $x\ge 1$ platí

$$\sum_{n\le x}1=[x].$$

Podľa predošlej vety potom dostávame

$$\sum_{d\le x}\Big[\frac{x}{d}\Big]\mu(d)=1.$$

Z tejto rovnosti vyplýva

$$\sum_{d\le x}\frac{x}{d}\mu(d)+\mathcal{O}\Big(\sum_{d\le x}\mu(d)\Big)=1. \tag{80}$$

Ak si uvedomíme, že $\sum_{d\le x}\mu(d)=\mathcal{O}(x)$, tak dostávame

$$\sum_{d\le x}\frac{\mu(d)}{d}=\mathcal{O}(1). \tag{81}$$

∘

Zaujímavá je súvislosť sumačnej funkcie $M(x) = \sum_{n \leq x} \mu(x)$ s nekonečným radom $\sum_{n=1}^{\infty} \frac{\mu(n)}{n}$.

Príklad 129. Dá sa dokázať, že

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0$$

práve vtedy, keď

$$\lim_{x \to \infty} \frac{M(x)}{x} = 0.$$

Ak platí druhá rovnosť, tak prvá rovnosť vyplýva z (80). Označme teraz $m(x) = \sum_{n \leq x} \frac{\mu(n)}{n}$. Potom si môžeme vyjadriť

$$M(N) = \sum_{n \leq N} n(m(n) - m(n-1)), N = 2, 3, \ldots$$

Preto

$$M(N) = \sum_{n \leq N} nm(n) - \sum_{n \leq N} nm(n-1)) = \sum_{n \leq N} nm(n) - \sum_{n \leq N-1} (n+1)m(n) =$$

$$= Nm(N) - \sum_{n \leq N-1} m(n).$$

Ak platí prvá rovnosť, tak $\lim_{N \to \infty} m(N) = 0$ a teda podľa vyjadrenia $M(N)$ pomocou predošlých úprav platí aj druhá rovnosť. ∘

8 Prvočísla vo zvyškových triedach

Už sme dokázali, že existuje nekonečne veľa prvočísel. Myšlienka, ktorá pochádza od Euklida, sa dá použiť aj na dôkaz toho, že existuje nekonečne veľa prvočísel v tvare $4k+3, 6k+5, 3k+2$. Dôležité tam bolo to, že napríklad po delení 4 môže mať nepárne prvočíslo zvyšok iba 1 alebo 3. Teraz sa budeme zaoberať všeobecným prípadom. Je zrejmé, že ak $km + \ell$ je prvočíslo rôzne od ℓ, tak $(m, \ell) = 1$.

Budeme dokazovať nasledujúce tvrdenie:

Veta 46. Ak m, ℓ sú prirodzené čísla a $(m, \ell) = 1$ tak,

$$\sum_{\substack{p \leq x \\ p \equiv \ell}} \frac{\ln p}{p} = \frac{1}{\varphi(m)} \ln x + \mathcal{O}(1)$$

a

$$\sum_{\substack{p\le x\\ p\equiv \ell}} \frac{1}{p} = \frac{1}{\varphi(m)} \ln\ln x + \mathcal{O}(1).$$

Ak platí prvá rovnosť, tak druhú rovnosť odvodíme analogickým postupom ako v Príklade 122.

Pre ďalšie úvahy bude užitočné spoznať štruktúru redukovaného zvyškového systému modulo m. Táto štruktúra je najjednoduchšia v prípade $m = 2, 4, p^\alpha$, kde p nepárne prvočíslo. V týchto prípadoch existuje primitívny koreň. To sme dokázali v predošlom texte. Tento fakt využijeme na dôkaz nasledujúcej vety, ktorá nám poskytne istý celkový pohľad.

Veta 47. Nech $m \in \mathbb{N}$, $m > 1, 8 \nmid m$ **a** $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$**, je kánonický rozklad** m**. Potom existujú prirodzené čísla** $g_1, \dots, g_k$**, že pre každé** $a \in \mathbb{N}, (a, m) = 1$ **existujú jednoznačne určené** $j_1, \dots, j_k$**,** $0 \le j_s < \varphi(p_s^{\alpha_s})$**,** $s = 1, \dots, k$ **také, že**

$$a \equiv g_1^{j_1} \dots g_k^{j_k} \pmod{m}. \tag{82}$$

Rád prvku g_s **modulo** m **je** $\varphi(p_s^{\alpha_s})$.

Dôkaz. Čínska veta o zvyškoch nám umožňuje definovať zobrazenie

$$\Psi : \mathbb{Z}^*_{p_1^{\alpha_1}} \times \dots \times \mathbb{Z}^*_{p_k^{\alpha_k}} \to \mathbb{Z}^*_m$$
$$\Psi((a_1, \dots, a_k)) = a, \tag{83}$$

kde $a \in \mathbb{Z}^*_m$ je číslo, ktoré vyhovuje kongruenciám

$$a \equiv a_s \pmod{p_i^{\alpha_s}},\ s = 1, \dots, k.$$

Toto zobrazenie je izomorfizmus grúp. Označme $\tilde{g}_s, s = 1, \dots, k$ primitívny koreň modulo $p_s^{\alpha_s}$. Potom číslo a dané rovnosťou (83) sa dá vyjadriť

$$\Psi((\tilde{g}_1^{j_1}, \dots, \tilde{g}_k^{j_k})) = a. \tag{84}$$

Ak označíme

$$g_s = \Psi((1 \dots \tilde{g}_s \dots 1)), \tag{85}$$

(na s tom mieste je $\tilde{g}_s$, ostatné sú 1), tak z rovnosti (84) dostávame

$$a = g_1^{j_1} \dots g_k^{j_k}.$$

Nakoniec z rovnosti (85) vyplýva,

$$g_s^{\varphi(p_s^{\alpha_s})} = \Psi((1 \dots \tilde{g}_s^{\varphi(p_s^{\alpha_s})} \dots 1)) = \Psi((1 \dots 1 \dots 1)) = 1.$$

□

Príklad 130. Uvažujme zobrazenie Ψ zostrojené v predošlom dôkaze

$$\Psi : \mathbb{Z}_3^* \times \mathbb{Z}_5^* \to \mathbb{Z}_{15}^*.$$

Primitívny koreň modulo 3 je 2 a primitívny koreň modulo 5 je 3. V tomto prípade dostáveme $\Psi((2,1)) = 11$ a $\Psi((1,3)) = 13$.

V prípade $2^\alpha, \alpha \geq 3$ neexistuje primitívny koreň. Pre nepárne a v tomto prípade platí ,

$$a \equiv (2^\alpha - 1)^{\ell_1} 5^{\ell_2} \pmod{2^\alpha}$$

pričom $\ell_1 \in \{0,1\}, 0 \leq \ell_2 \leq 2^\alpha - 2$.

Predchádzajúcim postupom sa preto dá dokázať:

Veta 48. Ak vo Vete 47 $m = 2^\alpha p_1^{\alpha_1} \dots p_k^{\alpha_k}$**, je kánonický rozklad** m**, tak existujú prirodzené čísla** $g_1, \dots, g_k$**, že pre každé** $a \in \mathbb{N}, (a,m) = 1$ **existujú jednoznačne určené** $\ell_1 \in \{0,1\}, 0 \leq \ell_2 \leq 2^{\alpha-2}$**,** $j_1, \dots, j_k$**,** $0 \leq j_i < \varphi(p_i^{\alpha_i})$**,** $i = 1, \dots, k$ **také, že**

$$a \equiv h_1^{\ell_1} h_2^{\ell_2} g_1^{j_1} \dots g_k^{j_k} \pmod{m}, \tag{86}$$

kde $h_1 = \Psi((2^n - 1, 1, \dots, 1)$ a $h_2 = \Psi((1, 5, \dots, 1)$.

8.1 Dirichletove charaktery

V tejto časti vytvoríme také zobrazenia, ktoré umožnia oddeľovať sčítance v sumách podľa zvyškových tried. Budeme ich nazývať charaktery.

Nech $m \in \mathbb{N}$ a $m > 1$. Zobrazenie $\mathcal{X} : \mathbb{N} \to \mathcal{C}$ sa nazýva **Dirichletov charakter modulo** m ak spĺňa nasledujúce podmienky:
1) $\mathcal{X}$ je periodické modulo m, teda $a_1 \equiv a_2 \pmod{m} \Rightarrow \mathcal{X}(a_1) = \mathcal{X}(a_2)$.
2) Pre každé $a \in \mathbb{N}$ **platí** $\mathcal{X}(a) \neq 0$ **práve vtedy, keď** $(m,a) = 1$**.**
3) Pre každé $a, b \in \mathbb{N}$ **platí** $\mathcal{X}(ab) = \mathcal{X}(a)\mathcal{X}(b)$**.**
Skrátene budeme hovoriť "charakter".

Najjednoduchším príkladom charakteru modulo m je charakter $\mathcal{X}_0$, pre ktorý platí $\mathcal{X}_0(a) = 1$ ak $(a,m) = 1$ a $\mathcal{X}_0(a) = 0$, ak a, m sú súdeliteľné. Tento charakter sa nazýva **hlavný charakter**.

Z vlastností 2) a 3) vyplýva $\mathcal{X}(1) = 1$. Ak $a \in \mathbb{N}$ a $(a,m) = 1$, tak podľa Eulerovej vety platí $a^{\varphi(m)} \equiv 1 \pmod{m}$. Z vlastnosti 3) teda vyplýva

$$\mathcal{X}(a)^{\varphi(m)} = \mathcal{X}(a^{\varphi(m)}) = 1.$$

Dokázali sme teda, že v prípade $(a,m) = 1$ je hodnota $\mathcal{X}(a)$ koreňom binomickej rovnice

$$x^{\varphi(m)} - 1 = 0. \tag{87}$$

To znamená, že

$$\mathcal{X}(a) = e^{\frac{2\pi ik}{\varphi(m)}} \tag{88}$$

pre nejaké $k = 0, \ldots, \varphi(m) - 1$, ktoré závisí od a. Z periodicity, teda z vlastnosti 1), vyplýva, že charakter je jednoznačne daný hodnotami na redukovanom zvyškovom systéme modulo m. Ak pritom zoberieme do úvahy, že rovnica (88) má $\varphi(m)$ koreňov, vidíme, že existuje iba konečne veľa charakterov modulo m. Množinu všetkých charakterov modulo m budeme označovať symbolom $\mathbf{X}(m)$.

Na tomto mieste uvedieme rovnosť, ktorá nám umožní oddelovať sčítance v sume podľa zvyškových tried. Symbolom $n \equiv \ell$ myslíme kongruenciu modulo m.

Pre každú aritmetickú funkciu f platí

$$\sum_{\substack{n \leq x \\ n \equiv \ell}} f(n) = \frac{1}{\varphi(m)} \sum_{\mathcal{X}} \overline{\mathcal{X}(\ell)} \sum_{n \leq x} \mathcal{X}(n) f(n). \tag{89}$$

Všetky ďalšie úvahy v tejto časti budú viesť k dôkazu tejto rovnosti.

Veta 49. Pre každé $m \in \mathbb{N}, m > 1$ platí

$$|\mathbf{X}(m)| = \varphi(m) \tag{90}$$

a pre každé $a \in \mathbb{N}$ platí

$$a \not\equiv 1 \pmod{m} \Rightarrow \exists \mathcal{X} \in \mathbf{X}(m); \mathcal{X}(a) \neq 1. \tag{91}$$

Dôkaz. Budeme predpokladať, že m má tvar ako vo Vete 47. V takom prípade pre dané a platí

$$\mathcal{X}(a) = \mathcal{X}(g_1)^{j_1} \cdot \ldots \cdot \mathcal{X}(g_k)^{j_k}.$$

To znamená, že charakter $\mathcal{X}$ je jednoznačne určený hodnotami $\mathcal{X}(g_s), s = 1, \ldots, k$. Rád prvku g_s je $\varphi(p_s^{\alpha_s})$. Z toho vyplýva, že hodnota $\mathcal{X}(g_s)$ je koreňom binomickej rovnice

$$x^{\varphi(p_s^{\alpha_s})} = 1.$$

To znamená, že

$$\mathcal{X}(g_s) = e^{\frac{2\pi i \ell_s}{\varphi(p_s^{\alpha_s})}}$$

pričom $0 \leq j_s < \varphi(p_s^{\alpha_s})$. Teda, ak a je v tvare ako vo Vete 47, tak

$$\mathcal{X}(a) = e^{\frac{2\pi i \ell_1 j_1}{\varphi(p_1^{\alpha_1})}} \cdot \ldots \cdot e^{\frac{2\pi i \ell_k j_k}{\varphi(p_k^{\alpha_k})}}.$$

Toto vyjadrenie je jednoznačné a preto existuje práve $\varphi(p_1^{\alpha_1})\dots\varphi(p_k^{\alpha_k}) = \varphi(m)$ charakterov modulo m.

Ak $a \not\equiv 1 \pmod m$, tak existuje s, pre ktoré $a \not\equiv 1 \pmod{p_s^{\alpha_s}}$. Z toho vyplýva

$$a \equiv g_s^{\ell} \pmod{p_s^{\alpha_s}},$$

pričom $0 < \ell < \varphi p_s^{\alpha^s}$. Teraz môžeme definovať charakter $\mathcal{X}$ tak, že $\mathcal{X}(g_j) = 1$, ak $j \neq s$ a $\mathcal{X}(g_s) = e^{\frac{2\pi i}{\varphi(p_s^{\alpha^s})}}$. V tomto prípade platí

$$\mathcal{X}(a) = e^{\frac{2\pi i\ell}{\varphi(p_s^{\alpha^s})}} \neq 1.$$

□

Množina $\mathbf{X}(m)$ tvorí grupu vzhľadom na násobenie prirodzene definované pomocou násobenia komplexných čísel. Teda pre $\mathcal{X}_1, \mathcal{X}_2 \in \mathbf{X}(m)$ definujeme súčin charakterov

$$(\mathcal{X}_1\mathcal{X}_2)(a) = \mathcal{X}_1(a)\mathcal{X}_2(a),$$

pre každé $a \in \mathbb{Z}_m$. Neutrálnym prvkom v tejto grupe je hlavný charakter $\mathcal{X}_0$. Hodnoty charakterov sú korene rovnice (87). To znamená, že pre každé $a \in \mathbb{Z}_m^*$ platí $|\mathcal{X}(a)| = 1$. Inak povedané $\mathcal{X}(a)\overline{\mathcal{X}(a)} = 1$. Teda vidíme, že inverzným prvkom k danému charakteru $\mathcal{X}$ je charakter komplexne združený, teda $\mathcal{X}^{-1} = \overline{\mathcal{X}}$, kde

$$\overline{\mathcal{X}}(a) = \overline{\mathcal{X}(a)}.$$

Táto grupa sa nazýva **grupa charakterov** modulo m.

Veta 50. Ak $a \equiv 1 \pmod m$**, tak**

$$\sum_{\mathcal{X}} \mathcal{X}(a) = \varphi(m). \tag{92}$$

Ak $a \not\equiv 1 \pmod m$**, tak**

$$\sum_{\mathcal{X}} \mathcal{X}(a) = 0. \tag{93}$$

Dôkaz. Prvá rovnosť vyplýva z prvej časti Vety 49 a z toho, že v tomto prípade platí $\mathcal{X}(a) = 1$ pre každý charakter $\mathcal{X} \in \mathbf{X}(m)$.

Ak $a \not\equiv 1 \pmod m$, tak podľa druhej časti Vety 49 existuje istý charakter $\mathcal{X}_1 \in \mathbf{X}(m)$ taký, že $\mathcal{X}_1(a) \neq 1$. Potom

$$\mathcal{X}_1(a)\sum_{\mathcal{X}} \mathcal{X}(a) = \sum_{\mathcal{X}} \mathcal{X}_1(a)\mathcal{X}(a) = \sum_{\mathcal{X}} (\mathcal{X}_1\mathcal{X})(a).$$

Ak $\mathcal{X}$ prebieha celú množinu $\mathbf{X}(m)$, tak aj $\mathcal{X}\mathcal{X}_1$ prebieha celú túto množinu. Preto z predošlej rovnosti dostávame

$$\mathcal{X}_1(a)\sum_{\mathcal{X}}\mathcal{X}(a)=\sum_{\mathcal{X}}\mathcal{X}(a).$$

To znamená

$$(\mathcal{X}_1(a)-1)\sum_{\mathcal{X}}\mathcal{X}(a)=0.$$

Ako sme už spomínali, $\mathcal{X}_1(a)\neq 1$ a teda posledná rovnosť môže platiť iba v prípade, že platí rovnosť (93). □

Už sa blížime k spomínanému dôkazu rovnosti (89). Ak označíme a^{-1} inverzný prvok k a mo- dulo m pre $(a,m)=1$, tak $a^{-1}a\equiv 1 \pmod m$. Preto pre $\mathcal{X}\in\mathbf{X}(m)$ platí $\mathcal{X}(a^{-1}a)=1$. Po úprave dostáveme $\mathcal{X}(a^{-1})\mathcal{X}(a)=1$. To znamená

$$\mathcal{X}(a^{-1})=\overline{\mathcal{X}(a)}. \tag{94}$$

Veta 51. Ak $m\in\mathbb{N}$**, tak pre každé** $k,\ell\in\mathbb{N},(k,m)=1,(\ell,m)=1$**, platí**

$$k\equiv\ell \pmod m \Rightarrow \sum_{\mathcal{X}}\mathcal{X}(k)\overline{\mathcal{X}(\ell)}=\varphi(m)$$

a

$$k\not\equiv\ell \pmod m \Rightarrow \sum_{\mathcal{X}}\mathcal{X}(k)\overline{\mathcal{X}(\ell)}=0$$

Dôkaz. Budeme postupovať podľa (94). Ak označíme symbolom ℓ^{-1} inverzný prvok k ℓ modulo m, tak dostávame

$$\mathcal{X}(k)\overline{\mathcal{X}(\ell)}=\mathcal{X}^{-1}(\ell)\mathcal{X}(k)=\mathcal{X}(\ell^{-1})\mathcal{X}(k)=\mathcal{X}(\ell^{-1}k).$$

Teda ak $k\equiv\ell \pmod m$, tak $k\ell^{-1}\equiv 1 \pmod m$. Z toho vyplýva podľa prvej časti predošlej vety prvá rovnosť. Podobne ak $k\not\equiv\ell \pmod m$, tak dostávame druhú časť vety. □

Ak budeme postupne upravovať pomocou tejto vety pravú stranu rovnosti (89), dostaneme ľavú stranu.

8.2 Použitie von Mangoldtovej funkcie

Budeme potrebovať takú aritmetickú funkciu, ktorá odlišuje prvočísla a zároveň poznáme jej vlastnosti. Jednou z takých funkcií je von Mangoltova funkcia Λ. Ak ju dosadíme do predošlého príkladu, dostávame rovnosť

$$\frac{1}{\varphi(m)}\sum_{\substack{n\leq x\\ n\equiv\ell}}\frac{\Lambda(n)}{n}=\sum_{\mathcal{X}}\overline{\mathcal{X}(\ell)}\sum_{n\leq x}\frac{\Lambda(n)\mathcal{X}(n)}{n}.$$

Túto rovnosť môžeme vyjadriť v tvare

$$\frac{1}{\varphi(m)}\sum_{\substack{n\le x\\ n\equiv\ell}}\frac{\Lambda(n)}{n}=\sum_{n\le x}\frac{\mathcal{X}_0(n)\Lambda(n)}{n}+\sum_{\mathcal{X}\neq\mathcal{X}_0}\overline{\mathcal{X}(\ell)}\sum_{n\le x}\frac{\Lambda(n)\mathcal{X}(n)}{n}. \tag{95}$$

Činiteľ $\mathcal{X}_0(\ell)$ je rovný 1 a teda ho pri prvej sume môžeme vynechať. Teraz budeme upravovať sumy v tejto rovnosti tak aby vniesli do veci čo najviac jasno. Pre výraz na ľavej strane platí

Lema 1.

$$\sum_{\substack{n\le x\\ n\equiv\ell}}\frac{\Lambda(n)}{n}=\sum_{\substack{p\le x\\ p\equiv\ell}}\frac{\ln p}{p}+\mathcal{O}(1).$$

Dôkaz.

$$\sum_{\substack{n\le x\\ n\equiv\ell}}\frac{\Lambda(n)}{n}=\sum_{\substack{p\le x\\ p\equiv\ell}}\frac{\ln p}{p}+\mathcal{O}\Big(\sum_{\substack{p^\alpha\le x\\ 2\le\alpha}}\frac{\ln p}{p}\Big)=$$

$$=\sum_{\substack{p\le x\\ p\equiv\ell}}\frac{\ln p}{p}+\mathcal{O}\Big(\sum_{p\le x}\frac{\ln p}{p^2}\sum_{\alpha=0}^{\infty}\frac{1}{p^\alpha}\Big)=\sum_{\substack{p\le x\\ p\equiv\ell}}\frac{\ln p}{p}+\mathcal{O}(1).$$

□

Prvú sumu napravo v (95) si môžeme vyjadriť

$$\sum_{n\le x}\frac{\mathcal{X}_0(n)\Lambda(n)}{n}=\sum_{n\le x}\frac{\Lambda(n)}{n}-\sum_{\substack{n\le x\\ (n,m)>1}}\frac{\Lambda(n)}{n}. \tag{96}$$

Ak zoberieme do úvahy vyjadrenie funkcie Λ dostávame, že menšiteľ v poslednej rovnosti neprevyšuje hodnotu

$$\sum_{p\mid m}\ln p\Big(\frac{1}{p}+\frac{1}{p^2}+\dots\Big)=\mathcal{O}(1).$$

Dosadením do (96) vidíme, že

$$\sum_{n\le x}\frac{\mathcal{X}_0(n)\Lambda(n)}{n}=\sum_{n\le x}\frac{\Lambda(n)}{n}+\mathcal{O}(1).$$

Lema 2. Pre $x>1$ platí

$$\sum_{n\le x}\frac{\Lambda(n)}{n}=\ln x+\mathcal{O}(1).$$

Dôkaz. Vieme, že platí

$$\sum_{n\leq x} \ln n = x\ln x + \mathcal{O}(\ln x).$$

Ak si uvedomíme definíciu funkcie Λ, tak predošlú rovnosť môžeme vyjadriť

$$\sum_{n\leq x}\sum_{d|n} \Lambda(d) = x\ln x + \mathcal{O}(\ln x).$$

To znamená

$$x\ln x + \mathcal{O}(\ln x) = \sum_{kd\leq x} \Lambda(d) = \sum_{d\leq x} \Lambda(d) \sum_{k\leq \frac{x}{d}} 1 = \sum_{d\leq x} \Lambda(d)\Big[\frac{x}{d}\Big].$$

Preto

$$x\sum_{d\leq x} \frac{\Lambda(d)}{d} + \mathcal{O}\Big(\sum_{d\leq x}\Lambda(d)\Big) = x\ln x + \mathcal{O}(\ln x). \tag{97}$$

Keď si uvedomíme, že $\psi(x) = \sum_{d\leq x}\Lambda(d) = \mathcal{O}(x)$ a vydelíme rovnosť (97) x - om dostávame tvrdenie. □

Rovnosť (95) sa nám týmto spôsobom podarilo upraviť takto

$$\frac{1}{\varphi(m)} \sum_{\substack{p\leq x\\ n\equiv \ell}} \frac{\ln p}{p} = \ln x + \sum_{\mathcal{X}\neq\mathcal{X}_\prime} \overline{\mathcal{X}(\ell)} \sum_{n\leq x} \frac{\Lambda(n)\mathcal{X}(n)}{n} + \mathcal{O}(1). \tag{98}$$

Ak sa nám podarí dokázať, že hodnoty $\sum_{n\leq x} \frac{\Lambda(n)\mathcal{X}(n)}{n}$ sú pre $\mathcal{X}\neq\mathcal{X}_0$ ohraničéné, tak sme dokázali prvú rovnosť z Vety 46.

8.3 Dirichletove L rady

Aby sme dokázali ohraničenosť hore spomínaných veličín využijeme dva tipy nekonečných radov. Budeme vychádzať z toho, že konvergujú.

Veta 52. Ak $r_1,\ldots,r_m$ je úplný zvyškový systém modulo m, tak

$$\sum_{n=1}^{m} \mathcal{X}_0(r_n) = \varphi(m) \tag{99}$$

a pre $\mathcal{X}\neq\mathcal{X}_0$ platí

$$\sum_{n=1}^{m} \mathcal{X}(r_n) = 0. \tag{100}$$

Dôkaz. Rovnosť (99) je zrejmá.
Ak $\mathcal{X} \neq \mathcal{X}_0$, tak existuje také $a \in \mathbb{N}, (a,m) = 1$, že

$$\mathcal{X}(a) \neq 1. \tag{101}$$

V tomto prípade je aj $ar_n, n = 1, \ldots, m$ úplný zvyškový systém modulo m. To znamená

$$\sum_{n=1}^{m} \mathcal{X}(r_n) = \sum_{n=1}^{m} \mathcal{X}(ar_n) = \sum_{n=1}^{m} \mathcal{X}(a)\mathcal{X}(r_n) = \mathcal{X}(a) \sum_{n=1}^{m} \mathcal{X}(r_n).$$

Z rovnosti (101) vyplýva rovnosť (100). □

Z rovnosti (100) vyplýva dôležitý odhad:

$$\sum_{n=k}^{N+k} = \mathcal{O}(1) \tag{102}$$

pre $k, N \in \mathbb{N}$ a $\mathcal{X} \neq \mathcal{X}_0$.

Teraz sme pripravení na použitie nasledujúceho kritéria konvegencie:

Veta 53. Nech $\{a(n)\}$ je taká postupnosť komplexných čísel, že

$$\sum_{n=1}^{N} a(n) = \mathcal{O}(1). \tag{103}$$

Ak $\{b(n)\}$ je nerastúca postuposť kladných reálnych čísel, ktorá konverguje k 0 tak a) nekonečný rad

$$\sum_{n=1}^{\infty} a(n)b(n)$$

konverguje.
b) Pre $N > 1$ platí

$$\sum_{n \leq N} a(n)b(n) = \mathcal{O}(b_N).$$

Dôkaz. Položme

$$A(n) = \sum_{k=1}^{n} a(k).$$

Pre čiastočné súcty spomínaného radu potom plati

$$\sum_{n=N+1}^{N+M} a(n)b(n) = \sum_{n=N+1}^{N+M} (A(n) - A(n-1))b(n) =$$

$$= \sum_{n=N+1}^{N+M} A(n)b(n) - \sum_{n=N+1}^{N+M} A(n-1)b(n) =$$

$$= \sum_{n=N+1}^{N+M} A(n)b(n) - \sum_{n=N}^{N+M-1} A(n)b(n+1) =$$

$$= \sum_{n=N+1}^{N+M-1} A(n)(b(n) - b(n+1)) - A(N)b(N+1) + A(M+N)b(N+M).$$

Vidíme teda, že pre $\mathcal{X} \neq \mathcal{X}_0$ rady

$$L(s, \mathcal{X}) = \sum_{n=1}^{\infty} \frac{\mathcal{X}(n)}{n^s}$$

$$L'(s, \mathcal{X}) = \sum_{n=1}^{\infty} \frac{\mathcal{X}(n) \ln n}{n^s}$$

konvegujú pre $s > 0$. Najprv budeme využívať ich hodnoty pre $s = 1$:

$$L(1, \mathcal{X}) = \sum_{n=1}^{\infty} \frac{\mathcal{X}(n)}{n} \tag{104}$$

a

$$L'(1, \mathcal{X}) = \sum_{n=1}^{\infty} \frac{\mathcal{X}(n) \ln n}{n} \tag{105}$$

konvergujú.

Lema 3. Pre $\mathcal{X} \neq \mathcal{X}_0$ a $x > 1$ platí

$$L'(1, \mathcal{X}) = L(1, \mathcal{X}) \sum_{n \leq x} \frac{\Delta(n)\mathcal{X}(n)}{n} + \mathcal{O}(1).$$

Dôkaz. Pre $x > 1$ a definície Λ platí

$$\sum_{n \leq x} \frac{\mathcal{X}(n) \ln n}{n} = \sum_{n \leq x} \frac{\mathcal{X}(n)}{n} \sum_{d|n} \Lambda(d) =$$

$$= \sum_{kd \leq x} \frac{\mathcal{X}(kd)}{kd} \Lambda(d) = \sum_{d \leq x} \sum_{k \leq \frac{x}{d}} \frac{\mathcal{X}(kd)}{kd} \Lambda(d) = \sum_{d \leq x} \frac{\mathcal{X}(d)\Lambda(d)}{d} \sum_{k \leq \frac{x}{d}} \frac{\mathcal{X}(k)}{k}.$$

Podľa vety 53 b) si môžeme vyjadriť

$$\sum_{k\leq \frac{x}{d}} \frac{\mathcal{X}(k)}{k} = L(1,\mathcal{X}) + \mathcal{O}\Big(\frac{d}{x}\Big).$$

Po dosadení do predošlej rovnosti dostávame

$$\sum_{n\leq x} \frac{\mathcal{X}(n)\ln n}{n} = L(1,\mathcal{X}) \sum_{d\leq x} \frac{\mathcal{X}(d)\Lambda(d)}{d} + \mathcal{O}\Big(\frac{1}{x}\sum_{d\leq x} \mathcal{X}(d)\Lambda(d)\Big) =$$

$$= L(1,\mathcal{X}) \sum_{d\leq x} \frac{\mathcal{X}(d)\Lambda(d)}{d} + \mathcal{O}\Big(\frac{1}{x}\sum_{d\leq x} \ln d\Big) = L(1,\mathcal{X}) \sum_{d\leq x} \frac{\mathcal{X}(d)\Lambda(d)}{d} + \mathcal{O}(1).$$

□

Z tohoto tvrdenie hneď vidíme, že

$$L(1,\mathcal{X}) \neq 0 \Longrightarrow \sum_{n\leq x} \frac{\mathcal{X}(n)\Lambda(n)}{n} = \mathcal{O}(1). \tag{106}$$

Preto na dôkaz prvej rovnosti Vety 1 stačídokázať, že hodnoty $L(1,\mathcal{X})$ sú nenulové pre $\mathcal{X} \neq \mathcal{X}_0$.

Lema 4. Pre $x > 1$ platí

$$\sum_{n\leq x} \frac{\mathcal{X}(n)\Lambda(n)}{n} = -\ln n + L(1,\mathcal{X}) \sum_{d\leq x} \mathcal{X}(d)\mu(d)\ln\frac{x}{d} + \mathcal{O}(1).$$

Dôkaz. Najprv dokážeme, že pre $n \in \mathbb{N}$, $n > 1$ a $x > n$ platí

$$\sum_{d|n} \mu(d)\ln\frac{x}{d} = \Lambda(n) \tag{107}$$

Von Mandolgtova funcia Λ je definovaná tak, aby

$$\Lambda(n) = \sum_{d|n} \mu(d)\ln\frac{n}{d}.$$

Teda

$$\Lambda(n) = \sum_{d|n} \mu(d)\Big(\ln\frac{n}{d} - \ln\frac{x}{d}\Big) + \sum_{d|n} \mu(d)\ln\frac{x}{d}.$$

Prvý sčítanec si moôžeme upraviť na tvar

$$\sum_{d|n} \mu(d)\ln\frac{n}{x} = \ln\frac{n}{x}\sum_{d|n} \mu(d) = 0.$$

Pre $n = 1$ platí

$$\sum_{d|n} \mu(d) \ln \frac{x}{d} = \ln x.$$

Druuhá rovnosť zrejmá. Von Mandolgtova funcia Λ je definovaná tak, aby

$$\Lambda(n) = \sum_{d|n} \mu(d) \ln \frac{n}{d}.$$

Teda

$$\Lambda(n) = \sum_{d|n} \mu(d) \Big(\ln \frac{n}{d} - \ln \frac{x}{d} \Big) + \sum_{d|n} \mu(d) \ln \frac{x}{d}.$$

Prvý sčítanec si moôžeme upraviť na tvar

$$\sum_{d|n} \mu(d) \ln \frac{n}{x} = \ln \frac{n}{x} \sum_{d|n} \mu(d) = 0.$$

Podľa (**??**) si môžeme vyjadriť

$$\sum_{n\le x} \frac{\mathcal{X}(n)\Lambda(n)}{n} = \sum_{n\le x} \frac{\mathcal{X}(n)}{n} \sum_{d|n} \mu(d) \ln \frac{x}{d} - \ln x =$$

$$= -\ln x + \sum_{kd\le x} \frac{\mathcal{X}(kd)}{kd} \mu(d) \ln \frac{x}{d} = -\ln x + \sum_{d\le x} \frac{\mathcal{X}(d)}{d} \mu(d) \ln \frac{x}{d} \sum_{k\le \frac{x}{d}} \frac{\mathcal{X}(k)}{k} =$$

$$= -\ln x + \sum_{d\le x} \frac{\mathcal{X}(d)}{d} \mu(d) \ln \frac{x}{d} \Big(L(1,\mathcal{X}) + \mathcal{O}\Big(\frac{d}{x}\Big)\Big) =$$

$$= -\ln x + L(1,\mathcal{X}) \sum_{d\le x} \frac{\mathcal{X}(d)}{d} \mu(d) \ln \frac{x}{d} + \mathcal{O}\Big(\frac{1}{x} \sum_{d\le x} \ln \frac{x}{d}\Big).$$

Z toho podľa príkladu 105 dostávame tvrdenie. □

Z tohoto tvrdenie vylýva

$$L(1,\mathcal{X}) = 0 \Longrightarrow \sum_{n\le x} \frac{\mathcal{X}(n)\Lambda(n)}{n} = -\ln x + \mathcal{O}(1), \tag{108}$$

pre $\mathcal{X} \neq \mathcal{X}_0$.

Teda ak označíme s počet takých charakterov $\mathcal{X}$ modulo m pre ktoré $L(1,\mathcal{X}) = 0$ dostávame

$$\sum_{n\le x} \frac{\Lambda(n)}{n} = \sum_{\mathcal{X}} \sum_{n\le x} \frac{\Lambda(n)\mathcal{X}(n)}{n} = -(s-1)\ln x + \mathcal{O}(1).$$

L'avá strana nadobúda kladné hodnoty. Ak $s > 1$ tak pravá strana konverguje do $-\infty$. Teda $s \leq 1$. Je zrejmé, že platí $L(1, \overline{\mathcal{X}}) = \overline{L(1, \mathcal{X})}$. Preto ak $L(1, \mathcal{X}) = 0$ tak charakter $\mathcal{X}$ musí nadobúdať reálne hodnoty. Preto sačí dokazať, že $L(1, \mathcal{X}) \neq 0$ ak $\mathcal{X} \neq \mathcal{X}_0$ pre reálny charakter $\mathcal{X}$ modulo m.

Definujme si funkciu

$$F(n) = \sum_{d|n} \mathcal{X}(n). \tag{109}$$

Táto funkcia je multiplikatívna a pre $n = p_1^{\alpha_1} \dots p_j^{\alpha_j}$ preto platí

$$F(n) = \prod_{i=1}^{j} \sum_{k=0}^{\alpha_i} \mathcal{X}(p_i)^k.$$

Ak $\mathcal{X}(p_i) = 1$ tak $\sum_{k=0}^{\alpha_i} \mathcal{X}(p_i)^k = \alpha_i + 1$. V prípade $\mathcal{X}(p_i) = -1$ máme $\sum_{k=0}^{\alpha_i} \mathcal{X}(p_i)^k = \frac{1-(-1)^{\alpha_1+1}}{2}$. Preto $F(n) \geq 0$ a v prípade, že všetky exponenty α_i sú párne, teda $n = k^2$ pre $k \in \mathbb{N}$ platí $F(n) \geq 1$. Ak si definujeme

$$G(x) = \sum_{n \leq x} \frac{F(n)}{\sqrt{n}}, \tag{110}$$

tak

$$G(x) \geq \sum_{n^2 \leq x} \frac{F(n)}{n} \geq \sum_{n \leq \sqrt{x}} \frac{1}{n}.$$

Preto

$$\lim_{x \to \infty} G(x) = \infty. \tag{111}$$

Funkciu G si môžeme vyjadriť aj iným spôsobom.

$$G(x) = \sum_{n \leq x} \frac{F(n)}{\sqrt{n}} = \sum_{n \leq x} \frac{1}{\sqrt{n}} \sum_{d|n} \mathcal{X}(d) = \sum_{kd \leq x} \frac{\mathcal{X}(d)}{\sqrt{kd}},$$

Pre $x \geq 1$. Ak $kd \leq x$ Tak $k \leq \sqrt{x}$ alebo $d \leq \sqrt{x}$. Preto z poslednej rovnosti dostávame

$$G(x) = \sum_{d \leq \sqrt{x}} \sum_{k \leq \frac{x}{d}} \frac{\mathcal{X}(d)}{\sqrt{kd}} + \sum_{\sqrt{x} < d \leq x} \sum_{k \leq \frac{x}{d}} \frac{\mathcal{X}(d)}{\sqrt{kd}} =$$

$$= \sum_{d \leq \sqrt{x}} \frac{\mathcal{X}(d)}{\sqrt{d}} \sum_{k \leq \frac{x}{d}} \frac{1}{\sqrt{k}} + \sum_{k \leq \sqrt{x}} \frac{1}{\sqrt{k}} \sum_{\sqrt{x} < d \leq \frac{x}{k}} \frac{\mathcal{X}(d)}{\sqrt{d}} := S_1 + S_2.$$

Prvý ščítanec môžeme upravovať

$$S_1 = \sum_{d\le\sqrt{x}} \frac{\mathcal{X}(d)}{\sqrt{d}}\Big(2\sqrt{\frac{x}{d}} + K + \mathcal{O}\Big(\sqrt{\frac{d}{x}}\Big)\Big) = \sqrt{x}\sum_{d\le\sqrt{x}} \frac{\mathcal{X}(d)}{d} + \mathcal{O}(1) =$$

$$= \sqrt{x}\Big(L(1,\mathcal{X}) + \mathcal{O} = \Big(\frac{1}{\sqrt{x}}\Big) + \mathcal{O}(1) = \sqrt{x}L(1,\mathcal{X}) + \mathcal{O}(1).$$

Pre druhý ščítanec platí

$$S_2 = \sum_{k\le\sqrt{x}} \frac{1}{\sqrt{k}}\Big(L(\frac{1}{2},\mathcal{X}) + \mathcal{O}\Big(\sqrt{\frac{k}{x}}\Big) - L(\frac{1}{2},\mathcal{X}) + \mathcal{O}\Big(\sqrt[4]{\frac{1}{x}}\Big)\Big) =$$

$$= \sum_{k\le\sqrt{x}} \frac{1}{\sqrt{k}}\Big(\mathcal{O}\Big(\sqrt{\frac{k}{x}}\Big) + \mathcal{O}\Big(\sqrt[4]{\frac{1}{x}}\Big)\Big) = \mathcal{O}(1).$$

Odvodili sme ronvosť

$$G(x) = \sqrt{x}L(1,\mathcal{X}) + \mathcal{O}(1).$$

To znamená, že $L(1,\mathcal{X}) = 0$ je v spore s (111). Tým sme dokázali prvú rovnosť Vety 46.

9 Asymptotická hustota

9.1 Úvodné pojmy

Nech $S \subset \mathbb{N}$. Hovoríme, že množina S **má asymptotickú hustotu**, ak existuje limita

$$\lim_{N\to\infty} \frac{1}{N}|[1,N]\cap S| := \mathfrak{d}(S).$$

Hodnota $\mathfrak{d}(S)$ sa nazýva **asymptotická hustota** množiny S.

Asymptotickú hustotu môžeme chápať ako istú intuitívnu "pravdepodobnosť" , že náhodne vybrané prirodzené číslo bude prvkom danej množiny. Ak $S \in \mathcal{D}$ a $N \in \mathbb{N}$ je také prirodzené číslo, že $\frac{|[1,N]\cap S|}{N} \in (\mathfrak{d}(S)-\varepsilon, \mathfrak{d}(S)+\varepsilon)$, pričom $\varepsilon > 0$ je "veľmi malé" reálne číslo, tak pravdepodobnosť, že náhodne vybrané prirodzené číslo z intervalu $[1,N]$ je prvkom S, bude "blízko" $\mathfrak{d}(S)$.

Príklad 131. Ak označíme $\mathbb{N}^2 = \{n^2; n \in \mathbb{N}\}$, tak vidíme, že pre každé $N \in \mathbb{N}$ platí

$$|[1,N]\cap\mathbb{N}^2| = [\sqrt{N}].$$

Teda $\mathbb{N}^2$ má asymptotickú hustotu a $\mathfrak{d}(\mathbb{N}^2) = 0$.

Príklad 132. Dá sa dokázať, že pre každé reálne čísla $\alpha > 1, \beta \geq 0$ má množina celých častí

$$A = \{[\alpha n + \beta]; n \in \mathbb{N}\}$$

asymptotickú hustotu a $\mathfrak{d}(A) = \frac{1}{\alpha}$.

Príklad 133. Dá sa dokázať, že množina $S \subset \mathbb{N}$ má asymptotickú hustotu práve vtedy, keď existuje taká rastúca postupnosť prirodzených čísel $\{N_k\}$, že

$$\lim_{k\to\infty} \frac{N_{k+1}}{N_k} = 1$$

a existuje limita

$$\lim_{k\to\infty} \frac{|[1, N_k] \cap S|}{N_k} = \lambda.$$

Vtedy $\mathfrak{d}(S) = \lambda$.

Veta 54. Nekonečná množina $A = \{a_1 < a_2 < \cdots < a_n < \dots\} \subset \mathbb{N}$ má asymptotickú hustotu práve vtedy, keď existuje limita

$$\lim_{n\to\infty} \frac{n}{a_n} = \lambda. \tag{112}$$

Vtedy $\mathfrak{d}(A) = \lambda$.

Dôkaz. Pre každé $n \in \mathbb{N}$ platí

$$|[1, a_n] \cap A| = n. \tag{113}$$

Teda v prípade, že $\mathfrak{d}(S) = \lambda$, dostávame

$$\lim_{n\to\infty} \frac{n}{a_n} = \lim_{n\to\infty} \frac{|[1, a_n] \cap A|}{a_n} = \alpha.$$

Predpokladajme, že (112) platí . Ak $N \in \mathbb{N}$, tak pre nejaké $k(N) \in \mathbb{N}$ platí

$$a_{k(N)} \leq N < a_{k(N)+1}.$$

Potom $|[1, N] \cap A| = k(N)$. Teda

$$\frac{k(N)}{a_{k(N)+1}} \leq \frac{|[1, N] \cap A|}{N} \leq \frac{k(N)}{a_{k(N)}}.$$

Teraz vidíme, že z (112) vyplýva

$$\lim_{N\to\infty} \frac{|[1, N] \cap A|}{N} = \lambda.$$

□

Príklad 134. Ak A má asymptotickú hustotou a $\mathfrak{d}(A) > 0$, tak $\lim_{n\to\infty} \frac{a_n}{a_{n+1}} = 1$.

Príklad 135. Ak $\alpha > 1$ je reálne číslo a množina A má asymptotickú hustotu, tak aj jej podmožina množina $\{a_{[\alpha n]}, n \in \mathbb{N}\}$ má asymptotickú hustotu, ktorá je rovná $\frac{\mathfrak{d}(A)}{\alpha}$.

Príklad 136. Podľa predošlého príkladu sa dá dokázať , že asymptotická hustota má tzv. **Darbouxovu vlastnosť**. To znamená, případe keď množina A má asymptotickú hustotu, tak pre každé $\beta \in [0, \mathfrak{d}(A)]$ existuje taká podmnožina $B \subset A$, že $\mathfrak{d}(B) = \beta$.

9.2 Vlastnosti systému množín s asymptotickou hustotou

Systém všetkých množín, ktoré majú asymptotickú hustotu budeme označovať symblom $\mathcal{D}$. Tento systém má nasledujúce vlastnosti:

Veta 55. Ak $S_1, S_2 \in \mathcal{D}$, tak
i) $S_1 \cap S_2 = \emptyset \Longrightarrow S_1 \cup S_2 \in \mathcal{D} \wedge \mathfrak{d}(S_1 \cup S_2) = \mathfrak{d}(S_1) + \mathfrak{d}(S_2)$.
ii) $S_1 \subset S_2 \Longrightarrow S_2 \setminus S_1 \in \mathcal{D} \wedge \mathfrak{d}(S_2 \setminus S_1) = \mathfrak{d}(S_2) - \mathfrak{d}(S_1)$

Dôkaz. Dôkaz tohoto tvrdenia je jednoduchý. V prípade i) totiž platí

$$|[1, N] \cap (S_1 \cup S_2)| = |[1, N] \cap S_1| + |[1, N] \cap S_2|$$

pre $N \in \mathbb{N}$. Podobne v prípade ii) zase

$$|[1, N] \cap (S_2 \setminus S_1)| = |[1, N] \cap S_2| - |[1, N] \cap S_1|.$$

□

Nie každá množina má asymptotickú hustotu. Niekedy, aby sme do istých vecí mohli vniesť jasno, budeme používať funkciu

$$\overline{\mathfrak{d}}(S) = \limsup_{N\to\infty} \frac{1}{N} |[1, N] \cap S|.$$

Táto funkcia sa nazýva **horná asymptotická hustota**. Jej dôležité vlastnosti sú: Pre $S_1, S_2 \subset \mathbb{N}$ platí

$$\overline{\mathfrak{d}}(S_1 \cup S_2) \leq \overline{\mathfrak{d}}(S_1) + \overline{\mathfrak{d}}(S_2) \tag{114}$$

$$S_1 \subset S_2 \Longrightarrow \overline{\mathfrak{d}}(S_1) \leq \overline{\mathfrak{d}}(S_2). \tag{115}$$

Veta 56. Množina $S \subset \mathbb{N}$ patrí do $\mathcal{D}$ práve vtedy, keď

$$\overline{\mathfrak{d}}(S) + \overline{\mathfrak{d}}(\mathbb{N} \setminus S) \leq 1. \tag{116}$$

Dôkaz. Istými úpravami sa dá odvodiť, že

$$1 - \overline{\mathfrak{d}}(\mathbb{N} \setminus S) = \liminf_{N \to \infty} \frac{|S \cap [1, N]|}{N}.$$

Preto $S \in \mathcal{D}$ práve vtedy

$$\overline{\mathfrak{d}}(S) + \overline{\mathfrak{d}}(\mathbb{N} \setminus S) = 1. \tag{117}$$

Podľa (114) dostáveme, že vždy

$$\overline{\mathfrak{d}}(S) + \overline{\mathfrak{d}}(\mathbb{N} \setminus S) \geq 1.$$

Z toho vyplýva, že (117) je ekvivalentné s (116). □

Príklad 137. Ak $A \subset \mathbb{N}$ a $\overline{\mathfrak{d}}(A) + \overline{\mathfrak{d}}(\mathbb{N} \setminus A) \leq 1$, tak $A \in \mathcal{D}$ a $\mathfrak{d}(A) = \overline{\mathfrak{d}}(A)$.

Príklad 138. Nech $A_1, \ldots, A_k \subset \mathbb{N}$ sú disjunktné množiny. Ak $A_1 \cup \cdots \cup A_k = \mathbb{N}$ a $\overline{\mathfrak{d}}(A_i) \leq \delta_i$,$i = 1, \ldots, k$, pričom $\delta_1 + \cdots + \delta_k = 1$, tak $A_i \in \mathcal{D}$ a $\mathfrak{d}(A_i) = \delta_i$ pre $i = 1, \ldots, k$.

Príklad 139. Nech $S \in \mathcal{D}$ a $S_1, \ldots, S_k \subset \mathbb{N}$ sú disjunktné množiny. Ak $S_1 \cup \cdots \cup S_k = S$ a $\sum_{i=1}^{k} \overline{\mathfrak{d}}(S_i) \leq 1$, tak $S_i \in \mathcal{D}$ pre $i = 1, \ldots, k$, pričom $\sum_{i=1}^{k} \mathfrak{d}(S_i) = \mathfrak{d}(S)$.

Asymptotická hustota nie je σ - aditívna. Preto je niekedy potrebné nájsť také podmienky, ktoré zaručia slabšiu formu σ - aditivity. Pri nasledujúcich úvahách bude hrať dôležitú úlohu horná asymptotická hustota.

Veta 57. i) Množina S patrí do $\mathcal{D}$ práve vtedy, keď

$$\forall \varepsilon > 0 \exists S_\varepsilon \in \mathcal{D}; S_\varepsilon \subset S \wedge \overline{\mathfrak{d}}(S \setminus S_\varepsilon) < \varepsilon.$$

V tomto prípade platí $\mathfrak{d}(S) = \sup\{\mathfrak{d}(S_\varepsilon); \varepsilon > 0\}$.
ii) Množina S patrí do $\mathcal{D}$ práve vtedy, keď

$$\forall \varepsilon > 0 \exists S_\varepsilon \in \mathcal{D}; S \subset S_\varepsilon \wedge \overline{\mathfrak{d}}(S_\varepsilon \setminus S) < \varepsilon.$$

Dôkaz. i) Pre dané ε si môžeme vyjadriť

$$|[1,N]\cap S| = |[1,N]\cap S_\varepsilon| + |[1,N]\cap (S\setminus S_\varepsilon)|.$$

Z toho vyplýva

$$\mathfrak{d}(S_\varepsilon) \le \limsup_{N\to\infty} \frac{|[1,N]\cap S|}{N} \le \mathfrak{d}(S_\varepsilon)+\varepsilon.$$

A rovnako

$$\mathfrak{d}(S_\varepsilon) \le \liminf_{N\to\infty} \frac{|[1,N]\cap S|}{N} \le \mathfrak{d}(S_\varepsilon)+\varepsilon.$$

Teda vidíme, že

$$\limsup_{N\to\infty} \frac{|[1,N]\cap S|}{N} - \liminf_{N\to\infty} \frac{|[1,N]\cap S|}{N} < \varepsilon.$$

Pre $\varepsilon \to 0^+$ dostávame, že existuje limita

$$\lim_{N\to\infty} \frac{|[1,N]\cap S|}{N} = \mathfrak{d}(S).$$

Časť ii) vyplýva z i) tak, že ju použijeme na množinu $\mathbb{N}\setminus S$. □

Z tejto vety okamžite vyplýva

Veta 58. Nech $A_1 \subset A_2 \subset \cdots \subset A_k \subset \ldots$ **sú množiny patriace do** $\mathcal{D}$**. Položme** $A = \cup_{k=1}^{\infty} A_k$**. Ak** $\lim_{n\to\infty} \overline{\mathfrak{d}}(A\setminus A_n) = 0$**, tak** $A \in \mathcal{D}$ **a** $\mathfrak{d}(A) = \lim_{n\to\infty} \mathfrak{d}(A_n)$**.**

Veta 59. Ak $B_1, B_2, \ldots, B_k, \ldots$ **sú dizjunktné patriace do** $\mathcal{D}$ **a** $\lim_{n\to\infty} \overline{\mathfrak{d}}(\cup_{k=n}^{\infty} B_k) = 0$**, tak** $\cup_{k=1}^{\infty} B_k$ **patrí do** $\mathcal{D}$ **a**

$$\overline{\mathfrak{d}}\Big(\bigcup_{k=1}^{\infty} B_k\Big) = \sum_{k=1}^{\infty} \mathfrak{d}(B_k).$$

Z týchto skutočností sa dá odvodiť výsledok, ktorý v roku 1965 dokázal Ralph Alexander:

Veta 60. Ak $A_1, A_2, \ldots A_n, \ldots$ **sú dizjunktné množiny z** $\mathcal{D}$ **a existuje taký konvergentný nekonečný rad** $\sum_{n=1}^{\infty} c_n$**, že pre každé** $n \in \mathbb{N}, N \in \mathbb{N}$ **platí**

$$\frac{|[1,N]\cap A_n|}{N} \le c_n,$$

tak množina $A = \cup_{n=1}^{\infty}$ **patrí do** $\mathcal{D}$ **a**

$$\mathfrak{d}(A) = \sum_{n=1}^{\infty} \mathfrak{d}(A_n).$$

Dôkaz. Pre každé $n \in \mathbb{N}$ platí

$$A \setminus \bigcup_{n=1}^{k} A_n = \bigcup_{n=k+1}^{\infty} A_n.$$

A teda

$$\frac{|[1,N] \cap (A \setminus \bigcup_{n=1}^{k} A_n)|}{N} \leq \sum_{n=k+1}^{\infty} c_k.$$

Z toho vyplýva

$$\overline{\mathfrak{d}}\Big(A \setminus \bigcup_{n=1}^{k} A_n\Big) \leq \sum_{n=k+1}^{\infty} c_k.$$

□

9.3 Zvyškové triedy

Tak, ako sme už spomínali, zvyškové triedy budeme označovať

$$r + (m) = \{n \in \mathbb{N}; n \equiv r \pmod{m}\},$$

pre $m \in \mathbb{N}, r \in \mathbb{Z}$. [1] Pre $N \in \mathbb{N}$ platí

$$|(r + (m)) \cap [1,N]| = |\{k \in \mathbb{N}; r + km \leq N\} = \Big[\frac{N-r}{m}\Big].$$

Teda $r + (m) \in \mathcal{D}$ a

$$\mathfrak{d}(r + (m)) = \frac{1}{m}. \tag{118}$$

Podmienka dizjunktného prieniku časti i) vety 55 sa vo všeobecnosti nedá vynechať. Niekedy je dobré nájsť také podsystémy $\mathcal{D}$ pre, ktoré sa vynechať dá. Nasledujúci je jedným z nich.

Symbolom $\mathcal{D}_0$ budeme označovať systém všetkých množín v tvare $\cup_{i=1}^{k} r_i + (m_i)$. Teda všetky zjednotenia konečného počtu zvyškových tried. Ak $S \in \mathcal{D}_0$ je množina v takomto tvare a položíme $m = m_1 \dots m_k$, tak každá zvyšková trieda $r_i + (m_i)$ sa dá vyjadriť ako dizjunktné zjednotenie zvyškových tried $\ell + (m)$. Teda S má asymptotickú hustotu. Z toho vyplýva

$$\mathcal{D}_0 \subset \mathcal{D}. \tag{119}$$

[1] Toto označenie má význam v tom, že (m) znamená hlavný ideál generovaný m v okruhu celých čísel $\mathbb{Z}$ a $r+(m)$ príslušné triedy rozkladu. My síce uvažujeme iba "polovicu" tohoto ideálu, jeho kladnú časť. Ale všetky vlastnosti týchto množín sú kópiami vlastností ideálov.

V roku 1994 dokázal Tibor Šalát zaujímavú rovnosť. Nech p je prvočíslo. Označme $\alpha_p(n)$ exponent, s ktorým vystupuje p v kánonickom rozklade prirodzeného čísla n. Teda, ak $p \nmid n$, tak $\alpha_p(n) = 0$. Definujme si množinu

$$M_p = \{n \in \mathbb{N}; \alpha_p(n)|n\}.$$

Šalátov výsledok je

Propozícia 1. Pre každé prvočíslo p množina M_p patrí do $\mathcal{D}$ a

$$\mathfrak{d}(M_p) = (p-1)\sum_{k=1}^{\infty} \frac{1}{kp^{k-\alpha_p(k)+1}}.$$

Dôkaz. Označíme si množiny

$$B_k = \{n \in \mathbb{N}; \alpha_p(n) = k \wedge k|n\},$$

kde $k = 1, 2, 3, \ldots,$. Vidíme, že platí

$$M_p = \bigcup_{k=1}^{\infty} B_k.$$

Ukážeme, že sa dá použiť Veta 59. V prvom rade vidíme, že množiny B_k sú disjunktné. Keď sa pozrieme na definíciu množín B_k, uvedomíme si, že

$$B_k = (kp^{k-\alpha_p(k)}) \setminus (kp^{k-\alpha_p(k)+1}).$$

Teda $B_k \in \mathcal{D}$ a

$$\mathfrak{d}(B_k) = \frac{1}{kp^{k-\alpha_p(k)}} - \frac{1}{kp^{k-\alpha_p(k)+1}} = \frac{p-1}{kp^{k-\alpha_p(k)+1}}.$$

Pre $k > N$ pre dané $k_0 \in \mathbb{N}$ platí $B_k \subset (p^N)$. Teda $\cup_{k=N}^{\infty} B_k \subset (p^N)$. Preto $\lim_{N\to\infty} \overline{\mathfrak{d}}(\cup_{k=N}^{\infty} B_k) = 0$. Vidíme teraz, že tvrdenie vyplýva z Vety 59. □

Podobným spôsobom ako (119) sa dá dokázať:

$$S, S' \in \mathcal{D}_0 \Longrightarrow S \cap S' \in \mathcal{D}_0, S \cup S' \in \mathcal{D}_0. \tag{120}$$

Z toho vyplýva

$$\mathfrak{d}(S \cup S') = \mathfrak{d}(S) + \mathfrak{d}(S') - \mathfrak{d}(S \cap S'). \tag{121}$$

Príklad 140. Nech $m_1, m_2 \in \mathbb{N}$ sú nesúdeliteľné. Ak $r_1, r_2 \in \mathbb{Z}$, tak podľa Čínskej zvyškovej vety platí $(r_1 + (m_1)) \cap (r_2 + (m_2)) = r_3 + (m_1 m_2)$. Preto $\mathfrak{d}((r_1 + (m_1)) \cap (r_2 + (m_2)) = \frac{1}{m_1 m_2}$. Z toho vyplýva

$$\mathfrak{d}((r_1 + (m_1)) \cup (r_2 + (m_2)) = \frac{1}{m_1} + \frac{1}{m_2} - \frac{1}{m_1 m_2} = 1 - \Big(1 - \frac{1}{m_1}\Big)\Big(1 - \frac{1}{m_2}\Big).$$

Veta 61. i) Ak $m_1, \ldots, m_k$, sú navzájom nesúdeliteľné prirodzené čísla, $k \in \mathbb{N}$, tak množina $\cup_{j=1}^{k} r_j + (m_j)$, kde $r_1, \ldots, r_n \in \mathbb{Z}$, má asymptotickú hustotu, pričom

$$\mathfrak{d}\Big(\bigcup_{j=1}^{k} r_j + (m_j)\Big) = 1 - \prod_{j=1}^{k} \Big(1 - \frac{1}{m_j}\Big),$$

ii) Ak $m_1, m_2, \ldots, m_k, \ldots$ sú navzájom nesúdeliteľné čísla, tak množina $A = \cup_{k=1}^{\infty}(m_k)$ patrí do $\mathcal{D}$ a

$$\mathfrak{d}(A) = 1 - \prod_{k=1}^{\infty} \Big(1 - \frac{1}{m_k}\Big).$$

Dôkaz. Časť i) vyplýva z princípu zapojenia a vypojenia, alebo sa dá dokázť indukciou. Podobne ako v predošlom príklade.

Na časť ii) použijeme Vetu 58. Označme

$$A_k = \bigcup_{j=1}^{k} (m_k).$$

Potom

$$A = \bigcup_{k=1}^{\infty} A_k.$$

Predpokladajme najprv, že rad $\sum_{k=1}^{\infty} \frac{1}{m_k}$ diverguje. V tom prípade dostáveme podľa i)

$$\lim_{k \to \infty} \mathfrak{d}(A_k) = 1.$$

Z toho podľa Vety 58 dostávame $\mathfrak{d}(A) = 1$. Predpokladajme teraz, že rad $\sum_{k=1}^{\infty} \frac{1}{m_k}$ konverguje. Množinu A si môžeme vyjadriť ako

$$A = A_k \cup \bigcup_{n=k+1}^{\infty} (m_k).$$

Teda

$$A \setminus A_k \subset \bigcup_{n=k+1}^{\infty} (m_k).$$

Teraz si uvedomíme, že

$$|[1, N] \cap (m_j)| = \Big[\frac{N}{m_j}\Big].$$

A teda

$$|[1, N] \cap (A \setminus A_k)| \leq \sum_{j=k+1}^{\infty} \Big[\frac{N}{m_j}\Big].$$

Preto

$$\overline{\mathfrak{d}}(A \setminus A_k) \leq \sum_{j=k+1}^{\infty} \frac{1}{m_j}.$$

Z podmienky konvergencie daného radu vyplýva teda $\lim_{k\to\infty} \overline{\mathfrak{d}}(A \setminus A_k) = 0$. Podľa Vety 58 dostáveme tvrdenie ii). □

Pomocou časti i) Vety 61 dokážeme výsledok Pála Erdösa z roku 1934.

Propozícia 2. Označme

$$B_N = \bigcup_{m=N+1}^{2N} (m).$$

Potom $\lim_{N\to\infty} \mathfrak{d}(B_N) = 0$.

Dôkaz. Pre každé $N \in \mathbb{N}$ platí

$$\bigcup_{m=1}^{N} (m) = \bigcup_{p\leq N} (p) := S_N.$$

Z toho podľa i) Vety 61 vyplýva, že $S_N \in \mathcal{D}$, pre $N \in \mathbb{N}$ a

$$\mathfrak{d}(S_N) = 1 - \prod_{p\leq N} \Big(1 - \frac{1}{p}\Big). \tag{122}$$

Potom $B_N = S_{2N} \setminus S_N$ a teda z (122) dostávame $B_N \in \mathcal{D}$ a

$$\mathfrak{d}(B_N) = \prod_{p\leq N} \Big(1 - \frac{1}{p}\Big) - \prod_{p\leq 2N} \Big(1 - \frac{1}{p}\Big).$$

Z toho vyplýva

$$\lim_{N\to\infty} \mathfrak{d}(B_N) = 0.$$

□

Tento výsledok z roku sa dá zosilniť

Príklad 141. Nech $\ell_N > j_N, N = 1, 2, 3, \ldots$ a $J_N \to \infty$ for $N \to \infty$. Potom

$$\lim_{N\to\infty} \mathfrak{d}\Big(\bigcup_{m=j_N}^{\ell_N} (m)\Big) = 0.$$

Príklad 142. Uvažujme množinu $C_N = \bigcup_{m=N}^{\infty}(m)$, $N = 1, 2, 3, \ldots$. Potom pre každé N platí

$$\bigcup_{N\le p} (p) \subset C_N.$$

Z toho vyplýva podľa vety 61, že $C_N \in \mathcal{D}$ a $\mathfrak{d}(C_N) = 1$.

Príklad 143. Množinu prirodzených čísel v tvare $p_1 \ldots p_k$, p_i sú rozne prvočísla budeme označovať symbolom Q_2. Takéto čísla sa nazývajú **bezkvadratické čísla**. Pôvodne **Quadratfreie Zahlen**. Túto množinu tvoria prirodzené čísla ktoré nie sú deliteľné druhou mocninou žiadneho prvočísla. Z toho vyplýva

$$Q_2 = \mathbb{N} \setminus \bigcap_p (p^2).$$

Zjednotenie na pravej strane prebieha cez celú množinu prvočísel. Podľa predošlej vety dostávame $Q_2 \in \mathcal{D}$ a

$$\mathfrak{d}(Q_2) = \prod_p \Big(1 - \frac{1}{p^2}\Big) = \frac{6}{\pi^2}.$$

Tento výsledok môže pôsobiť dosť prekvapivo. Z hľadiska kánonického rozkladu sa zdá, že ide o zriedkavé prípady prirodzených čísel. Z nášho príkladu však vyplýva, že pri usporiadaní podľa veľkosti je ich viac ako polovica.

Príklad 144. Podobne sa dá dokázať, že množina Q_n, ktorá obsahuje všetky prirodzené čísla, ktoré majú v kánonickom rozklade exponenty menšie ako n, má asymptotickú hustotu $\frac{1}{\zeta(n)}$.

Príklad 145. Nech $p_1 < p_2 < \cdots < p_n < \ldots$ sú také prvočísla, že

$$\sum_{n=1}^{\infty} \frac{1}{p_n} = \infty.$$

Označme S množinu všetkých prirodzených čísel, ktoré neobsahujú v kánonickom rozklade tieto prvočísla. Potom $S \in \mathcal{D}$ a $\mathfrak{d}(S) = 0$.

Príklad 146. Neprázdna množina $M \subset \mathbb{N}$ sa nazýva **uzavretá vzhľadom na deliteľnost** ak

$$\forall m \in M \forall d \in \mathbb{N}; d|m \Rightarrow d \in M \tag{123}$$

a

$$\forall m_1, m_2 \in M; [m_1, m_2] \in M. \tag{124}$$

V takomto prípade môžeme každému prvočíslu p priradiť hodnoty

$$e(p) = \max\{k; p^k \in M\}.$$

Potom platí

$$M = \mathbb{N} \setminus \bigcup_{e(p)<\infty} (p^{e(p)+1}). \tag{125}$$

Teda M má symptotickú hustotu a

$$\mathfrak{d}(M) = \prod_{e(p)<\infty} \Big(1 - \frac{1}{p^{e(p)+1}}\Big).$$

Medzi výsledky Ralpha Alexandra patrí aj nasledujúca aplikácia "slabšej" σ aditivity.

Veta 62. Nech $r_n + (m_n), 0 \leq r_n < m_n$, $n \in \mathbb{N}$ **sú také dizjunktné množiny, že množina** $A = \{r_n; n \in \mathbb{N}\}$ **má asymptotickú hustotu. Potom nekonečný rad** $\sum_{n=1}^{\infty} \frac{1}{m_n}$ **konverguje a množina**

$$C = \bigcup_{n=1}^{\infty} r_n + (m_n)$$

má asymptotickú hustotu, pričom

$$\mathfrak{d}(C) = \mathfrak{d}(A) + \sum_{n=1}^{\infty} \frac{1}{m_n}.$$

Dôkaz. Z toho, že dané množiny sú dizjunktné,vyplýva

$$\sum_{n=1}^{N} \frac{1}{m_n} \leq 1$$

a teda tento nekonečný rad konverguje. Označme $H_n = (r_n + (m_n)) \setminus r_n$. Potom

$$C = A \cup \bigcup_{n=1}^{\infty} H_n. \tag{126}$$

Pre každú množinu H_n platí

$$\frac{|[1,N]\cap H_n|}{N}\leq\frac{1}{m_n}.$$

Z Vety 60 dostávame, že množina $\cup_{n=1}^{\infty}H_n$ má asymptotickú hustotu, ktorá sa rovná súčtu daného nekonečného radu. Z toho, že množiny napravo v (126) sú dizjunktné vyplýva tvrdenie vety. □

Vznikla otázka, či každé zjednotenie "ideálov" má asymptotickú hustotu. Besichovich zostrojil množinu, ktorá na danú otázku dáva negatívnu odpoveď.

Veta 63. Existuje taká postupnosť prirodzených čísel $m_n, n\in\mathbb{N}$, že množina $\cup_{n=1}^{\infty}(m_n)$ nemá asymptotickú hustotu.

Dôkaz. Nech $B_N, N\in\mathbb{N}$ sú množiny z Propozície 2 Uvažujme $\varepsilon>0$. Podľa Vety **??** môžeme utvoriť takú postupnosť $N_1<N_2<\ldots N_k<\ldots$, že

$$\mathfrak{d}(B_{N_k})<\frac{\varepsilon}{2^{k+1}},$$

a

$$N_{k+1}>2N_k\ ,\ k=1,2,3,\ldots.$$

a

$$\frac{|[1,N_{k+1}]\cap B_{N_j}|}{N_{k+1}}\leq\frac{\varepsilon}{2^k},\tag{127}$$

pre $j=1,\ldots,k$. Označme

$$B=\bigcup_{k=1}^{\infty}B_{N_k}.$$

Potom pre $k\in\mathbb{N}$ máme

$$|[1,2N_k]\cap B|\geq N_k.$$

Preto

$$\overline{\mathfrak{d}}(B)\geq\limsup_{k\to\infty}\frac{|[1,2N_k]\cap B|}{2N_k}\geq\frac{1}{2}.$$

Z druhej strany podľa (127) dostávame

$$|[1,N_k]\cap B|\leq\sum_{j=1}^{k}|[1,N_k]\cap B_{N_j}|\leq\sum_{j=1}^{k}\frac{\varepsilon}{2^j}N_k.$$

To znamená

$$\liminf_{k\to\infty} \frac{|[1,N_k]\cap B|}{N_k} < \varepsilon < \frac{1}{2}.$$

□

Túto časť ukončíme vetou, ktorá bude hrať kľúčovú úlohu v ďalšom.

Lema 5. Nech $S = \cup_{j=1}^{k} r_j + (m_j)$ **pre** $k \in \mathbb{N}$**,** $r_1, \dots, r_k \in \mathbb{Z}$**,** $m_1, \dots, m_k \in \mathbb{N}$**. Nech pre** $m \in \mathbb{N}$ **platí** $(m, m_j) = 1, j = 1, \dots, k$**. Potom pre každé** $r \in \mathbb{Z}$ **platí** $S \cap (r + (m)) \in \mathcal{D}$ a

$$\mathfrak{d}(S \cap (r + (m))) = \frac{1}{m}\mathfrak{d}(S).$$

Dôkaz. Množinu S môžeme vyjadriť v tvare disjunktného rozkladu

$$S = \bigcup_{i=1}^{r} \ell_i + (M),$$

kde $m = m_1 \dots m_k$. Z tohoto vyjadrenia vyplýva $\mathfrak{d}(S) = \frac{r}{M}$. Podľa Čínskej vety o zvyškoch dostávame

$$S \cap (r + (m)) = \bigcup_{i=1}^{r} \ell_i' + (mM),$$

pre vhodné $\ell_1', \dots, \ell_r' \in \mathbb{Z}$. Preto $\mathfrak{d}(S \cap (r + (m))) = \frac{1}{mM} = \frac{r}{M}\mathfrak{d}(S)$. □

Veta 64. Ak $m_1, m_2, \dots m_k$ sú nesúdeliteľné čísla, tak **množina** $\cup_{j=1}^{k}(m_j) \setminus (m_j^2)$ **má asymptotickú hustotu a**

$$\mathfrak{d}\Big(\bigcup_{j=1}^{k}(m_j) \setminus (m_j^2)\Big) = 1 - \prod_{j=1}^{k}\Big(1 - \frac{1}{m_j} + \frac{1}{m_j^2}\Big).$$

Dôkaz. Budeme postupovať indukciou. Pre $k = 1$ rovnosť platí . Nech platí pre $k - 1$. Potom

$$\mathfrak{d}\Big(\bigcup_{j=1}^{k-1}(m_j) \setminus (m_j^2)\Big) = 1 - \prod_{j=1}^{k-1} k\Big(1 - \frac{1}{m_j} + \frac{1}{m_j^2}\Big).$$

Označme si pre zjednodušenie

$$S = \bigcup_{j=1}^{k-1}(m_j) \setminus (m_j^2).$$

Potom

$$\bigcup_{j=1}^{k}(m_j) \setminus (m_j^2) = S \cup ((m_k) \setminus (m_k^)).$$

Teda

$$\mathfrak{d}\Big(\bigcup_{j=1}^{k}(m_j) \setminus (m_j^2)\Big) = \mathfrak{d}(S) + \mathfrak{d}((m_k) \setminus (m_k^2) - \mathfrak{d}(S \cap ((m_k) \setminus (m_k^2)). \quad (128)$$

Podľa Lemy 5 platí

$$\mathfrak{d}(S \cap ((m_k) \setminus (m_k^2)) = \mathfrak{d}(S \cap ((m_k)) - \mathfrak{d}(S \cap (m_k^2)) =$$

$$= \frac{1}{m_k}\mathfrak{d}(S) - \frac{1}{m_k^2}\mathfrak{d}(S) = \Big(\frac{1}{m_k} - \frac{1}{m_k^2}\Big)\mathfrak{d}(S).$$

Po dosadení do (128) dostávame, že tvrdenie platí aj pre k. □

Význam tejto vety bude spočívať hlavne v tom, že v prípade $\sum_{k=1}^{\infty}\frac{1}{m_j} = \infty$ platí

$$\lim_{k\to\infty}\prod_{j=1}^{k}\Big(1 - \frac{1}{m_j} + \frac{1}{m_j^2}\Big) = 0. \quad (129)$$

9.4 Rozdelenie postupností

Hovoríme, že postupnosť v , teda to isté čo aritmetická funkcia, je **rovnomerne rozdelená** ak $v(n) \in [0,1], n \in \mathbb{N}$ a pre každý interval $I \subset [0,1]$ platí $v^{-1}(I) \in \mathcal{D}$ a $\mathfrak{d}(v^{-1}(I)) = |I|$. Tento pojem definoval v roku 1916 Hermann Weyl.

Príklad 147. Priamym výpočtom asymptotickej hustoty sa dá dokázať, že postupnosť v, kde

$$\{v(n)\} = \Big\{\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \ldots, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \ldots, \Big\}$$

je rovnomerne rozdelená.

Príklad 148. Dá sa dokázať, že postupnosť v je rovnomerne rozdelená práve vtedy, ak existuje hustá podmožina $A \subset [0,1]$, že pre každé $x \in A$ platí $v^{-1}([0,x)) \in \mathcal{D}$ a $d(v^{-1}([0,x))) = x$.

Rovnomerne rozdelené postupnosti majú okrem iného použitie na odhad určitých integrálov. Nasledujúci výsledok nesie názov **Weylovo kritérium**.

Veta 65. Postupnosť $\{v(n)\}$ je rovomerne rozdelená práve vtedy, keď pre každú spojitú reálnu funkciu f definovanú na intervale $[0,1]$ platí

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} f(v(n)) = \int_0^1 f(x)dx. \tag{130}$$

Dôkaz. Predpokladajme, že platí (130). Ak $I \subset [0,1]$, tak pre každé $\varepsilon > 0$ existujú spojité f_1, f_2 také, že

$$f_1 \leq \mathbf{C}_I \leq f_2 \tag{131}$$

a

$$\int_0^1 f_2(x)dx - \int_0^1 f_1(x)dx < \varepsilon. \tag{132}$$

Z nerovností (131) vyplýva

$$\int_0^1 f_1(x)dx \leq |I| \leq \int_0^1 f_2(x)dx. \tag{133}$$

Z nerovností (131) dostávame

$$\frac{1}{N}\sum_{n=1}^{N} f_1(v(n)) \leq \frac{1}{N}\sum_{n=1}^{N} \mathbf{C}_I(v(n)) \leq \frac{1}{N}\sum_{n=1}^{N} f_2(v(n))$$

Hodnota $v(n)$ patrí do intervalu I práve vtedy, keď $n \in v^{-1}(I)$. To znamená $\mathbf{C}_I(v(n)) = \mathbf{C}_{v^{-1}(I)}(n)$. Posledné nerovnosti môžeme preto napísať v tvare

$$\frac{1}{N}\sum_{n=1}^{N} f_1(v(n)) \leq \frac{1}{N}\sum_{n=1}^{N} \mathbf{C}_{v^{-1}(I)}(n) \leq \frac{1}{N}\sum_{n=1}^{N} f_2(v(n))$$

pre $N = 1, 2, 3, \ldots$. Ak použijeme rovnosť (130) dostávame, že dostávame, že každý hromadný bod postupnostosti $\frac{1}{N}\sum_{n=1}^{N} \mathbf{C}_{v^{-1}(I)}(n), N = 1, 2, 3, \ldots$ patrí do intervalu $[\int_0^1 f_1(x)dx, \int_0^1 f_2(x)dx]$. Dĺžka toho intervalu neprevyšuje ε. Ak uvážime $\varepsilon \to 0^+$ dostávame, že táto postupnosť konverguje. Z nerovností (133) potom vyplýva

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} \mathbf{C}_{v^{-1}(I)}(n) = |I|.$$

Preto $v^{-1}(I) \in \mathcal{D}$ a $\mathfrak{d}(v^{-1}(I)) = I$.

Predpokladajme, že postupnosť je rovnomerne rozdelená. Potom pre každý interval $I \subset [0,1]$ platí

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathbf{C}_I(v(n)) = |I| = \int_0^1 \mathbf{C}_I(x)dx.$$

Z toho vyplýva, že pre každú schodkovitú funkciu s platí

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} s(v(n)) = \int_0^1 s(x)dx.$$

Každú spojitú funkciu na $[0,1]$ môžeme rovnomerne aproximovať schodkovitými funkciami a teda platí (130). □

Príklad 149. Weylove kritérium sa dá mierne preformulovať:
Postupnosť $\{v(n)\}, v(n) \in [0,1]$ **je rovnomerne rozdelená práve vtedy, keď**

$$\limsup_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(v(n)) \leq \int_0^1 f(x)dx$$

pre každú nezápornú spojitú funkciu definovanú na $[0,1]$.

Podľa Fejerovej vety vieme, že každú spojitú funkciu f definovanú na intervale $[0,1]$ takú, že $f(0) = f(1)$ môžeme rovnomerne aproximovať trigonometrickým polynómom v tvare $\sum_{n=-k}^{k} c_n e^{2\pi inx}$. Z toho vyplýva efektívnejšia forma Weylovho kritéria

Veta 66. Postupnosť $\{v(n)\}$ **prvkov intervalu** $[0,1]$ **je rovnomerne rozdelená práve vtedy, keď**

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi ihv(n)} = 0,$$

pre každé $h \in \mathbb{Z}, h \neq 0$**.**

Príklad 150. Podľa predošlej vety sa dá dokázať: Ak postupnosť $\{v(n)\}$ je rovnomerne rozdelená a $m \in \mathbb{Z}$ tak aj postupnosť zlomkových častí $\{\{mv(n)\}\}$ je rovnomerne rozdelená.

Príklad 151. Nech α je iracionálne číslo. Pomocou predošlej vety sa dá doká- zať, že postupnosť zlomkových častí $\{\{n\alpha\}\}$ je rovnomerne rozdelená. Vie- me, že $e^{2\pi ih\{n\alpha\}} = e^{2\pi ihn\alpha}$ a teda

$$\sum_{n=1}^{N} e^{2\pi ih\{n\alpha\}} = \sum_{n=1}^{N} e^{2\pi ihn\alpha} = \frac{e^{2\pi ih(N+1)\alpha} - 1}{e^{2\pi ih\alpha} - 1}$$

pre $h \neq 0$. Môžeme použiť vzorec pre súčet geometrickej postupnosti, pretože z podmienky iracionality α vyplýva $e^{2\pi i h\alpha} \neq 1$ pre $h \neq 0$.

Rovnomerné rozdelenie postupnosti z predošlého príkladu dokáže doplniť Dirichletov výsledok o diofantických aproximáciách. Teda o presnosti aproximácie iracionálneho čísla zlomkom vzhľadom na jeho menovateľ. Dirichlet dokázal, že **pre každé iracionálne číslo α existuje nekonečne veľa prirodzených čísel n ku ktorým existuje také k_n, že platí**

$$\left|\alpha - \frac{k_n}{n}\right| < \frac{1}{n^2}.$$

Tu dokážeme, že ich zase až tak "veľa" nie je.

Veta 67. Nech $\alpha > 0$ je iracionálne číslo a $f(n)$ je taká aritmetická funkcia, že

$$\lim_{n\to\infty} \frac{n}{f(n)} = 0. \tag{134}$$

Označme S množinu takých prirodzených čísel n pre ktoré existuje $k_n \in \mathbb{N}$, že

$$\left|\alpha - \frac{k_n}{n}\right| < \frac{1}{f(n)}.$$

Potom $S \in \mathcal{D}$ a $\mathfrak{d}(S) = 0$.

Dôkaz. Označme pre dané α a $c \in (0, \frac{1}{2})$ symbolom $S(c)$ množinu takých $n \in \mathbb{N}$ pre ktoré existuje také $p \in \mathbb{N}$, že

$$\left|\alpha - \frac{p}{n}\right| < \frac{c}{n}.$$

Táto nerovnosť je ekvivalentná

$$|\alpha n - p| < c.$$

To znamená

$$|\{\alpha n\} - [p - \alpha n]| < c.$$

To znamená, že $\{n\alpha\}$ musí byť vzdialené od najbližšieho celého čísla o menej ako c. Teda

$$S(c) = \{n \in \mathbb{N}; \{n\alpha\} \in (0, c)\} \cup \{n \in \mathbb{N}; \{n\alpha\} \in (1 - c, 1)\}.$$

Ak zoberieme do úvahy, že postupnosť $\{\{n\alpha\}\}$ je rovnomerne rozdelená dostávame, že $S(c) \in \mathcal{D}$ a $\mathfrak{d}(S(c)) = 2c$.

Z podmienky (134) vyplýva, že pre dané c existuje n_0, že pre $n > n_0$ platí $\frac{n}{f(n)} < c$. Preto

$$\frac{1}{f(n)} < \frac{c}{n}.$$

Z toho dostávem, že

$$S \setminus \{1, \ldots, n_0\} \subset S(c).$$

Teda $\overline{\mathfrak{d}}(S) < 2c$. Pre $c \to 0^+$ z toho vyplýva tvrdenie. □

9.5 Distribučná funkcia

Ak množina $v^{-1}((-\infty, x))$ patrí do $\mathcal{D}$ pre každé reálne číslo x, budeme hovoriť že postuposť $\{v(n)\}$ je $\mathcal{D}$ - **merateľná** V takom prípade sa funkcia

$$F(x) = \mathfrak{d}(v^{-1}((-\infty, x)))$$

nazýva **asymptotická distribučná funkcia** postupnosti v.

Príklad 152. Ak postupnosť $\{v(n)\}$ je rovnomerne rozdelená, tak postupnosť $\{v^2(n)\}$ má asymptotickú distribučnú funkciu $F(x) = 0$ pre $x \leq 0$,$F(x) = \sqrt{x}$ pre $x \in [0, 1]$, $F(x) = 1$ ak $x \geq 1$.

Príklad 153. Nech $\{v(n)\}$ je postupnosť prvkov intervalu $[a, b)$ a g je neklesajúca funkcia na tomto intervale, taká, že $g(a) = 0, g(b) = 1$. Ak pre každé $a_1 < b_1$ z $[a, b]$ platí $\overline{\mathfrak{d}}(v^{-1}([a_1, b_1)) \leq g(b_1) - g(a_1)$, tak $\{v(n)\}$ je $\mathcal{D}$ - merateľná postupnosť a g je jej asymptotická distribučná funkcia.

Príklad 154. Nech $\{v(n)\}$ je rovnomerne rozdelená postupnosť prvkov intervalu $(0, 1)$. Potom postupnosť zlomkových častí $\{u(n)\}$ kde $u(n) = \left\{\frac{1}{v(n)}\right\}$ je $\mathcal{D}$ meratelńá a jej asymptotická distribučná funkcia je

$$g(x) = \sum_{k=1}^{\infty} \frac{1}{k} - \frac{1}{k+x}.$$

Dá sa to dokázať tak, že si uvedomíme

$$u^{-1}([0, x)) = \bigcup_{k=1}^{\infty} v^{-1}\Big(\Big(\frac{1}{k+x}, \frac{1}{k}\Big]\Big).$$

Príklad 155. Nech $F : [0, 1] \to [0, 1]$ je rastúca spojitá funkcia, $F(0) = 0, F(1) = 1$. Postupnosť $\{v(n)\}, v(n) \in (0, 1), n \in \mathbb{N}$ je rovnomerne rozdelená práve vtedy, keď postupnosť $\{F(v(n))\}$ je $\mathcal{D}$ merateľná a jej asymptotická distribučná funkcia je F^{-1}.

Podobne ako Veta 65 sa dá dokázať:

Veta 68. Ak v je $\mathcal{D}$ ohraničená merateľná postupnosť a F je jej asymptotická distribučná, tak pre každú spojitú funnkciu f definovanú na intervale $[a,b], a, b$, ktorý obsahuje všetky hodnoty v platí

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N} f(v(n)) = \int_a^b f(x)dF(x). \tag{135}$$

Príklad 156. Podľa predošlej vety a príkladu 154 môžeme vypočítať

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\Big\{\frac{1}{v(n)}\Big\} = \int_0^1 x d\Big(\sum_{k=1}^{\infty}\frac{1}{k}-\frac{1}{k+x}\Big).$$

Ak použijeme metódu per partes, dostávame

$$\int_0^1 x d\Big(\sum_{k=1}^{\infty}\frac{1}{k}-\frac{1}{k+x}\Big) = \Big[x\Big(\sum_{k=1}^{\infty}\frac{1}{k}-\frac{1}{k+x}\Big)\Big]_0^1 - \int_0^1\Big(\sum_{k=1}^{\infty}\frac{1}{k}-\frac{1}{k+x}\Big)dx =$$

$$= 1-\sum_{k=1}^{\infty}\frac{1}{k} - [\ln(k+x)]_0^1.$$

9.6 Dualita zvyšková trieda, interval

Predpokladajme, že je daná postupnosť prirodzených čísel

$$B = \{1 = B_0 < B_1 < \cdots < B_k < \dots\},$$

pre ktorú platí $B_k | B_{k+1}$. Každé prirodzené číslo n môžeme jednoznačne vyjadriť v tvare

$$n = \sum_{k=0}^{\infty} b_k(n) B_k \tag{136}$$

pričom $0 \le b_i(n) < \frac{B_i}{B_{i+1}}$, $i = 0, \dots, k+1$, existuje také k_0, že pre $k > k_0$ platí $b_k(n) = 0$. Teda tento rad je vlastne konečný. Ak analyzujeme tento rozvoj vidíme, že

$$n \equiv b_0(n) \pmod{B_1},$$

ďalej

$$n \equiv b_0(n) + b_1(n)B_1 \pmod{B_2}.$$

Vo všeobecnosti

$$n \equiv b_0(n) + b_1(n)B_1 + \cdots + b_{k-1}(n)B_{k-1} \pmod{B_k} \tag{137}$$

pre $k = 1, 2, 3, \ldots$.

Pomocou tohoto rozvoja sa dá priradiť číslu n hodnota

$$v_B(n) = \sum_{k=0}^{\infty} \frac{b_k(n)}{B_{k+1}}. \tag{138}$$

Z podmienok pre $b_k(n)$ dostávame

$$v_B(n) < \sum_{k=0}^{\infty} \frac{\frac{B_{k+1}}{B_k} - 1}{B_{k+1}} = \sum_{k=0}^{\infty} \frac{1}{B_k} - \frac{1}{B_{k+1}} = 1.$$

To znamená, že $v_B(n) \in [0, 1]$.

Veta 69. Postupnosť v_B daná rovnosťami (136) a (138) **je rovnomerne rozdelená.**

Dokážeme to pomocou nasledujúceho faktu.

Veta 70. Nech $0 = a_1^n < a_2^n < \cdots < a_{k_n}^n = 1$, pre $n - 1, 2, 3, \ldots$ je taký systém delení intervalu $[0, 1]$, že

$$\lim_{n\to\infty} \max\{a_i^n - a_{i-1}^n; i = 2, \ldots, k_n\} = 0. \tag{139}$$

Postupnosť v, $v(n) \in [0, 1]$, je rovnomerne rozdelená práve vtedy, keď pre každé $n \in \mathbb{N}$ platí

$$\overline{\mathfrak{d}}(v^{-1}([a_i^n, a_{i+1}^n))) \leq a_{i+1}^n - a_i^n, \tag{140}$$

pre $i = 1, \ldots, k_n - 1$.

Dôkaz. Vieme, že

$$\bigcup_{i=1}^{k_n-1} v^{-1}([a_i^n, a_{i+1}^n)) = \mathbb{N}$$

pre všetky $n = 1, 2, 3, \ldots$. Z príkladu 138 potom vyplýva , že $v^{-1}([a_i^n, a_{i+1}^n)) \in \mathcal{D}$ a $\mathfrak{d}(v^{-1}([a_i^n, a_{i+1}^n)) = a_{i+1}^n - a_i^n$, pre $n \in \mathbb{N}$, $i = 1, \ldots, k_n - 1$. A teda $v^{-1}([0, a_i^n) \in \mathcal{D}$ pričom

$$\mathfrak{d}(v^{-1}([0, a_i^n))) = a_i^n,$$

pre všetky spomínané i a n. Z podmienky (139) vyplýva, že pre kaďé $x \in [0,1]$ a $\varepsilon > 0$ existuje také n a i, že $a_i^n \leq x \leq a_{i+1}^n$ pričom $a_{i+1}^n - a_i^n < \varepsilon$. To znamená $[0, a_i^n) \subset [0, x) \subset [0, a_{i+1}^n)$. Preto

$$v^{-1}([0, a_i^n)) \subset v^{-1}([0, x)) \subset v^{-1}([0, a_{i+1}^n)),$$

pričom

$$v^{-1}([0, a_{i+1}^n)) \setminus v^{-1}([0, a_i^n)) = v^{-1}([a_i^n, a_{i+1}^n)).$$

Z podmienky (140) preto dostávame

$$\mathfrak{d}(v^{-1}([0, a_{i+1}^n))) - \mathfrak{d}(v^{-1}([0, a_i^n))) < \varepsilon.$$

Tým sme dokázali $v^{-1}([0, x)) \in \mathcal{D}$ a $\mathfrak{d}(v^{-1}([0, x))_{=} x$. Rovnako sa dokáže $v^{-1}([0, x]) \in \mathcal{D}$ a $\mathfrak{d}(v^{-1}([0, x])_{=} x$. □

Aby sme mohli použiť túto vetu, budeme uvažovat postupnosť delení intervalu $[0, 1)$ definovaný pomocou postupnosti B nasledovne

$$[0,1) = \bigcup_{j=0}^{B_k - 1} \Big[\frac{j}{B_k}, \frac{j+1}{B_k}\Big),$$

pre $j \in \mathbb{N}$. Intervaly na pravej strane sa nazývajú intervaly k - **tého poradia**.

Príklad 157. Ak $B_k = 10^k, k = 1, 2, 3, \ldots$, tak intervaly prvého poradia sú

$$\Big[0, \frac{1}{10}\Big), \Big[\frac{1}{10}, \frac{2}{10}\Big), \ldots, \Big[\frac{9}{10}, \frac{10}{10}\Big).$$

Intervaly druhého poradia sú

$$\Big[0, \frac{1}{100}\Big), \Big[\frac{1}{100}, \frac{2}{100}\Big), \ldots, \Big[\frac{99}{100}, \frac{100}{100}\Big).$$

číslo $0,123$ patrí do intervalu prvého poradia $\Big[\frac{1}{10}, \frac{2}{10}\Big)$. Potom do jeho podintevalu $\Big[\frac{12}{100}, \frac{13}{100}\Big)$, potom do podintervalu $\Big[\frac{123}{100}, \frac{124}{100}\Big)$.

Na dôkaz Vety 69 stačí dokázať, že pre každé $j_k = 0, \ldots, B_k - 1$ existuje také r_k, že

$$v_B^{-1}\Big(\Big[\frac{j_k}{B_k}, \frac{j_k+1}{B_k}\Big)\Big) = r_k + (B_k). \tag{141}$$

Aby sme ukázali túto súvislosť zvyškovych tried a intervalov, využijeme to, že každé číslo $\alpha \in [0, 1)$ sa dá jednoznačne vyjadriť v tvare Cantorovho radu

$$\alpha = \sum_{k=0}^{\infty} \frac{a_k(\alpha)}{B_{k+1}}, \tag{142}$$

pričom $a_k \leq \frac{B_{k+1}}{k} - 1$ a pre nekonečne veľa k platí $a_k < \frac{B_{k+1}}{B_k} - 1$.

Veta 71. Pre každý interval k - teho poradia $\left[\frac{j_k}{B_k}, \frac{j_k+1}{B_k}\right)$ existuje taká jednoznačne určená postupnosť $s_1, \ldots, s_k$, že $\alpha \in \left[\frac{j_k}{B_k}, \frac{j_k+1}{B_k}\right)$ práve vtedy, keď $a_i(\alpha) = s_{i+1}, i = 0, \ldots, k-1$.

Dôkaz. Interval $k-1$ poriadia má dizjunktný rozklad na intervaly k - teho poradia. Teda k intervalu k - teho poradia existujú jednoznačne určené intervaly prvého až $k-1$ - ho poradia

$$\left[\frac{j_1}{B_1}, \frac{j_1+1}{B_1}\right) \supset \left[\frac{j_2}{B_2}, \frac{j_2+1}{B_2}\right) \supset \cdots \supset \left[\frac{j_k}{B_k}, \frac{j_k+1}{B_k}\right).$$

Z toho dostávame, že α je prvkom daného intervalu k - teho poradia práve vtedy keď je prvkom každého jeho nadintervalu ℓ - tého poradia.

Číslo α patrí do intervalu ℓ - tého poradia $\left[\frac{j_\ell}{B_\ell}, \frac{j_\ell+1}{B_\ell}\right)$ práve vtedy, keď $B_\ell\alpha \in [j_\ell, j_\ell+1)$. Teda $[B_\ell\alpha] = j_\ell$. Ak sa vrátime k rozvoju (142), dostávame

$$[B_\ell\alpha] = B_\ell \sum_{i=0}^{\ell-1} \frac{a_i(\alpha)}{B_{i+1}}.$$

To znamená

$$\sum_{i=0}^{\ell-1} \frac{a_i(\alpha)B_\ell}{B_{i+1}} = j_\ell.$$

Teda si môžeme vyjadriť

$$a_{\ell-1}(\alpha) = j_\ell - \sum_{i=0}^{\ell-2} \frac{a_i(\alpha)B_\ell}{B_{i+1}} \tag{143}$$

Preto $\alpha \in \left[\frac{j_1}{B_1}, \frac{j_1+1}{B_1}\right)$ práve vtedy, keď $a_0(\alpha) = j_1 := s_1$. Podobne $\alpha \in \left[\frac{j_2}{B_2}, \frac{j_2+1}{B_2}\right)$ práve vtedy

$$a_1(\alpha) = j_2 - \frac{B_2 j_1}{B_1} := s_2.$$

Takto pomocou rovnosti (143) dostaneme všetky $s_i, i = 1, \ldots, k$. □

9.7 Aditívne aritmetické funkcie

Aritmetická funkcia f sa nazýva **aditívna**, ak pre ľubovoľné $a, b \in \mathbb{N}$ platí

$$(a, b) = 1 \Longrightarrow f(ab) = f(a) + f(b). \tag{144}$$

Pál Erdös v roku 1937 dosiahol výsledky, ktoré charakterizujú rozdelenie hodnôt aditívnych funkcií na reálnej osi.

Aditívna aritmetická funkcia f sa nazýva **silno aditívna** , ak pre každé prvočíslo p a $\alpha > 0$ platí $f(p) = f(p^\alpha)$.

Veta 72. Nech f je silno aditívna aritmetická funkcia, taká že

$$\sum_p \frac{f(p)}{p} < \infty. \tag{145}$$

Potom postupnosť $\{f(n)\}$ je $\mathcal{D}$ - merateľná a jej asymptotická distribučná funkcia je spojitá.

Dôkaz bude vychádzať z nasledujúcich faktov. Silno aditívna aritmetická funkcia je jednoznačne určená hodnotami, ktoré nadobúda v prvočíselných argumentoch. Môžeme to vyjadriť

$$f(m) = \sum_{p|m} f(p). \tag{146}$$

Dôležitú úlohu bude hrať to, že takejto funkcii sa dá priradiť postupnosť periodických funkcií

$$f_n(m) = \sum_{\substack{p|m \\ p\leq n}} f(p). \tag{147}$$

pre $n \in \mathbb{N}$. Tieto funkcie sú periodické s periódou $P = p_1 p_2 \dots p_{\pi(n)}$. Táto hodnota vznikne vynásobením všetkých prvočísel, ktoré neprevyšujú n. V úvahách, ktoré povedú k dôkazu Vety 72 sa oprieme o fakt, že pre reálne číslo x si môžeme vyjadriť

$$f_n^{-1}((-\infty, x)) = \bigcup_{\substack{1\leq m\leq P \\ f_n(m)<x}} m + (P).$$

To znamená, že

$$f_n^{-1}((-\infty, x)) \in \mathcal{D}. \tag{148}$$

Lema 6. Nech f je nezáporná silno aditívna funkcia, prostá na množine prvočísel, ktorá spĺňa podmienku (145). Potom

$$\lim_{n\to\infty} \overline{\mathfrak{d}}(\{m \in; f(m) - f_n(m) > \delta\}) = 0$$

pre každé $\delta > 0$.

Dôkaz. Pre $n \in \mathbb{N}$ platí

$$f(m) - f_n(m) = \sum_{\substack{p|m \\ p>n}} f(p).$$

Označme $A_n = \{m \in; f(m) - f_n(m) > \delta\}$. Aby sme odhadli počet prvkov $A_n \cap [1, N]$ sa budeme snažiť odhadnúť počet takých $m \leq N$, že spomínaný rozdiel prevyšuje dané $\delta > 0$. Pomocou úprav dostávame

$$\sum_{m\leq N} f(m) - f_n(m) = \sum_{m\leq N} \sum_{\substack{p|m \\ p>n}} f(p) = \sum_{n<p\leq N} \sum_{kp\leq N} f(p) =$$

$$= \sum_{n<p\leq N} f(p) \sum_{kp\leq N} 1 = \sum_{n<p\leq N} f(p)\Big[\frac{N}{p}\Big].$$

To znamená

$$\sum_{m\leq N} f(m) - f_n(m) = N \sum_{n<p\leq N} \frac{f(p)}{p} + \mathcal{O}(\pi(N)).$$

Preto počet ščítancov v sume na ľavej strane, ktoré prevyšujú δ, nemôže prevyšovať hodnotu

$$\frac{N}{\delta} \sum_{n<p\leq N} \frac{f(p)}{p} + \mathcal{O}(\pi(N)).$$

Teda

$$\frac{1}{N}|A_n \cap [1, N]| \leq \frac{1}{\delta} \sum_{n<p} \frac{f(p)}{p} + \mathcal{O}\Big(\frac{\pi(N)}{N}\Big).$$

Ak zoberieme do úvahy odhad pre prvočíselnú funkciu podľa Čebyševovych nerovností , dostávame z poslednej nerovnosti

$$\overline{\mathfrak{d}}(A_n) \leq \frac{1}{\delta} \sum_{n<p} \frac{f(p)}{p}.$$

Preto z podmienky (145) vyplýva $\lim_{n\to\infty} \overline{\mathfrak{d}}(A_n) = 0$. □

Lema 7. Nech f je nezáporná aditívna aritmetická funkcia, ktorá je prostá na množine prvočísel Potom pre každé $\varepsilon > 0$ existuje také $\delta > 0$, že pre každý interval I platí

$$|I| < \delta \Longrightarrow \overline{\mathfrak{d}}(f^{-1}(I)) < \varepsilon.$$

Dôkaz. Predpokladajme, že $q_1 < \cdots < q_s$ sú rôzne prvočísla. Uvažujme interval I taký, že $|I| < \delta$. Ľubovoľnú množinu A môžeme pokryť takto

$$A \subset \Big(A \cap \bigcup_{i=1}^{s}(q_i) \setminus (q_i^2)\Big) \cup \Big(\mathbb{N} \setminus \Big(\bigcup_{i=1}^{s}(q_i) \setminus (q_i^2)\Big).$$

Z toho vyplýva podľa Vety 61

$$\overline{\mathfrak{d}}(A) \leq \overline{\mathfrak{d}}\Big(A \cap \Big(\bigcup_{i=1}^{n}(q_i) \setminus (q_i^2)\Big)\Big) + \prod_{i=1}^{n}\Big(1 - \frac{1}{q_i} + \frac{1}{q_i^2}\Big). \tag{149}$$

Rad prevrátených hodnôt prvočísel diverguje. Prvočísla $q_1, \ldots, q_s$ môžeme preto podľa (129) vybrať tak, že druhý sčítanec v poslednej nerovnosti je ľubovoľne blízko k 0.

Funkcia f je prostá na množine prvočísel. Môžeme preto zvoliť kladné číslo δ také, že

$$\delta < \min\{|f(q_i) - f(q_j)|; i \neq j, i, j = 1, \ldots, n\}.$$

Nech I je taký interval, že $|I| < \delta$. Položme $A = f^{-1}(I)$. Označme sčítanec na pravej strane (149) symbolom A_1. Každý prvok A_1 sa dá vyjadriť v tvare $q_j n$ pričom $(q_j, n) = 1$. Nech $m_1, \ldots, m_k$ sú rôzne prvky A_1. Ak $q_j | m_i, q_j | m_\ell$, tak

$$\frac{m_i}{q_j} \neq \frac{m_\ell}{q_j}.$$

Predpokladajme, že

$$\frac{m_i}{q_j} = \frac{m_\ell}{q_k}.$$

pre $j \neq k$. Potom by platilo

$$f\Big(\frac{m_i}{q_j}\Big) = f\Big(\frac{m_\ell}{q_k}\Big).$$

To znamená

$$f(m_i) - f(q_j) = f(m_\ell) - f(q_k).$$

Teda po úprave

$$f(m_i) - f(m_\ell) = f(q_j) - f(q_k).$$

To nemôže nastať, lebo $m_i, m_\ell \in f^{-1}(I)$ a teda $|f(m_i) - f(m_\ell)| < \delta$. To znamená, že ak každé z čísel m_i vydelíme tým q_{j_i}, ktoré je jeho deliteľom,

dostávame K rôznych prirodzených čísel $\frac{m_i}{q_{j_i}}$. Ak $N \in \mathbb{N}$ a predpokladáme $m_i \leq N, i = 1, \ldots, K$, tak

$$\frac{m_i}{q_{j_i}} \leq \frac{N}{q_{j_i}} \leq \frac{N}{q_1}.$$

Preto $K \leq \frac{N}{q_1}$. Tým sme dokázali

$$|A_1 \cap [1, N]| \leq \frac{N}{q_1}.$$

To znamená $\overline{\mathfrak{d}}(A_1) \leq \frac{1}{q_1}$. Vidíme, že vhodnou voľbou q_1 a potom $q_2, \ldots, q_n$ dosiahneme $\overline{\mathfrak{d}}(A) < \varepsilon$. □

Dôkaz vety 72 . Stačí dokázať, že pre $x \in \mathbb{R}$ platí

$$f^{-1}([x, \infty)) = \mathbb{N} \setminus f^{-1}(-\infty, x)) \in \mathcal{D}$$

Pre každé n a $m \in \mathbb{N}$ platí $f_n(m) \leq f(m)$. Preto

$$f^{-1}([x, \infty)) \subset f_n^{-1}([x, \infty)). \tag{150}$$

Množinový rozdiel si môžeme vyjadriť

$$f^{-1}([x, \infty)) \setminus f_n^{-1}([x, \infty)) = \{m \in \mathbb{N}; f(m) \geq x \wedge f_n(m) < x\} \subset$$

$$\subset f^{-1}([x, x + \delta)) \cup \{m; f(m) - f_n(m) > \delta\},$$

pre každé $\delta > 0$. Zvoľme pre dané $\varepsilon > 0$ také $\delta > 0$ aby platila implikácia z Lemy 7. Potom platí

$$\overline{\mathfrak{d}}(f^{-1}([x, \infty)) \setminus f_n^{-1}([x, \infty))) \leq$$

$$\leq \overline{\mathfrak{d}}(f^{-1}([x, x + \delta))) + \overline{\mathfrak{d}}(\{m; f(m) - f_n(m) > \delta\}) \leq$$

$$\leq \varepsilon + \overline{\mathfrak{d}}(\{m; f(m) - f_n(m) > \delta\}).$$

Druhý sčítanec konverguje do 0 pre $n \to \infty$ a teda $f^{-1}([x, \infty)) \in \mathcal{D}$. □

9.8 Nivenova veta

Pre štúdium množín, ktoré majú asymptotickú hustotu 0, a ktoré sú spojené s deliteľnosťou, má veľký význam výsledok Ivana Nivena z roku 1951.

Nech $S \subset \mathbb{N}$. Označme pre dané prvočíslo p symbolom S_p množinu tých prvkov S, ktoré sú deliteľné p a nie sú deliteľné p^2. Nivenov výsledok znie

Veta 73. Ak $p_1, p_2, \ldots, p_k \ldots$ **je taká postupnosť prvočísel, že**

$$\sum_{k=1}^{\infty} \frac{1}{p_k} = \infty, \tag{151}$$

tak $\mathfrak{d}(S) = 0$ **práve vtedy, keď** $\mathfrak{d}(S_{p_k}) = 0$ **pre všetky** $k = 1, 2, 3, \ldots$.

Dôkaz. Pre prvočíslo p platí $S_p = S \cap ((p) \setminus (p^2))$. Teda

$$S \subset \bigcup_{j=1}^{n} S_{p_j} \cup \Big(\mathbb{N} \setminus \bigcup_{j=1}^{n} (p_j) \setminus (p_j^2)\Big).$$

Z toho vyplýva

$$\overline{\mathfrak{d}}(S) \leq \prod_{j=1}^{n} \Big(1 - \frac{1}{p_j} + \frac{1}{p_j^2}\Big).$$

Z predpokladu o divergencii spomínaného radu dostávame, že výraz na pravej strane poslednej nerovnosti konverguje do 0 a teda $\mathfrak{d}(S) = 0$. □

Príklad 158. Ak S bude označovať množinu takých prirodzených čísel $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ takých, že všetky exponenty α_i sú väčšie ako 1, tak podľa predošlej vety platí $\mathfrak{d}(S) = 0$.

Nasledujúca vlastnosť asymptotickej hustoty vyplýva priamo z definície alebo z Vety 112.

Veta 74. Ak $S \in \mathcal{D}$ **a** $m \in \mathbb{N}$**, tak aj množina** $mS = \{ms; s \in S\}$ **patrí do** $\mathcal{D}$ **a**

$$\mathfrak{d}(mS) = \frac{\mathfrak{d}(S)}{m}.$$

Označme symbolom $M(k)$ množinu tých prirodzených čísel, ktoré majú najviac k prvočísel v kánonickom rozklade.

Propozícia 3. Pre $k \in \mathbb{N}$ **platí** $M(k) \in \mathcal{D}$ **a** $\mathfrak{d}(M(k)) = 0$**.**

Dôkaz. Budeme postupovať indukciou podľa k. $M(1) = \{p^\alpha; p \in P, \alpha \in \mathbb{N}\}$. Pre každé prvočíslo p teda platí

$$M(1)_p = \{p\}.$$

Preto $\mathfrak{d}(M(1)_p)) = 0$, podľa Vety 73 dostávame $\mathfrak{d}(M(1) = 0$. Predpokladajme, že $\mathfrak{d}(M(k-1)) = 0$. Stačí si uvedomiť , že pre kaďé prvočíslo p platí

$$M(k)_p \subset pM(k-1).$$

Teda podľa Vety 74 dostávame $\mathfrak{d}(M(k)_p) \leq \frac{1}{p}\mathfrak{d}(M(k-1)) = 0$. Z Vety 73 vyplýva $\mathfrak{d}(M(k)) = 0$. □

V práci Novoselova z roku 1961 je dokázané:

Propozícia 4. Nech $\{p_n\}$ je postupnosť prvočísel, ktorá spĺňa podmienku (151). Nech $S \subset \mathbb{N}$ je nekonečná množina. Pre každé $s \in S$ definujme $q_s = \min\{p_j; p_j|s\}$, ak niektoré z prvočísel delí dané s. V opačnom prípade $q_s = s$. Ak

$$\lim_{s\in S} q_s = \infty \tag{152}$$

tak $S \in \mathcal{D}$ a $\mathfrak{d}(S) = 0$.

Dôkaz. Z podmienky (152) vyplýva, že množina S_{p_n} je konečná pre každé n a teda tvrdenie vyplýva z Vety 73. □

Každé prirodzené číslo n sa dá jednoznačne vyjadriť v tvare kánonického rozkladu $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Označme symbolom $N(s)$, $s = 0, 1, 2, \dots$ množinu takých prirodzených čísel n, ktoré v kánonickom rozklade majú najviac s nepárnych exponentov $\alpha_i, i = 1, \dots, k$. Napríklad $N(0) = \{n^2; n \in \mathbb{N}\}$.

Propozícia 5. Pre každé $s \in \mathbb{N}$ platí , $N(s) \in \mathcal{D}$ a $\mathfrak{d}(N(s)) = 0$.

Dôkaz. Budeme postupovať indukciou podľa s.

Uvažujme prvočíslo p. Ak $a \in N(1)_p$, tak $a = pm^2, (m, p) = 1$, kde $m \in \mathbb{N}$. To znamená $N(1)_p \subset p\mathbb{N}^2$. Preto z Vety 74 vyplýva $\mathfrak{d}(N(1)_p) = 0$. Pretože p je ľubovolné prvočíslo, dostávame z Vety 73, že $\mathfrak{d}(N(1)) = 0$.

Predpokladajme, že tvrdenie platí pre $s-1$. Ak $a \in N(s)_p$ tak $a = pn, (p, n) = 1$, pričom pn nemá viac ako s prvočísel s nepárnym exponentom v kánonickom rozklade. Potom ale n nemá viac ako $s-1$ prvočísel so nepárnym exponentom v kánonickom rozklade. Teda $n \in N(s-1)$. Teda platí $N(s)_p \subset pN(s-1)$. Teda podľa indukčného predpokladu $\mathfrak{d}(N(s)) = \frac{1}{p}\mathfrak{d}(N(s-1)) = 0$. Znovu podľa Vety 73 dostávame $\mathfrak{d}(N(s)) = 0$. □

Študent FMFI UK Viliam Furík študoval množinu

$$T = \{n \in \mathbb{N}; \tau(n)|n\}.$$

Propozícia 6. $T \in \mathcal{D}$ **a** $\mathfrak{d}(T) = 0$.

Dôkaz. Množinu T môžeme rozložiť

$$T = (T \cap N(s)) \cup (T \cap (\mathbb{N} \setminus N(s)), s \in \mathbb{N}. \tag{153}$$

Podľa predošlej propozície platí

$$\mathfrak{d}((T \cap N(s))) = 0.$$

Z (153) teda dostávame

$$\overline{\mathfrak{d}}(T) \leq \overline{\mathfrak{d}}(T \cap (\mathbb{N} \setminus N(s)). \tag{154}$$

Ak $n \in T \cap (\mathbb{N} \setminus N(s))$, tak n obsahuje aspoň $s+1$ prvočísel v kánonickom rozklade. Z podmienky $\tau(n)|n$ teda vyplýva $2^{s+1}|n$. Preto $T \cap (\mathbb{N} \setminus N(s)) \subset (2^{s+1})$. Teda z (154) vyplýva $\overline{\mathfrak{d}}(T) \leq \frac{1}{2^{s+1}}$. Pretože s je ľubovoľné dostávame nakoniec $\mathfrak{d}(T) = 0$. □

Štefan Porubský v roku 1978 dokázal pomocou Vety 73 tento výsledok:

Veta 75. Nech je daná celočíselná aritmetická funkcia g a dve celočíselné multiplikatívne aritmetické funkcie f_1, f_2. Prepokladajme, že existuje postupnosť prvočísel $p_1 < p_2 < p_3 < \cdots < p_n < \ldots$ taká, že

$$\sum_{n=1}^{\infty} \frac{1}{p_n} = \infty$$

pre ktorú platí

$$f_1(p_k) \nmid g(n),\ k = 1, 2, 3, \ldots,\ n \in \mathbb{N}. \tag{155}$$

Ďalej predpokladajme, že pre každé k existuje postupnosť prvočísel $q_{k,j}$, že $f_1(p_k)|f_2(q_{k,j})$ a

$$\sum_{j=1}^{\infty} \frac{1}{q_{k,j}} = \infty.$$

Definujme si množinu

$$S = \{n \in \mathbb{N}; (f_1(n), f_2(n)) = g(n)\}.$$

Potom $S \in \mathcal{D}$ a $\mathfrak{d}(S) = 0$.

Dôkaz. Pre každé k platí

$$S_{p_k} = \{p_k m; (p_k, m) = 1 \wedge (f_1(p_k)f_1(m), f_2(p_k)f_2(m)) = g(p_k m)\} =$$

$$= p_k\{m; (p_k, m) = 1 \wedge (f_1(p_k)f_1(m), f_2(p_k)f_2(m)) = g(p_k m)\} := p_k S^{(k)}.$$

Ak by existovalo prirodzené číslo $m \in S^{(k)}_{q_{ki}}$, tak $m = q_{ki}m_1$. Potom

$$(f_1(p_k)f_1(q_{ki})f_1(m_1)), f_2(p_k)f_2(q_{ki})f_2(m_1))) = g(p_k m).$$

A teda z podmienky $f_1(p_k)|f_2(q_{ki})$ dostávame $f_1(p_k)|g(p_k m)$ a to je spor s predpokladom (155). Preto $S^{(k)}_{q_{ki}} = \emptyset$, teda $\mathfrak{d}(S_{p_k}) = 0$, teda podľa Vety 73 dostávame $\mathfrak{d}(S) = 0$. □

Propozícia 7. Pre každé celé číslo c platí , že množina

$$S = \{n \in \mathbb{N}; (\varphi(n), \sigma(n)) = c\}$$

patrí do $\mathcal{D}$ a $\mathfrak{d}(S) = 0$.

Dôkaz. Pre všetky prvočísla p, až na konečný počet platí $\varphi(p) = p-1 \nmid c$. Ak p, q sú prvočísla, tak podmienka $\varphi(p)|\sigma(q)$ znamená $p-1|q+1$. Teda $q+1 = k(p-1)$. Čo je to isté, ako $q = k(p-1)-1$. Podľa Dirichletovej vety existuje taká postupnosť prvočísel $q_k = k(p-1)-1$, že

$$\sum_{k=1}^{\infty} \frac{1}{q_k} = \infty.$$

Z toho, že q_k je prvočíslo, vyplýva $\sigma(q_k) = q_k+1 = k(p-1)$. Preto $\varphi(p)|\sigma(q_k)$. Vidíme, že sú splnené všetky podmienky Vety 75. □

9.9 Direktný rozklad

V tejto časti sa budeme venovať štrukturálnemu výsledku, ktorý dokázal v roku 1976 Saffari.

Nech $A, B \subset \mathbb{N}$. Hovoríme, že tieto množiny tvoria **direktný rozklad** $\mathbb{N}$, ak sa každé prirodzené číslo dá vyjadriť jediným spôsobom v tvare $ab, a \in A, b \in B$. Zapisujeme to

$$A \odot B = \mathbb{N}. \tag{156}$$

Množiny A, B sa nazývajú v tomto prípade **direktné faktory.**

Príklad 159. Ak $A = \{2^k; k = 0, 1, 2, 3, \dots\}$ a B je množina nepárnych prirodzených čísel, tak $\mathbb{N} = A \odot B$.

Veta 76. Ak platí (156) **, tak $A \in \mathcal{D}$ a**

$$\mathfrak{d}(A) = \Big(\sum_{b \in B} \frac{1}{b}\Big)^{-1}.$$

Rovnosť (156) si môžeme vyjadriť aj v tvare

$$\mathbb{N} = \bigcup_{b\in B} bA, \tag{157}$$

pričom rozklad na pravej strane je dizjunktný.

Príklad 160. Ak platí (156) a $A \in \mathcal{D}$, tak

$$\mathfrak{d}(A) = \Big(\sum_{b\in B} \frac{1}{b}\Big)^{-1}.$$

Z tohoto príkladu vidíme, že stačí dokázať $A \in \mathcal{D}$. Takto postupoval Saffari s využitím nasledujúceho príkladu.

Príklad 161. Ďalším príkladom direkného rozkladu je

$$\mathbb{N} = Q_k \odot \mathbb{N}^k,$$

kde $\mathbb{N}^k = \{n^k; n \in \mathbb{N}\}$.

My takto postupovať nebudeme. Dôkaz vety 76, ktorý uvedieme, je zjednodušený dôkaz tejto vety. Publikoval ho v roku 1979 H. Daboussi.

Z (157) vyplýva, že pre každé $N \in \mathbb{N}$ platí

$$[1, N] \cap \mathbb{N} = \bigcup_{\substack{b\in B\\ b\le N}} [1, N] \cap bA.$$

Z dizjunktnosti tohoto rozkladu preto dostávame

$$N = \sum_{\substack{b\in B\\ b\le N}} |[1, N] \cap bA|.$$

Teda

$$N = \sum_{\substack{b\in B\\ b\le N}} \Big|\Big[1, \frac{N}{b}\Big] \cap A\Big|. \tag{158}$$

Postupne budeme vnášať jasno do poslednej rovnosti. Začneme prípravnými úvahami. Funkcia $\mathbf{C}_S$, pre $S \subset \mathbb{N}$, definovaná rovnosťami :

$$\mathbf{C}_S(n) = 1 \text{ pre } n \in S \text{ a } \mathbf{C}_S(n) = 0 \text{ pre } n \notin S,$$

sa nazýva **charakteristická funkcia** množiny S. Pomocou nej si môžeme vyjadriť

$$\frac{|[1, N] \cap S|}{N} = \frac{1}{N} \sum_{n=1}^{N} \mathbf{C}_S(n).$$

Rovnosť (156) je ekvivalentná rovnosti

$$\mathbf{C}_A * \mathbf{C}_B = 1. \tag{159}$$

Ak $y > 0$, tak symbolom G_y označíme množinu takých prirodzených čísel, ktoré obsahujú v kánonickom rozklade iba prvočísla menšie ako y. Symbolom H_y označíme množinu tých prirodzených čísel, ktoré obsahujú v kánonickom zase rozklade iba prvočísla väčšie alebo rovné y. Každé prirodzené číslo n si môžeme pomocou kánonického rozkladu vyjadriť jednoznačne v tvare $n_1 n_2$, $n_1 \in G_y$, $n_2 \in H_y$. To znamená

$$\mathbb{N} = G_y \odot H_y.$$

Preto, ak pre jednodušenie označíme $f_y = \mathbf{C}_{G_y}$, $h_y = \mathbf{C}_{H_y}$, tak

$$f_y * h_y = 1.$$

Rad $\sum_{k=1}^{\infty} \frac{f_y(k)}{k}$ konverguje a platí

$$\sum_{k=1}^{\infty} \frac{f_y(k)}{k} = \prod_{p<y} \Big(1 - \frac{1}{p}\Big)^{-1} \tag{160}$$

Z rovnosti (159) dostávame $f_y = (f_y \mathbf{C}_A) * (f_y \mathbf{C}_B)$. Preto

$$\sum_{k=1}^{\infty} \frac{f_y(k)}{k} = \Big(\sum_{a\in A} \frac{f_y(a)}{a}\Big)\Big(\sum_{b\in B} \frac{f_y(b)}{b}\Big).$$

Z vety 61 dostávame, že $H_y \in \mathcal{D}$ a

$$\mathfrak{d}(H_y) = \prod_{p\le y} \Big(1 - \frac{1}{p}\Big).$$

Preto z (160) vyplýva

$$\mathfrak{d}(H_y) = \Big(\sum_{k=1}^{\infty} \frac{f_y(k)}{k}\Big)^{-1} = \Big(\sum_{a\in A} \frac{f_y(a)}{a}\Big)^{-1}\Big(\sum_{b\in B} \frac{f_y(b)}{b}\Big)^{-1}.$$

A teda

$$\Big(\sum_{a\in A} \frac{f_y(a)}{a}\Big)\mathfrak{d}(H_y) = \Big(\sum_{b\in B} \frac{f_y(b)}{b}\Big)^{-1}. \tag{161}$$

Kľúčovú úlohu bude hrať aritmetická funkcia

$$c_y = (f_y \mathbf{C}_A) * h_y$$

pre $y > 0$.

Lema 8.

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}c_y(n)=\Big(\sum_{b\in B}\frac{f_y(b)}{b}\Big)^{-1}.$$

Dôkaz. Z definície funkcie c_y vyplýva

$$\sum_{n\le N}c_y(n)=\sum_{n\le N}\sum_{d|n}f_y(d)\mathbf{C}_A(d)h_y\Big(\frac{n}{d}\Big)=\sum_{kd\le N}f_y(d)\mathbf{C}_A(d)h_y(k)=$$

$$\sum_{d\le N}\sum_{k\le\frac{N}{d}}f_y(d)\mathbf{C}_A(d)h_y(k)=\sum_{d\le N}f_y(d)\mathbf{C}_A(d)\sum_{k\le\frac{N}{d}}h_y(k)=$$

$$=\sum_{\substack{d\le N\\ d\in A}}f_y(d)\sum_{k\le\frac{N}{d}}h_y(k).$$

Preto

$$\frac{1}{N}\sum_{n=1}^{N}c_y(n)=\sum_{\substack{a\le N\\ a\in A}}\frac{f_y(a)}{a}\frac{a}{N}\sum_{k\le\frac{N}{a}}h_y(k)=.$$

$$=\sum_{\substack{a\le\sqrt{N}\\ a\in A}}\frac{f_y(a)}{a}\frac{a}{N}\sum_{k\le\frac{N}{a}}h_y(k)+\sum_{\substack{\sqrt{N}<a\le N\\ a\in A}}\frac{f_y(a)}{a}\frac{a}{N}\sum_{k\le\frac{N}{a}}h_y(k).\qquad(162)$$

Druhá suma konverguje do 0 ak $N\to\infty$. Označme si

$$\delta_{a,N}=\frac{a}{N}\sum_{n\le\frac{N}{a}}h_y(n).$$

Pre $\varepsilon>0$ existuje také N_0, že pre $N>N_0$ a $a\le\sqrt{N}$ platí

$$|\mathfrak{d}(H_y)-\delta_{a,N}|<\varepsilon.$$

Preto keď analyzujeme prvú sumu v (162), dostávame

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}c_y(n)=\Big(\sum_{a\in A}\frac{f(a)}{a}\Big)\mathfrak{d}(H_y)=\Big(\sum_{b\in B}\frac{f(b)}{b}\Big)^{-1},$$

pričom poslednú rovnosť sme dostali podľa (161). □

V súvislosti s touto lemou bude dôležitý nasledujúci fakt. Pre každé $N\in\mathbb{N}$ existuje také $y>0$, že $\{1,\dots,N\}\subset G_y$. Z toho vyplýva

$$\lim_{y\to\infty}\sum_{b\in B}\frac{f_y(b)}{b}=\sum_{b\in B}\frac{1}{b}.\qquad(163)$$

Lema 9. Pre každé $M \in \mathbb{N}$ a $y > 0$ platí

$$|[1, M] \cap A| \leq \sum_{n=1}^{M} c_y(n).$$

Dôkaz. Platí

$$(f_y \mathbf{C}_A) * (f_y \mathbf{C}_B) * h_y = 1. \tag{164}$$

Aby sme sa v tom ľahšie orientovali si stačí uvedomiť, že

$$(g_1 * g_2 * g_3)(n) = \sum_{d_1 d_2 d_3 = n} g_1(d_1) g_2(d_2) g_3(d_3)$$

pre aritmetické funkcie g_1, g_2, g_3 a $n \in \mathbb{N}$. Rovnosť (164) potom môžeme vyjadriť

$$\sum_{\substack{abc=n \\ a \in A, b \in B}} f_y(a) f_y(b) h_y(c) = 1$$

Preto

$$\sum_{n \leq M} \mathbf{C}_A(n) = \sum_{n \leq M} \mathbf{C}_A(n) \sum_{\substack{abc=n \\ a \in A, b \in B}} f_y(a) f_y(b) h_y(c) =$$

$$\sum_{\substack{a \in A \\ a \leq M}} f_y(a) \sum_{c \leq \frac{M}{a}} h_y(c) \sum_{\substack{b \leq \frac{M}{ac} \\ b \in B}} f_y(b) \mathbf{C}_A(abc).$$

Dokážeme, že posledná suma má najviac jeden nenulový ščítanec. Nech $ab_1c = a_1 \in A$ a súčasne $ab_2c = a_2 \in A$, $b_1, b_2 \in B$. Potom

$$\frac{a_2}{b_2} = \frac{a_1}{b_1}.$$

Teda

$$a_2 b_1 = a_1 b_2$$

Z toho, že každé prirodzené číslo sa v takom tvare dá vyjadriť jediným spôsobom vyplýva $a_1 = a_2, b_1 = b_2$. Preto

$$\sum_{n \leq M} \mathbf{C}_A(n) \leq \sum_{\substack{a \in A \\ a \leq M}} f_y(a) \sum_{c \leq \frac{M}{a}} h_y(c) = \sum_{\substack{a \in A \\ ac \leq M}} f_y(a) h_y(c) = \sum_{n \leq M} c_y(n).$$

□

Z lemy **??** a lemy 8 dostávame

$$\overline{\mathfrak{d}}(A) \leq \Big(\sum_{b\in B} \frac{f_y(b)}{b}\Big)^{-1}$$

pre $y > 0$. Preto ak zoberieme do úvahy (163) dostávame

$$\overline{\mathfrak{d}}(A) \leq \Big(\sum_{b\in B} \frac{1}{b}\Big)^{-1} \tag{165}$$

Skôr ako začneme dôkaz vety 76 definujeme

$$\underline{\mathfrak{d}}(S) = \liminf_{N\to\infty} \frac{[1,N]\cap S}{N},$$

pre $S \subset \mathbb{N}$. Táto hodnota sa nazýva **dolná asymptotická hustota** množiny S. Je zrejmé, že platí

$$S \in \mathcal{D} \Leftrightarrow \underline{\mathfrak{d}}(S) = \overline{\mathfrak{d}}(S)(= \mathfrak{d}(S)).$$

Dôkaz vety 76. Z rovnosti (158) si môžeme vyjadriť

$$\frac{|[1,N]\cap A|}{N} = 1 - \frac{1}{N} \sum_{\substack{1<b\leq N\\ b\in B}} \Big|[1,\frac{N}{b}]\cap A\Big| =$$

$$= 1 - \sum_{\substack{1<b\leq N\\ b\in B}} \frac{1}{b}\frac{b}{N}\Big|[1,\frac{N}{b}]\cap A\Big|.$$

Podľa Lemy 9 dostávame

$$1 - \sum_{\substack{1<b\leq N\\ b\in B}} \frac{1}{b}\frac{b}{N} \sum_{n\leq \frac{b}{N}} c_y(n) \leq \frac{|[1,N]\cap A|}{N}. \tag{166}$$

Ak rad $\sum_{b\in B} \frac{1}{b}$ diverguje, tak podľa Lemy 9 dostávame $A \in \mathcal{D}$ a $\mathfrak{d}(A) = 0$. Môžeme preto predpokladať, že tento rad konverguje. Z nerovností (166) pre $N \to \infty$ potom dostávame

$$1 - \Big(\sum_{b\in B} \frac{1}{b} - 1\Big)\Big(\sum_{b\in B} \frac{f_y(b)}{b}\Big)^{-1} \leq \underline{\mathfrak{d}}(A) \leq \overline{\mathfrak{d}}(A).$$

Výrazy na pravej strane posledných nerovností nezávisia na y. Ak $y \to \infty$, tak

$$1 - \Big(\sum_{b\in B}\frac{1}{b} - 1\Big)\Big(\sum_{b\in B}\frac{1}{b}\Big)^{-1} \le \underline{\mathfrak{d}}(A) \le \overline{\mathfrak{d}}(A).$$

Po roznásobení a úprave dostávame

$$\Big(\sum_{b\in B}\frac{1}{b}\Big)^{-1} \le \underline{\mathfrak{d}}(A) \le \overline{\mathfrak{d}}(A).$$

Z nerovnosti (165) nakoniec vyplýva tvrdenie vety 76. □

Príklad 162. Uvažujme množinu $S \subset \mathbb{N}$, ktorá obsahuje prirodzené čísla, ktoré majú 2 v kánonickom rozklade s párnym exponentom. Potom platí

$$\mathbb{N} = S \cup 2S,\ S \cap 2S = \emptyset.$$

Teda $\mathbb{N} = S \odot \{1, 2\}$. Podľa vety 76 dostávame $S \in \mathcal{D}$ a $\mathfrak{d}(S) = (1 + \frac{1}{2})^{-1}$.

Príklad 163. Nech p je prvočíslo a $k \in \mathbb{N}$. Označme v tomto príklade symbolom S množinu takých prirodzených čísel n, že $k|\alpha_p(n)$. Potom

$$\mathbb{N} = S \cup pS \cup \cdots \cup p^{k-1}S,$$

pričom tento rozklad je dizjunktný. Teda $\mathbb{N} = S \odot \{1, \ldots, p^{k-1}\}$. To znamená $S \in \mathcal{D}$ a

$$\mathfrak{d}(S) = \Big(\sum_{i=0}^{k-1}\frac{1}{p^i}\Big)^{-1} = \frac{p^k - p}{p^k - 1}.$$

Príklad 164. Podobne sa dá dokázať : Nech $\{p_i\}$ je daná konečná alebo nekonečná množina prvočísel a k nim priradená množina prirodzených čísel $\{k_i\}$. Ak $S \subset \mathbb{N}$ je množina takých prirodzených čísel n, že $k_i|\alpha_{p_i}(n)$ tak $S \in \mathcal{D}$ a

$$\mathfrak{d}(S) = \prod_i \frac{p_i^{k_i} - p_i}{p_i^{k_i} - 1}.$$

Príklad 165. Nech platí označenie ako v predošlom príklade. Predpokladajme naviac že je daná množina $\{r_i\}$, $0 \le r_i \le k_i - 1$. Označme

$$S_1 - \{n \in \mathbb{N}; \alpha_{p_i}(n) \equiv r_i \pmod{k_i}\}.$$

Potom $S_1 \in \mathcal{D}$ a

$$\mathfrak{d}(S) = \prod_i \frac{p_i^{k_i} - p_i}{p_i^{r_i}(p_i^{k_i} - 1)}.$$

9.10 Štatistická konvergencia

Tento pojem zaviedol Fast. Hovoríme, že postupnosť $\{v(n)\}$ **štatisticky konverguje** ku hodnote α, ak pre každé $\varepsilon > 0$ množina $v^{-1}((\alpha-\varepsilon, \alpha+\varepsilon))$ je $\mathcal{D}$ - merateľná a

$$\mathfrak{d}(v^{-1}((\alpha-\varepsilon, \alpha+\varepsilon)) = 1.$$

Zapisujeme to

$$\lim - stat_{n\to\infty} v(n) = \alpha.$$

Spomínanú množinu si môžeme vyjadriť aj v tvare

$$v^{-1}((\alpha-\varepsilon, \alpha+\varepsilon)) = \{n \in \mathbb{N}; |v(n) - \alpha| < \varepsilon\}.$$

Príklad 166. V prípade, že $\lim_{n\to\infty} v(n) = \alpha$ platí , že pre každé $\varepsilon > 0$ množina $v^{-1}((\alpha-\varepsilon, \alpha+\varepsilon))$ obsahuje všetky prirodzené čísla až na konečný počet.

V roku 1980 Tibor Šalát dokázal nasledujúcu charakteristiku štatistikej konvergencie:

Veta 77. Postupnosť $\{v(n)\}$ konverguje štatisticky k danej hdnote α práve vtedy, keď existuje množina $A \subset \mathbb{N}$, $A \in \mathcal{D}$, $\mathfrak{d}(A) = 1$ taká, že $\lim_A v(n) = \alpha$.

Táto veta vyplynie z nasledujúceho všeobecnejšieho výsledku. V jeho formulácii bude hrať dôležitú úlohu nasledujúci symbol: $A \prec B$ budeme označovať skutočnosť, že množina $A \setminus B$ je konečná. Inými slovami : najviac konečne veľa prvkov množiny A nepatrí do množiny B.

Príklad 167. Ak A, B sú konečné množiny, tak $A \prec B$ a $B \prec A$. Špeciálne $A \prec \emptyset$.

Príklad 168. Dá sa dokázať, že

$$A_1 \prec B_1, A_2 \prec B_2 \Rightarrow A_1 \cup A_2 \prec B_1 \cup B_2.$$

Ale pozor! Vo všeobecnosti neplatí

$$\bigcup_{i=1}^{\infty} A_i \prec \bigcup_{i=1}^{\infty} B_i$$

v prípade $A_i \prec B_i$.

Veta 78. Ak $B_1 \subset B_2 \subset B_3 \subset \cdots \subset B_k \ldots$ sú množiny patriace do $\mathcal{D}$ a $\mathfrak{d}(B_k) = 0$, tak existuje množina $B \in \mathcal{D}$, $\mathfrak{d}(B) = 0$ a $B_k \prec B$ pre všetky $k = 1, 2, 3, \ldots$.

Dôkaz. Z podmienky $\mathfrak{d}(B_k) = 0, k \in \mathbb{N}$ dostávame, že pre každé $k \in \mathbb{N}$ existuje také N_k, že pre $N \geq N_k$ platí

$$\frac{|[1, N] \cap B_k|}{N} \leq \frac{1}{k}. \tag{167}$$

Bez ujmy na všebecnosti môžeme predpokladať, že $N_{k+1} > N_k, k \in \mathbb{N}$. Označme teraz

$$B'_k = B_k \setminus [1, N_k].$$

Množinu B, ktorej existenciu dokazujeme, si definujeme takto

$$B = \bigcup_{k=1}^{\infty} B'_k.$$

Pre každé k platí $B_k \prec B'_k \subset A$. Preto stačí už iba dokázať, že $B \in \mathcal{D}$ a $\mathfrak{d}(B) = 0$.

Zvoľme nejaké N_k. Ak $N > N_k$, a $n \geq N$ $n \notin A'_j, j > k$. To znemená, že

$$B \cap [1, N] \subset B'_k \cap [1, N_k].$$

Pre $N > N_k$ existujé také $\ell > k$, že $N_\ell \leq N < N_{\ell+1}$. Z toho vyplýva

$$B \cap [1, N] \subset B'_\ell \cap [1, N_\ell].$$

Preto podľa (167) dostávame

$$\frac{|B \cap [1, N]|}{N} \leq \frac{|B'_\ell \cap [1, N_\ell]|}{N_j} < \frac{1}{\ell} < \frac{1}{k}.$$

Tým sme dokázali

$$\lim_{N \to \infty} \frac{|B \cap [1, N]|}{N} = 0,$$

a teda $\mathfrak{d}(B) = 0$. □

Príklad 169. Dá sa dokázať: Ak $A_1 \supset A_2 \supset A_3 \supset \cdots \supset A_k \subset \ldots$ sú množiny patriace do $\mathcal{D}$ a $\mathfrak{d}(A_k) = 1, k \in \mathbb{N}$, tak existuje množina $A \in \mathcal{D}$ taká, že $\mathfrak{d}(A) = 1$ a $A \prec A_k, k = 1, 2, 3, \ldots$.

Dôkaz vety 77. Nech $A \subset \mathbb{N}$, $\mathfrak{d}(A) = 1$ a $\lim_A v(n) = \alpha$. Potom pre každé $\varepsilon > 0$ existuje také $n_0 > 0$, že pre $n > n_0, n \in A$ platí $|v(n) - \alpha| < \varepsilon$. Z toho vyplýva $A \setminus [1, n_0] \subset v^{-1}((\alpha - \varepsilon, \alpha + \varepsilon))$. To znamená $v^{-1}((\alpha - \varepsilon, \alpha + \varepsilon)) \in \mathcal{D}$ a $\mathfrak{d}(v^{-1}((\alpha - \varepsilon, \alpha + \varepsilon))) = 1$. Teda $\lim - stat_{n\to\infty} v(n) = \alpha$.

Predpokladajme teraz, že postupnosť $\{v(n)\}$ štatisticky konverguje k hodnote α. Definujme množiny

$$B_k = \Big\{ n \in \mathbb{N}; |v(n) - \alpha| \geq \frac{1}{k} \Big\}, k \in \mathbb{N}.$$

Tieto množiny môžeme vyjadriť a aj v tvare

$$B_k = \mathbb{N} \setminus v^{-1}\Big(\Big(\alpha - \frac{1}{k}, \alpha + \frac{1}{k}\Big)\Big).$$

Z predpokladu o štatistickej konvergencii danej postupnosti vyplýva $B_k \in \mathcal{D}$ a $\mathfrak{d}(B_k) = 0$, pre $k \in \mathbb{N}$. Z definície vylpýva aj to, že $B_k \subset B_{k+1}$. Podlá vety 78 dostávame existenciu takej množiny $B \in \mathcal{D}$, že $B_k \prec B$ a $\mathfrak{d}(B) = 0$. Označme $A = \mathbb{N} \setminus B$. Potom $A \in \mathcal{D}$ a $\mathfrak{d}(A) = 1$. Pre každé prirodzené číslo k existuje N_k také, že $B_k \setminus [1, N_k] \subset B$ a teda $A \cap (B_k \setminus [1, N_k]) = \emptyset$. Z toho vyplýva, že pre $n > N_k, n \in A$ platí $n \notin B_k$, teda $n \in v^{-1}\Big(\Big(\alpha - \frac{1}{k}, \alpha + \frac{1}{k}\Big)\Big)$. Z toho bezprostredne vyplýva $\lim_A v(n) = \alpha$. □

Príklad 170. Zoberieme do úvahy, že pre $A_1, A_2 \in \mathcal{D}, \mathfrak{d}(A_1) = 1, \mathfrak{d}(A_2) = 1$ platí $A_1 \cap A_2 \in \mathcal{D}$ a $\mathfrak{d}(A_1 \cap A_2) = 1$. Potom môžeme dokázať, že zo štatistickej konvergencie postupnosti $\{v_1(n)\}$ k hodnote α_1 a $\{v_2(n)\}$ k hodnote α_2 vyplýva štatistická konvergencia $\{v_1(n) + v_2(n)\}$ k hodnote $\alpha_1 + \alpha_2$.

Veta 79. Ohraničená postupnosť $\{v(n)\}$ štatisticky konverguje k hodnote α vtedy a len vtedy keď

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} |v(n) - \alpha| = 0. \tag{168}$$

Dôkaz. Predpokladajme, že platí (168). Uvažujme $\varepsilon > 0$ a označme

$$S = \{n \in \mathbb{N}; |v(n) - \alpha| \geq \varepsilon\} = \mathbb{N} \setminus v^{-1}((\alpha - \varepsilon, \alpha + \varepsilon)).$$

Aby sme dokázali, že daná postupnosť štatisticky konverguje k α, stačí dokázať, že $S \in \mathcal{D}$ a $\mathfrak{d}(S) = 0$. Z definície množiny S vyplýva

$$\frac{\varepsilon}{N} \sum_{n=1}^{N} \mathbf{C}_S(n) \leq \frac{1}{N} \sum_{n=1}^{N} \mathbf{C}_S(n)|v(n) - \alpha| \leq \frac{1}{N} \sum_{n=1}^{N} |v(n) - \alpha|.$$

Zo (168) preto vyplýva $\varepsilon\mathfrak{d}(S) = 0$. Z toho, že $\varepsilon > 0$ vyplýva $\mathfrak{d}(S) = 0$.

Predpokladajme, že $\{v(n)\}$ štatisticky konverguje k α. Ak danému $\varepsilon > 0$ priradíme vyššie uvedenú množinu S, dostávame

$$S \in \mathcal{D} \ \wedge \ \mathfrak{d}(S) = 0. \tag{169}$$

Uvažovanú sumu si môžeme rozpísať

$$\frac{1}{N}\sum_{n=1}^{N}|v(n)-\alpha| = \frac{1}{N}\sum_{\substack{n\le N\\ n\in S}}|v(n)-\alpha| + \frac{1}{N}\sum_{\substack{n\le N\\ n\notin S}}|v(n)-\alpha|.$$

Z predpokladu, že postupnosť $\{v(n)\}$ je ohraničená dostávame pre prvú sumu

$$\frac{1}{N}\sum_{\substack{n\le N\\ n\in S}}|v(n)-\alpha| \le K\frac{1}{N}\sum_{n\le N}\mathbf{C}_S(n).$$

pre vhodnú konštantu $K > 0$. Z podmienky (169) preto vyplýva, že daná suma konverguje k 0 pre $N \to \infty$. Pri odhadovaní druhej sumy si stačí uvedomiť, že pre $n \notin S$ platí $|v(n) - \alpha| < \varepsilon$. Z toho vyplýva, že celý výraz je menší ako ε. Tým sme dokázali

$$\limsup_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}|v(n)-\alpha| \le \varepsilon.$$

Pretože $\varepsilon > 0$ je ľubovoľné, dokázali sme (168). □

9.11 Stredná hodnota, disperzia

Ak existuje vlastná limita

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}v(n) := E(v),$$

hovoríme, že postupnosť $\{v(n)\}$ **má strednú hodnotu** a $E(v)$ sa nazýva **stredná hodnota** v. Z tejto definície vyplýva: Ak postupnosti $\{v_1(n)\}$ a $\{v_2(n)\}$ majú strednú hodnotu a a_1, a_2 sú reálne čísla, tak aj postupnosť $\{a_1v_1(n) + a_2v_2(n)\}$ má strednú hodnotu a

$$E(a_1v_1 + a_2v_2) = a_1E(v_1) + a_2E(v_2). \tag{170}$$

Príklad 171. Ak postupnosť $\{v(n)\}$ je rovnomerne rozdelená modulo 1, tak má strednú hodnotu a $E(v) = \frac{1}{2}$.

Ak aj postupnosť $\{v^2(n)\}$ má strednú hodnotu, tak hodnota

$$D^2(v) = E(v^2) - (E(v))^2 \tag{171}$$

sa nazýva **disperzia** postupnosti v.

Príklad 172. Disperzia postupnosti, ktorá je rovnomerne rozdelená modulo 1, sa rovná $\frac{1}{12}$.

Pomocou úprav a (170) dostaneme

Veta 80. Nech postupnosti $\{v(n)\}$ a $\{v^2(n)\}$ majú strednú hodnotu. Potom

$$D^2(v) = E((v - E(v))^2) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} (v(n) - E(v))^2.$$

Teda podľa vety 79 dostávame

Veta 81. Ak $v(n)$ je ohraničená postupnosť a postupnosti $\{v(n)\}$ a $\{v^2(n)\}$ majú strednú hodnotu, tak $D^2(v) = 0$ práve vtedy, keď existuje $A \in \mathcal{D}$,$\mathfrak{d}(A) = 1$ taká, že $\lim_A v(n) = E(v)$.

Ak $v_1(n), \{v_2(n)\}$ sú také postupnosti, ktoré majú strednú hodnotu, že aj $v_1^2(n), \{v_2^2(n)\}$ a $\{v_1(n)v_2(n)\}$ majú strednú hodnotu, tak pre disperziu postupnosti $\{a_1v_1(n) + a_2v_2(n)\}$ platí

$$D^2(a_1v_1 + a_2v_2) = a_1^2D^2(v_1) + a_2^2D^2(v_2) + 2a_1a_2(E(v_1v_2) - E(v_1)E(v_2)). \tag{172}$$

Podľa vety 81 dostáveme:

Veta 82. Výraz na pravej strane rovnosti (172) je rovný 0 práve vtedy keď existuje taká množina $A \in \mathcal{D}$, $\mathfrak{d}(A) = 1$, že

$$\lim_A (a_1v_1(n) + a_1v_2(n)) = 0.$$

Príklad 173. Nech $\{v_1(n)\}, \{v_2(n)\}$ sú postupnosti rovnomerne rozdelené modulo 1. Potom množina $A \in \mathcal{D}$, $\mathfrak{d}(A) = 1$, taká že $\lim_A(v_1(n) - v_2(n)) = 0$ existuje práve vtedy, keď

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} v_1(n)v_2(n) = \frac{1}{3}.$$

Podobne sa dá dokázať, že rovnosť

$$\lim_A v_1(n) + v_2(n) = 1$$

je ekvivalentná

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} v_1(n)v_2(n) = -\frac{1}{6}.$$

10 Literatúra

Calda, E., Úloha o největších dělitelích čísel 1,2,3,...,2n
Rozhledy matematicko-fyzikální, Vol. 89 (2014), No. 2, 5–7
DABOUSSI, H., On the density of direct factors of the set of positive integers London Math. Soc. (2), 18, 1978, 1– 4
Novák, B., Vybrané kapitoly z teorie čísel,
Füstenberg, H., On the infinitude of primes,
Amer. Math. Monthly 62 (1955), 353
Kučera, M., "Devítková" vlastnost prvočísel, Rozhledy M.F. 99, (2024)
Vinogradov, I. M., Osnovy teoriji čisel,
Jedinák, D., Cifry, cifry, cifričky ... Rozhledy matematicko-fyzikální, Vol. 84 (2009), No. 2, 49–51
Kolibiar a kol., Algebra a príbuzné disciplíny,
NIVEN, I., The asymptotic density of sequences, Bull. Amer. Math. Soc. 57, 1951, 420–434
SAFFARI, B., On the asymptotic density of sets of integers. J. Lond. Math. Soc., II. Ser. 13, 475-485 (1976).
Znám, Š., Teória čísel, ALFA, Bratislava, 1979

Contents