KALEIDOSKOP TEORIE ČÍSEL (5. kapitola)

Martin Klazar

Vím, že čísla jsou krásná. A jestliže krásná nejsou, pak není krásné nic.

(Paul Erdős, *Sunday Times Magazine,* 27. listopadu 1988.)

Analogicky prožíval pan Š. číslice.
„Pro mne 2, 4, 6, 5 nejsou pouhá čísla. Mají tvar ...
1 — to je ostré číslo, nezávisle na jeho grafickém vyjádření,
je to něco ukončeného, tvrdého.
2 — to je plošší, čtverhranné, bělavé, bývá trochu našedlé ...
3 — to je zaostřený úlomek a točí se.
4 — to je opět čtvercové, tupé, podobné 2, ale mohutnější, tlusté ...
5 — plné zakončení v podobě kužele, věže, masívní.
6 — to následuje první za „5“, je bělavé.
8 — to je nevinné, modravě mléčné, podobné vápnu.“

(A. R. Lurija, *Malá knížka o velké paměti.*)

Toto je předběžný text 5. kapitoly (prvočísla) skript k mé přednášce *Úvod do teorie čísel*, kterou jsem konal na MFF UK v Praze v zimních semestrech školních roků 1996/97, 1998/99 a 1999/00. Zatím v preprintové řadě KAM-DIMATIA Series vyšly kapitoly 1 (základní pojmy a obraty), 2 (diofantické aproximace), 3 (diofantické rovnice) a 4 (kongruence) a budou v ní postupně vydány zbylé kapitoly 6 (geometrie čísel), 7 (číselné rozklady), 8 (medailony matematiků) a 9 (návody k řešením úloh). Obtížnost úloh je bodována 0 (nejlehčí) až 5 (nejtěžší).

září 2000 Martin Klazar

Obsah

Kapitola 5

Prvočísla

Není překvapující, že „malá násobilka“

$1 \times 1 = 1$	$1 \times 2 = 2$	$1 \times 3 = 3$	$1 \times 4 = 4$
$2 \times 1 = 2$	$2 \times 2 = 4$	$2 \times 3 = 6$	$2 \times 4 = 8$
$3 \times 1 = 3$	$3 \times 2 = 6$	$3 \times 3 = 9$	$3 \times 4 = 12$
$4 \times 1 = 1$	$4 \times 2 = 8$	$4 \times 3 = 12$	$4 \times 4 = 16$

neobsahuje $4 \cdot 4 = 16$ různých součinů, ale méně. Komutativita násobení $a \times b = b \times a$ způsobuje symetrii vzhledem k diagonále, a v tabulce tak máme 4 (na diagonále) plus $(16-4)/2 = 6$, celkem 10 různých součinů, že. Ve skutečnosti jich je jen devět: $1, 2, 3, 4, 6, 8, 9, 12$ a 16. Další faktor snižující počet součinů je ten, že $a \times b$ se může rovnat $c \times d$, ikdyž $\{a, b\} \neq \{c, d\}$. Naše tabulka obsahuje jedinou instanci tohoto jevu: $1 \times 4 = 2 \times 2$. Ve větší tabulce to však nastane častěji. Uvažme „velkou násobilku“ s n^2 položkami $1 \times 1, \ldots, n \times n$. Obsahuje alespoň cn^2 různých součinů ($c > 0$ je konstanta)? Zkuste odpovědět, aniž byste četli dále.

Taková konstanta c neexistuje a pro $n \to \infty$ velká násobilka obsahuje jen $o(n^2)$ součinů. Nahlédneme to podivuhodným argumentem využívajícím prvočísla. V oddílu 5.5 totiž dokážeme klasickou větu Godfreye Hardyho a Srinivasy Ramanujana, podle níž má „typické“ číslo z množiny $\{1, 2, \ldots, n\}$ zhruba $\log\log n$ prvočinitelů, počítáno včetně násobností. Skoro všechny součiny $a \times b$, kde $a, b \in \{1, 2, \ldots, n\}$, tedy mají asi $\log\log n + \log\log n = 2\log\log n$ prvočinitelů, včetně násobností. Ale typické číslo z množiny $\{1, 2, \ldots, n^2\}$ má, znovu podle věty Hardyho a Ramanujana, jen asi $\log\log n^2 = \log\log n + \log 2$ prvočinitelů. Součiny $a \times b$ jsou tedy poměrně netypická čísla a musí jich být jen $o(n^2)$.

V kapitole 5 symboly p a q označují prvočísla. Oddíly 5.1, 5.3 a 5.7 se zabývají rychlostí růstu prvočíselné funkce $\pi(x)$. Připomínáme, že pro reálné x je $\pi(x)$ počet prvočísel nepřesahujících x. V 5.1 dokážeme čtyřmi způsoby, že $\pi(x) \to \infty$ pro $x \to \infty$. V 5.3 to zpřesníme Čebyševovou větou 139, podle níž $\pi(x)$ roste, až na multiplikativní konstantu, jako funkce $x/\log x$. V Mertensově větě 141 odvodíme asymptotiky součtů $\sum_{p\le x} 1/p$ a $\sum_{p\le x} \log p/p$ a součinu $\prod_{p\le x}(1-1/p)$. Kapitolu zakončíme v oddílu 5.7 důkazem slavné Prvočíselné věty (věta 157): $\pi(x) \sim x/\log x$. V 5.7.1 uvádíme komplexně-analytický důkaz a v 5.7.2 elementární.

Věta 130 v oddílu 5.2 charakterizuje sudá dokonalá čísla pomocí Mersennových prvočísel. Lucasův–Lehmerův test, věta 132, popisuje algoritmus pro jejich vyhledávání, to jest pro testování prvočíselnosti čísel $2^q - 1$. V 5.4 uvádíme „formuli“ generující nekonečně mnoho prvočísel a rekurentní formuli pro n-té prvočíslo. Uvádíme důsledek řešení Hilbertova desátého problému: Lze sestrojit celočíselný polynom (více proměnných), jehož kladné hodnoty (pro argumenty probíhající $\mathbf{N}_0$) jsou právě všechna prvočísla. Dokážeme Prattovu větu 146: vlastnost „být prvočíslo“ má polynomiální certifikát.

V oddílu 5.5 odvodíme, že funkce $\omega(n)$ a $\Omega(n)$ mají průměrnou hodnotu zhruba $\log\log n$. Pak dokážeme hlubší výsledek, již zmíněnou Hardyho–Ramanujanovu větu, podle níž se $\omega(n)$ i $\Omega(n)$ rovnají zhruba $\log\log n$ pro skoro všechny argumenty n. Šnirelmanova věta 150 říká, že každé přirozené číslo větší než jedna je *součtem* omezeně mnoha prvočísel. Této perle aditivní teorie čísel je věnován oddíl 5.6.

Kromě 5.7 pracujeme jen s elementárními prostředky. Oddíly 5.6 a 5.7 obsahují náročnější materiál. Upozorňujeme na použití kvadratických zbytků v 5.2. Pro širší porozumění kontextu Prattovy věty 146 je třeba se obrátit k učebnicím výpočetní složitosti. První důkaz Prvočíselné věty v 5.7.1 používá jen „elementární komplexní analýzu“ (základní vlastnosti holomorfních funkcí, Cauchyho věta) a k jeho sledování plně postačuje absolvování základního kursu komplexní analýzy. Elementární důkaz v 5.7.2 pracuje jen s reálnou analýzou.

5.1 Je nekonečně mnoho prvočísel

a řada způsobů, jak to dokázat. Uvádíme čtyři důkazy.

EUKLIDŮV DŮKAZ je důkaz sporem. Předpokládejme, že prvočísel je konečně mnoho a že to jsou čísla $p_1, p_2, \ldots, p_k$. Uvážíme po sobě jdoucí čísla

$$n = p_1 p_2 \cdots p_k \ \text{ a } \ n+1 = p_1 p_2 \cdots p_k + 1 \ .$$

Nejmenší číslo $q \in \mathbf{N}, q > 1$, které dělí $n+1$ je prvočíslo (vzhledem k minimalitě) a dělí i n, protože každé prvočíslo dělí n. Pak ale q dělí i $1 = (n+1) - n$, což je spor.

GOLDBACHŮV DŮKAZ využívá vzájemné nesoudělnosti *Fermatových čísel* F_n,

$$F_n = 2^{2^n} + 1 \ .$$

Pro $m > n$ a $k = 2^{2^n}$ máme

$$\begin{aligned} F_m - 2 &= k^{2^{m-n}} - 1^{2^{m-n}} \\ &= (k+1)(k^{2^{m-n}-1} - k^{2^{m-n}-2} + \cdots - 1) \\ &= F_n(k^{2^{m-n}-1} - k^{2^{m-n}-2} + \cdots - 1) \ . \end{aligned}$$

Vidíme, že $F_n \backslash (F_m - 2)$. Čísla F_n jsou lichá, tedy $F_m \perp F_n$. Pro každé $n \in \mathbf{N}$ zvolíme prvočíslo q_n dělící F_n. Všechna q_n musí být různá a je jich tedy nekonečně mnoho. Nedalo by se položit $q_n = F_n$? Viz oddíl 5.3 a poznámky k 5.1.

EULERŮV DŮKAZ je analytický, jak se na člověka přezdívaného *Analysis incarnate* sluší. Pro každé reálné $s > 1$ platí *Eulerova identita*

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

Levá strana je totiž součinem geometrických řad

$$\prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots \right)$$

a po roznásobení dostáváme s pomocí věty 2 z 1.2 pravou stranu. (Podrobnosti jsou předmětem úlohy 2.) Předpokládejme, že prvočísel je konečně mnoho a podívejme se na chování identity pro $s \to 1^+$. Levá strana má konečnou limitu rovnou konečnému součinu $\prod 1/(1-1/p)$, ale pravá strana jde do nekonečna (řada $\sum_{n=1}^{\infty} 1/n$ diverguje). Opět máme spor.

Erdősův důkaz má kombinatorickou příchuť. Každé číslo $m \in \mathbf{N}$ má jednoznačné vyjádření $m = k^2 l$, kde $k, l \in \mathbf{N}$ a l je čtvercuprosté. Pokud $m \leq n$, připadá pro k v úvahu nejvýše $n^{1/2}$ hodnot a pro l nejvýše $2^{\pi(n)}$ hodnot (l je součinem různých prvočísel nepřesahujících n). Protože pro různá m jsou i dvojice k, l různé, musí platit nerovnost

$$n \leq \sqrt{n}\, 2^{\pi(n)} \ .$$

Tedy

$$\pi(n) \geq \tfrac{1}{2} \log_2 n$$

a $\pi(n) \to \infty$ pro $n \to \infty$. Úloha 3 ukazuje, jak se pro $\pi(n)$ dá jednoduše dokázat daleko silnější dolní odhad. Žel, jedná se o „důkaz“.

5.2 Dokonalá čísla a Mersennova prvočísla

Je vám 28 let? Pak se nacházíte v „dokonalém“ věku, protože číslo 28 dělí krom něj samotného ještě 1, 2, 4, 7 a 14 a hle,

$$28 = 1 + 2 + 4 + 7 + 14 \ .$$

Taková čísla se od dob pythagorejců nazývají *dokonalá*. Jinak řečeno, n je dokonalé, pokud $\sigma(n) = 2n$ (σ je funkce součtu dělitelů z 1. kapitoly). První dokonalé číslo je 6. Sudá dokonalá čísla se dají do určité míry popsat.

Věta 130 (Euler, 17??). *Sudé $n \in \mathbf{N}$ je dokonalé, právě když má tvar*

$$n = 2^m(2^{m+1} - 1) \ ,$$

kde $m \in \mathbf{N}$ a $2^{m+1} - 1$ je prvočíslo.

Důkaz. Číslo $2^{m+1} - 1$ označíme jako M_{m+1}. Nechť je prvočíslem, pak

$$\begin{aligned} \sigma(n) = \sigma(2^m(2^{m+1}-1)) &= 1 + 2^1 + \cdots + 2^m + M_{m+1}(1 + 2^1 + \cdots + 2^m) \\ &= 2^{m+1} - 1 + M_{m+1}(2^{m+1} - 1) \\ &= M_{m+1} 2^{m+1} \\ &= 2n \ . \end{aligned}$$

Naopak, nechť $n = 2^m b$ je dokonalé, $m > 0$ a b je liché. Z multiplikativity σ dostáváme $\sigma(n) = \sigma(2^m)\sigma(b) = (2^{m+1} - 1)\sigma(b)$. Víme, že $\sigma(n) = 2n$. Proto

$$\frac{2^{m+1} - 1}{2^{m+1}} = \frac{b}{\sigma(b)} \ .$$

Zlomek vlevo je v základním tvaru, proto

$$b = (2^{m+1} - 1)c \ \text{ a } \ \sigma(b) = 2^{m+1}c \ ,$$

kde $c \in \mathbf{N}$. Předpoklad $c > 1$ vede ke sporu: $1, c$ i $(2^{m+1} - 1)c$ jsou různí dělitelé b $(m > 0)$ a

$$\sigma(b) \geq 1 + c + (2^{m+1} - 1)c > 2^{m+1}c \ .$$

Proto $c = 1$, $n = 2^m b = 2^m(2^{m+1} - 1)$ a $\sigma(b) = \sigma(2^{m+1} - 1) = 2^{m+1} = b + 1$. Číslo n je uvedeného tvaru a $b = M_{m+1}$ je prvočíslo. $\diamondsuit$

Ikdyž není známo, zda existují lichá dokonalá čísla, leccos se o nich ví, viz poznámky a úloha 16. Čertovo kopýtko předchozího elegantního výsledku se skrývá v dodatku o čísle M_{m+1}. Abychom nalezli sudé dokonalé číslo, musíme zjistit, kdy je $M_m = 2^m - 1$ prvočíslo. Prvočísla tohoto tvaru se nazývají *Mersennova prvočísla*. Snadno se přesvědčíme, že nutnou podmínkou prvočíselnosti M_m je prvočíselnost m. Není to však postačující podmínka: $M_{11} = 2047 = 23 \cdot 89$. Z tohoto příkladu plyne následující poučení.

Tvrzení 131 (dělitelnost čísel M_q). *Nechť q je prvočíslo a $M_q = 2^q - 1$.*
1. *Pokud $q \equiv 3 \bmod 4$ a $2q + 1$ je rovněž prvočíslo, $2q + 1$ dělí M_q.*
2. *Když n dělí M_q, $n \equiv \pm 1 \bmod 8$ a $n \equiv 1 \bmod q$.*

DŮKAZ. **1.** Protože $p = 2q + 1 \equiv 7 \bmod 8$, podle 2 tvrzení 105 v kapitole 4 platí, že $\left(\frac{2}{p}\right) = 1$. Podle 1 tvrzení 103,

$$2^q = 2^{(p-1)/2} \equiv 1 \bmod p$$

a p dělí $2^q - 1$.

2. Obě kongruence stačí dokázat pro prvočíselné $n = p$ (proč?). Protože $2^q \equiv 1 \bmod p$ a q je prvočíslo, je q řádem prvku 2 v grupě $(\mathbf{Z}_p^*, \cdot)$. Ale i

$2^{p-1} \equiv 1 \bmod p$, podle Malé Fermatovy věty, a tak $q \backslash (p-1)$, což je druhá kongruence. Protože p i q jsou lichá, $p = 2kq + 1$. Podle 1 tvrzení 103

$$\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \equiv 2^{kq} \equiv 1 \bmod p \ .$$

Pomocí 2 tvrzení 105 dostáváme první konguenci. $\diamondsuit$

Není známo, je-li Mersennových prvočísel nekonečně mnoho. Seznam dosud objevených Mersennových prvočísel je v poznámkách. Lucas objevil, a Lehmer přesně dokázal, krásný a účinný způsob, jak prvočíselnost M_q testovat. Následující výsledek je známý jako *Lucasův–Lehmerův test*.

Věta 132 (Lehmer, 1935). *Nechť q je prvočíslo. $M_q = 2^q - 1$ je prvočíslo, právě když M_q dělí číslo r_{q-1}, které získáme rekurencí $r_1 = 4$ a $r_{n+1} = r_n^2 - 2$.*

Samozřejmě stačí počítat pouze modulo M_q, s mezivýsledky nepřesahujícími M_q^2. Například pro $q = 11$ dostáváme, modulo $M_{11} = 2047$,

$$\begin{array}{ll} r_1 = 4 & r_6 \equiv 119 \\ r_2 = 14 & r_7 \equiv 1877 \\ r_3 = 194 & r_8 \equiv 240 \\ r_4 \equiv 788 & r_9 \equiv 282 \\ r_5 \equiv 701 & r_{10} \equiv 1736 \ . \end{array}$$

Protože M_{11} nedělí r_{10}, M_{11} není prvočíslo.

Větu dokážeme elegantně a elementárně podle Lehmera. Budeme potřebovat několik pomocných výsledků. Položíme $a = 1 + \sqrt{3}$ a $b = 1 - \sqrt{3}$. Tedy $a + b = 2$, $ab = -2$ a $a - b = 2\sqrt{3}$. Dále nechť

$$U_r = \frac{a^r - b^r}{a - b} \ \text{ a } \ V_r = a^r + b^r, \ r = 1, 2, \ldots$$

Lemma 133. *Pro každé $r, s \in \mathbf{N}$ platí*
1. $2U_{r+s} = U_r V_s + V_r U_s$.
2. $(-2)^{s+1} U_{r-s} = U_s V_r - U_r V_s$.
3. $2V_{r+s} = V_r V_s + 12 U_r U_s$.
4. $U_{2r} = U_r V_r$.
5. $V_{2r} = V_r^2 + (-2)^{r+1}$.
6. $V_r^2 - 12 U_r^2 = (-2)^{r+2}$.

DŮKAZ. První tři identity se snadno ověří přímým dosazením. Čtvrtá plyne z první. Pátá a šestá plynou přímým dosazením. ◊

Z rekurencí nebo přímo z definice je zřejmé, že U_r a V_r jsou přirozená čísla. Všimněme si, že podle 6 řeší dvojice (V_r, U_r) zobecněnou Pelliánu $x^2 - 12y^2 = (-2)^{r+2}$. Srovnej tvrzení 59.

V dalším je $p > 3$ vždy prvočíslo.

Lemma 134.

$$U_p \equiv \left(\frac{3}{p}\right) \quad a \quad V_p \equiv 2 \bmod p \ .$$

DŮKAZ. Podle definice U_r a binomické věty

$$U_p = \tfrac{1}{2\sqrt{3}}((1+\sqrt{3})^p - (1-\sqrt{3})^p) = \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} 3^k \ .$$

Všechny binomické koeficienty kromě posledního jsou dělitelné p, takže

$$U_p \equiv 3^{(p-1)/2} \equiv \left(\frac{3}{p}\right) \bmod p \ .$$

(Podle Eulerova kritéria kvadratických zbytků.)

Druhá kongruence se dokáže podobně:

$$V_p = (1+\sqrt{3})^p + (1-\sqrt{3})^p = 2\sum_{k=0}^{(p-1)/2} \binom{p}{2k} 3^k \equiv 2 \cdot 3^0 \bmod p \ .$$

◊

Lemma 135. *Nechť p dělí U_m a m_0 je nejmenší takové $m \in \mathbf{N}$. Potom $m_0 \backslash m$ a $m_0 \leq p+1$.*

DŮKAZ. Nechť $p \backslash U_m$ a $m = rm_0 + s$, $0 \leq s < m_0$. Pomocí 1 a 2 lemmatu 133 plyne, že p dělí i U_s. Tedy $s = 0$.

Z 1 a 2 lemmatu 133 plyne dále $(U_1 = 1, V_1 = 2)$, že $2U_{p+1} = 2U_p + V_p$ a $-4U_{p-1} = 2U_p - V_p$. Takže, podle lemmatu 134,

$$-8U_{p-1}U_{p+1} = 4U_p^2 - V_p^2 \equiv 4(\pm 1)^2 - 4 = 0 \bmod p$$

a p dělí U_{p+1} nebo U_{p-1}. $\diamondsuit$

Důkaz věty 132. Nejprve dokážeme přímou implikaci

$$M = M_q = 2^q - 1 \text{ je prvočíslo } \Longrightarrow r_{q-1} \equiv 0 \bmod M_q \ .$$

Čísla $s_i = 2^{2^{i-1}} r_i$ splňují rekurenci $s_1 = 8$ a $s_{i+1} = s_i^2 - 2^{2^i+1}$. Tutéž rekurenci však splňují i čísla V_{2^i} (viz 5 lemmatu 133), a proto $s_i = V_{2^i}$. Stačí dokázat, že $s_{q-1} = V_{2^{q-1}} = V_{(M+1)/2}$ je dělitelné M_q. Podle 5 lemmatu 133 máme

$$V_{(M+1)/2}^2 = V_{M+1} + 4 \cdot 2^{(M-1)/2} \equiv V_{M+1} + 4 \bmod M \ ,$$

protože $(\frac{2}{M}) = 1$ ($M \equiv 7 \bmod 8$). Zbývá dokázat, že $V_{M+1} \equiv -4 \bmod M$. Podle 3 lemmatu 133 a lemmatu 134,

$$\begin{aligned} V_{M+1} &= V_M + 6U_M \\ &\equiv 2 + 6\left(\frac{3}{M}\right) \bmod M \ . \end{aligned}$$

Podle věty 106 (kvadratická reciprocita) $(\frac{3}{M}) = -(\frac{M}{3}) = -(\frac{1}{3}) = -1$, protože $M \equiv 3 \bmod 4$ a $M \equiv 1 \bmod 3$. Skutečně $V_{M+1} \equiv -4 \bmod M$ a M dělí r_{q-1}.

Dokážeme opačnou implikaci

$$M = M_q = 2^q - 1 \text{ dělí } r_{q-1} \Longrightarrow M \text{ je prvočíslo} \ .$$

M dělí $s_{q-1} = V_{2^{q-1}}$. Nechť p je libovolný prvočinitel M a m_0 buď jako v lemmatu 135. M a tedy i p dělí $U_{2^q} = U_{2^{q-1}} V_{2^{q-1}}$ (4 lemmatu 133). Podle lemmatu 135, $m_0 \backslash 2^q$. Kdyby m_0 dělilo 2^{q-1}, měli bychom kromě $p \backslash V_{2^{q-1}}$ ještě i $p \backslash U_{2^{q-1}}$, ale to nelze (6 lemmatu 133). Tudíž $m_0 = 2^q$. Podle lemmatu 135, $p \geq m_0 - 1 = 2^q - 1 = M$. $M = p$ je prvočíslo. Tím je věta 132 dokázána.

5.3 Čebyševovy a Mertensovy odhady

Pro důkaz Čebyševovy věty, podle níž pro $x \to \infty$ platí asymptotické odhady $x/\log x \ll \pi(x) \ll x/\log x$, budeme potřebovat odhady výrazů obsahujících *von Mangoldtovu funkci* $\Lambda : \mathbf{N} \to \mathbf{R}$,

$$\Lambda(n) = \begin{cases} \log p & \dots \quad n = p^r \\ 0 & \dots \quad \text{jinak} \ . \end{cases}$$

Lemma 136. *Pro $x \to \infty$ platí asymptotika*

$$\sum_{n \le x} \Lambda(n) \lfloor x/n \rfloor = x \log x - x + O(\log x) \ .$$

Důkaz. Použijeme tvrzení 16 v kapitole 1:

$$\begin{aligned} \sum_{n \le x} \Lambda(n) \lfloor x/n \rfloor &= \sum_{n \le x} \Lambda(n) \sum_{m \le x} \langle n \backslash m \rangle \\ &= \sum_{m \le x} \sum_{n \backslash m} \Lambda(n) = \sum_{m \le x} \log m \\ &= x \log x - x + O(\log x) \ . \end{aligned}$$

♢

Lemma 137. *Pro $x \to \infty$ platí asymptotika*

$$\sum_{n \le x} \Lambda(n)(\lfloor x/n \rfloor - 2\lfloor x/2n \rfloor) = x \log 2 + O(\log x) \ .$$

Důkaz. Použijeme předchozí lemma. Levá strana je vlastně

$$\sum_{n \le x} \Lambda(n) \lfloor x/n \rfloor - 2 \sum_{n \le x/2} \Lambda(n) \lfloor x/2n \rfloor$$

a

$$x \log x - x + O(\log x) - 2(\tfrac{x}{2} \log \tfrac{x}{2} - \tfrac{x}{2} + O(\log \tfrac{x}{2})) = x \log 2 + O(\log x) \ .$$

♢

Čebyševova funkce $\vartheta : \mathbf{R} \to \mathbf{R}$ je definována jako

$$\vartheta(x) = \sum_{p \le x} \log p \ .$$

Dá se shora odhadnout pěkným kombinatorickým obratem.

Lemma 138. *Pro každé kladné $x \in \mathbf{R}$ platí nerovnost*

$$\vartheta(x) < (4 \log 2) x \ .$$

Důkaz. Pro $n \in \mathbf{N}$ platí

$$2^{2n} = (1+1)^{2n} \geq \binom{2n}{n} \geq \prod_{n<p\leq 2n} p = \exp(\vartheta(2n) - \vartheta(n)) \ .$$

Pro reálné $x > 1$ a $m \in \mathbf{N}$ splňující $2^{m-1} < x \leq 2^m$ odtud dostáváme

$$\vartheta(x) \leq \sum_{k=1}^{m} (\vartheta(2^k) - \vartheta(2^{k-1})) \leq \sum_{k=1}^{m} 2^k \log 2 < 4x \log 2 \ .$$

$\diamondsuit$

Nyní máme vše připraveno k důkazu Čebyševovy věty.

Věta 139 (Čebyšev, 1852). *Pro $x \to \infty$ platí*

$$\frac{x}{\log x} \ll \pi(x) \ll \frac{x}{\log x} \ .$$

Důkaz. Protože $\lfloor a \rfloor - 2\lfloor a/2 \rfloor \leq 1$ pro každé $a \in \mathbf{R}$, plyne z lemmatu 137, že

$$x \log 2 + O(\log x) \leq \sum_{n\leq x} \Lambda(n) = \sum_{p\leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p \leq \log x \sum_{p \leq x} 1 = \pi(x) \log x \ .$$

Máme dokázán dolní odhad $\pi(x)$. Kompaktní „binomická“ podoba tohoto argumentu je v úloze 19.

Podle lemmatu 138 a definice $\vartheta(x)$

$$(4\log 2)x > \vartheta(x) \geq \sum_{x^{1/2}<p\leq x} \log p \geq \sum_{x^{1/2}<p\leq x} \tfrac{1}{2} \log x \geq \tfrac{1}{2} \log x \cdot (\pi(x) - x^{1/2}) \ .$$

Máme dokázán horní odhad $\pi(x)$. $\diamondsuit$

Čebyšev podobnými, ale složitějšími postupy získal v obou odhadech dobré konstanty a odvodil z nich

Tvrzení 140 (Bertrandův postulát). *Pro každé přirozené $n > 1$ v intervalu $(n, 2n)$ leží alespoň jedno prvočíslo.*

Důkaz tohoto tvrzení neuvádíme.

Nahradíme-li 1 v sumě $\pi(x) = \sum_{p\le x} 1$ sčítancem řádu $o(1)$, dají se elementárně získat přesné asymptotiky. Upravíme jinak výraz na levé straně v lemmatu 136:

$$\sum_{n\le x} \Lambda(n)\lfloor x/n\rfloor = \sum_{p\le x} \lfloor x/p\rfloor \log p + \sum_{p^v\le x} \langle v\ge 2\rangle \lfloor x/p^v\rfloor \log p \ .$$

V prvním součtu máme $\ll x/\log x$ sčítanců (podle Čebyševovy věty). Odstraněním všech $\lfloor$ a $\rfloor$ uděláme proto chybu $\ll (\log x)\cdot x/\log x = x$. Druhý součet je nejvýše

$$x \sum_{m,v=2}^{\infty} \frac{\log m}{m^v} \ll x \ .$$

Celkem

$$\sum_{n\le x} \Lambda(n)\lfloor x/n\rfloor = x\sum_{p\le x} \frac{\log p}{p} + O(x) \ .$$

Z lemmatu 136 tak plyne, že součet

$$M_1(x) = \sum_{p\le x} \frac{\log p}{p}$$

má asymptotiku

$$M_1(x) = \log x + O(1) \ .$$

Pomocí Abelovy sumace (tvrzení 18 v kapitole 1) odtud získáme asymptotiku pro sumu se sčítancem p^{-1}:

$$\sum_{p\le x} \frac{1}{p} = \sum_{p\le x} \frac{\log p}{p}\cdot\frac{1}{\log p} = \frac{M_1(x)}{\log x} + \int_2^x \frac{M_1(t)\ dt}{t\log^2 t} \ .$$

První sčítanec je $1 + O(\log^{-1} x)$, druhý se rovná

$$\begin{aligned} & \int_2^x \frac{dt}{t\log t} + \int_2^x \frac{(M_1(t)-\log t)\ dt}{t\log^2 t} = \\ = \ & \log\log x - \log\log 2 + \int_2^\infty \frac{(M_1(t)-\log t)dt}{t\log^2 t} - \int_x^\infty \frac{(M_1(t)-\log t)\ dt}{t\log^2 t} \\ = \ & \log\log x - \log\log 2 + c + O(\log^{-1} x) \end{aligned}$$

(protože, podle asymptotiky M_1, $M_1(t) - \log t = O(1)$). Celkem pro

$$M_2(x) = \sum_{p \le x} \frac{1}{p}$$

máme asymptotiku

$$M_2(x) = \log\log x + c_1 + O(\log^{-1} x)\ .$$

Nakonec zjistíme, jak rychle jde k nule součin $\prod_{p \le x}(1 - 1/p)$.

$$\begin{aligned}
\log \prod_{p \le x} \left(1 - \frac{1}{p}\right) &= \sum_{p \le x} \log(1 - 1/p) = -\sum_{p \le x} \sum_{n=1}^{\infty} \frac{(1/p)^n}{n} \\
&= -M_2(x) - \sum_{n,p} \frac{\langle n \ge 2\ \&\ p \le x \rangle}{np^n} \\
&= -M_2(x) - \sum_{n,p} \frac{\langle n \ge 2 \rangle}{np^n} + \sum_{n,p} \frac{\langle n \ge 2\ \&\ p > x \rangle}{np^n}\ .
\end{aligned}$$

První suma konverguje, ikdyž obor sumace rozšíříme z p na všechna $m \ge 2$. Druhá suma je nejvýše

$$\sum_{n \ge 2} n^{-1} \sum_{m > x} m^{-n} \ll \sum_{n \ge 2} x^{1-n}(n-1)^{-1} n^{-1} \ll x^{-1}\ .$$

Celkem, s využitím asymptotiky M_2, máme pro

$$M_3(x) = \prod_{p \le x} \left(1 - \frac{1}{p}\right)$$

po odlogaritmování asymptotiku

$$M_3(x) = \frac{c_2}{\log x} \cdot \Big(1 + O(\log^{-1} x)\Big)\ .$$

Asymptotiky veličin $M_1(x), M_2(x)$ a $M_3(x)$ shrneme do jedné věty.

Věta 141 (Mertens, 1874). *Existují konstanty c_1 a c_2 ($c_2 > 0$) tak, že pro $x \to \infty$*

1. $$\sum_{p \le x} \frac{\log p}{p} = \log x + O(1)\ .$$

2. $$\sum_{p \le x} \frac{1}{p} = \log\log x + c_1 + O(\log^{-1} x)\ .$$

3. $$\prod_{p \le x} \left(1 - \frac{1}{p}\right) = \frac{c_2}{\log x} + O(\log^{-2} x)\ .$$

5.4 Vzorce pro prvočísla

Řada Fermatových čísel $F_n = 2^{2^n} + 1$ začíná

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537, F_5 = 4294967297, \ldots$$

Fermat se domníval, že každé F_n je prvočíslo. F_0, F_1, F_2, F_3 a F_4 jsou prvočísla, ale F_5 nikoli, jak v r. 1732 ukázal Euler: $4294967297 = 641 \cdot 6700417$. Složenost F_5 je zřejmá i z této úvahy:

$$\begin{aligned} 2^{32} &= 16 \cdot 2^{28} \\ &= (641 - 5^4) \cdot 2^{28} \\ &= 641m - (5 \cdot 2^7)^4 \\ &= 641m - (641 - 1)^4 \\ &= 641n - 1\ . \end{aligned}$$

Kromě prvních pěti hodnot není známo žádné jiné prvočíselné F_n.

Fermatova domněnka byla vlastně návrhem na prostou (dokonce rostoucí) funkci $F : \mathbf{N} \to \mathbf{N}$, která (i) nabývá pouze prvočíselných hodnot a (ii) je popsána konečnou aritmeticko-analytickou formulí. Fermatova funkce $F(n) = 2^{2^n} + 1$ splňuje jistě druhou podmínku, nesplňuje však první. Uvedeme příklad funkce, která splňuje první podmínku a předstírá, že splňuje i druhou.

Tvrzení 142 (Wrightův vzorec). *Existuje reálné číslo α takové, že*

$$F(n) = \left\lfloor 2^{2^{\cdot^{\cdot^{2^\alpha}}}} \right\rfloor \Big\}\ n \textit{ dvojek}$$

je prvočíslo pro každé $n \in \mathbf{N}$.

Důkaz. Vyjdeme z tvrzení 140. Podle něj můžeme definovat posloupnost prvočísel $p_1, p_2, \ldots$ tak, že

$$2^{p_n} < p_{n+1} < 2^{p_n+1} \ .$$

Položíme $u_n = \log_2^{(n)} p_n$ ((n) znamená n binárních logaritmů) a $v_n = \log_2^{(n)}(p_n+1)$. Protože $p_n < \log_2 p_{n+1} < \log_2(p_{n+1}+1) \le p_n + 1$, platí

$$u_n < u_{n+1} < v_{n+1} \le v_n \ .$$

Pro $n \to \infty$ jde u_n k limitě α a pro každé $n \in \mathbf{N}$ platí $u_n < \alpha < v_n$. Tudíž

$$p_n < 2^{2^{\cdot^{\cdot^{2^\alpha}}}} < p_n + 1 \quad (n \text{ dvojek})$$

a tvrzení je dokázáno. ◇

Dá se formulí zachytit posloupnost $p_1 = 2, p_2 = 3, \ldots$, kde p_n je n-té prvočíslo? Následující rekurence je, když nic jiného, alespoň elegantní.

Tvrzení 143 (Gandhiho formule). *Součin $p_1 p_2 \ldots p_n$ označíme P_n. Pak*

$$p_n = \left\lfloor 1 - \log_2 \left(-\frac{1}{2} + \sum_{d \backslash P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor \ ,$$

kde μ je Möbiova funkce.

Důkaz. Součet v rekurenci označíme S. Máme dokázat nerovnosti

$$2^{1-p_n} + \tfrac{1}{2} \ge S > 2^{-p_n} + \tfrac{1}{2} \ .$$

Počítejme:

$$\begin{aligned} S \cdot (2^{P_{n-1}} - 1) &= \sum_d \langle d \backslash P_{n-1} \rangle \cdot \mu(d)(1 + 2^d + 2^{2d} + \cdots + 2^{P_{n-1}-d}) \\ &= \sum_{k=0}^{P_{n-1}-1} 2^k \sum_d \langle d \backslash (k, P_{n-1}) \rangle \cdot \mu(d) \\ &= \sum_{k=0}^{P_{n-1}-1} \langle (k, P_{n-1}) = 1 \rangle \cdot 2^k \quad (\text{tvrzení } 6) \ . \end{aligned}$$

Poslední sumu označíme jako T. Jistě $T \geq 2^{P_{n-1}-p_n} + 2^{P_{n-1}-1}$ a $S \geq T/(2^{P_{n-1}}-1) > 2^{-p_n} + 2^{-1}$. Z druhé strany (pro $n > 1$)

$$\begin{aligned} T &\leq \sum_{k=0}^{P_{n-1}-1} 2^k - \sum_{k=0}^{P_{n-1}-1} \langle P_{n-1} - p_n < k < P_{n-1} - 1 \rangle \cdot 2^k \\ &= 2^{P_{n-1}-1} + 2^{P_{n-1}-p_n+1} - 1 \ . \end{aligned}$$

Odtud

$$S \leq \frac{T}{2^{P_{n-1}}-1} \leq \frac{1}{2} + 2^{1-p_n} \cdot \frac{2^{P_{n-1}} - 2^{p_n-2}}{2^{P_{n-1}}-1}$$

a $S < \frac{1}{2} + 2^{1-p_n}$. $\diamondsuit$

Následující důsledek Matijasevičova řešení desátého Hilbertova problému překonává elegancí oba předchozí výsledky.

Tvrzení 144 (Matijasevičovo vyjádření). *Lze předložit takový celočíselný polynom Q o m neznámých (konkrétní příklad uvádíme v poznámkách), že*

$$\{Q(x_1, x_2, \ldots, x_m) : \ x_i \in \mathbf{N}_0\} \cap \mathbf{N} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots\} \ .$$

DŮKAZ. Podle tvrzení 79 z pododdílu 3.5.3 je množina prvočísel (jako každá rekurzivně spočetná množina) diofantická. Lze tedy sestrojit polynom $R \in \mathbf{Z}[x_1, \ldots, x_m]$ tak, že pro každé $x_1 \in \mathbf{N}_0$ má rovnice $R(x_1, x_2, \ldots, x_m) = 0$ řešení $x_2, \ldots, x_m \in \mathbf{N}_0$ tehdy a jen tehdy, je-li x_1 prvočíslo. Je očividné, že kladné hodnoty polynomu $Q(x_1, \ldots, x_m) = x_1(1 - R(x_1, \ldots, x_m)^2)$ na $x_i \in \mathbf{N}_0$ jsou pak právě všechna prvočísla. $\diamondsuit$

Není znám algoritmus, který by pro vstup $n \in \mathbf{N}$ po polynomiálním počtu kroků (polynomiálním v $\log n$) rozhodl, zda n je či není prvočíslo. (V jistém praktickém smyslu však takové algoritmy známé jsou, viz poznámky.) Překvapivě je však známa metoda certifikace, která, pokud n prvočíslo je, prvočíselnost n dokáže v polynomiálním počtu kroků. Než certifikát prvočíselnosti a jeho ověřování vysvětlíme, připomeneme několik pojmů z teorie výpočetní složitosti.

Dvě nejdůležitější složitostní třídy rozhodovacích úloh představují **P** a **NP**. Neformálně řečeno, **P** obsahuje úlohy, které lze vyřešit deterministickým algoritmem v počtu kroků polynomiálním ve velikosti vstupu, a **NP** úlohy, které lze takto vyřešit nedeterministickým algoritmem. Ekvivalentně, úloha je v **NP**, existuje-li pro ni algoritmus certifikace, kterým lze o každém řešení úlohy v polynomiálním počtu kroků dokázat, že jde skutečně o řešení. Podáme podrobnější definice.

Σ buď pevně daná konečná abeceda a Σ^* množina všech konečných slov nad Σ. Rozhodovací úloha se kóduje *formálním jazykem* L, což je podmnožina $L \subset \Sigma^*$. (L jsou řešení úlohy a $\Sigma^*\backslash L$ její „neřešení“.) Třída **P** se definuje následovně. $L \in \mathbf{P}$, právě když existuje $k \in \mathbf{N}$ a Turingův stroj M takový, že pro každé slovo $u \in \Sigma^*$ platí

$$u \in L \iff M \text{ přijme } u \text{ v nejvýše } |u|^k + k \text{ krocích} .$$

Pomocí $|u|$ značíme délku slova a „M přijímá u v n krocích“ znamená, že se M po výpočtu na u po n krocích zastaví v přijímajícím stavu. Pro $u \notin L$ se M po výpočtu na u zastaví v odmítajícím stavu nebo se nezastaví vůbec.

Člen $+k$ v definici **P** slouží pouze k „ošetření“ slov délky 0 a 1. Vzhledem k apriornímu odhadu délky výpočtu se lehce ukáže, že v definici **P** se lze omezit na Turingovy stroje, které mají právě dva koncové stavy ANO (přijímající) a NE (odmítající) a které se zastaví pro každé slovo $u \in \Sigma^*$. Tudíž $L \in \mathbf{P}$, právě když $(\Sigma^*\backslash L) \in \mathbf{P}$.

Podáme podrobnější definici třídy **NP**. Certifikátem rozumíme binární relaci $R \subset \Sigma^* \times \Sigma_1^*$, kde Σ_1 je další konečná abeceda. Přiřadíme jí jazyk L_R nad abecedou $\Sigma \cup \Sigma_1 \cup \{\circ\}$ definovaný jako

$$L_R = \{u \circ v : \ R(u, v)\} ,$$

kde symbol $\circ$ neleží v Σ. $L \in \mathbf{NP}$, právě když existuje $k \in \mathbf{N}$ a certifikát R takový, že (i) $L_R \in \mathbf{P}$ a (ii) pro každé slovo $u \in \Sigma^*$ platí

$$u \in L \iff \exists\, v \in \Sigma_1^* \, [|v| \le |u|^k + k \;\&\; R(u, v)] .$$

Podmínku (i) nazveme *polynomiální ověřitelností* R a nerovnost $|v| \le |u|^k + k$ v (ii) *polynomiální velikostí* R. R splňující (i) a (ii) nazveme *polynomiálním certifikátem* úlohy L. Podobnou úvahou jako pro třídu **P** nahlédneme, že se lze omezit na polynomiální certifikáty splňující pro každé $u \in \Sigma^*, v \in \Sigma_1^*$ implikaci $R(u, v) \Rightarrow |v| < |u|^k + k$. Je jasné, že $\mathbf{P} \subset \mathbf{NP}$. Definujeme $\mathbf{coNP} = \{L : \ (\Sigma^*\backslash L) \in \mathbf{NP}\}$. Patrně $\mathbf{P} \subset \mathbf{NP} \cap \mathbf{coNP}$. Smysl certifikace je tento. Pokud $L \in \mathbf{NP}$ a nevíme, jestli $L \in \mathbf{P}$, může být pro dané slovo $u \in \Sigma^*$ obtížné rozhodnout, zda $u \in L$. Pokud se nám to už ale po dlouhém výpočtu podaří potvrdit, snadno každého, kdo věci rozumí, ale nemá čas, například šéfa, přesvědčíme o náležení $u \in L$. Předložíme prostě slovo $v \in \Sigma_1^*$ takové, že $|v| < |u|^k + k$ a platí $R(u, v)$; R je polynomiální certifikát L. Šéf pouze v počtu kroků polynomiálním v $|u| + |v|$, což je počet polynomiální i v $|u|$, zkontroluje, že opravdu $u \circ v \in L_R$.

Jako příklad si vezmeme jazyk S obsahující všechna složená přirozená čísla větší než 1. Konkrétněji, $\Sigma = \{0, 1\}$ a čísla jsou kódována svými binárními zápisy. Velikost vstupu $n \in \mathbf{N}$ je tedy $\lceil \log_2 n \rceil$. Například $11001 \in S$ (25 je složené), $11101 \notin S$ (29 není složené) a $0011 \notin S$ (slovo není binárním zápisem čísla z $\mathbf{N}$). Zmínili jsme již, že není známo, zda $S \in \mathbf{P}$. Lehce se vidí, že $S \in \mathbf{NP}$. Certifikát R (zadefinujeme ho neformálně, bez kódování slovy) obsahuje (všechny) trojice (n, k, l) přirozených čísel větších než 1 takové, že $n = kl$. Jde o certifikát S, pro složené $n \in \mathbf{N}$ prostě předložíme některou trojici $(n, k, l) \in R$, a pro nesložené n žádná taková trojice neexistuje. Je polynomiálně velký, protože $k, l < n$, i polynomiálně ověřitelný. Algoritmus rozpoznávající L_R pro každé vstupní slovo nejprve ověří, zda vůbec jde syntakticky o kód trojice čísel (n, k, l). Pokud ne, výpočet ihned ukončí ve stavu NE. Pokud ano, ověří, zda $n, k, l > 1$ & $n = kl$. Pokud ne, přejde do stavu NE, pokud ano, přejde do stavu ANO. Vše trvá jen $O(\log^2 n)$ kroků, protože dobře známý školský algoritmus vynásobí dvě čísla o nejvýše l (binárních) cifrách za $O(l^2)$ kroků.

Zajímavější je množina prvočísel P. Zmínili jsme již, že není známo, zda $P \in \mathbf{P}$. Už víme, že $P \in \mathbf{coNP}$. Ve větě 146 ukážeme, že $P \in \mathbf{NP}$. Doslovný převod definice prvočíselnosti $n \in P \iff n > 1 \; \& \; \forall m < n \; [m = 1 \vee n \not\equiv 0 \bmod m]$ nevede k polynomiálně ověřitelnému certifikátu, neboť dává algoritmus vyžadující více než n kroků (počet kroků exponenciální v $\log n$). Zkusme jiný nápad. Uvažme polynom $Q(x_1, \ldots, x_m)$ z tvrzení 144 a certifikát R obsahující ty $m + 1$-tice $(b, a_1, \ldots, a_m) \in \mathbf{N}_0^{m+1}$, že $Q(a_1, \ldots, a_m) = b$ a $b > 0$. Podle tvrzení 144 jde o certifikát prvočíselnosti (čísla b). Snadno se vidí, že je polynomiálně ověřitelný. Zádrhel ale nyní vězí v druhém požadavku. Bez další analýzy důkazu tvrzení 79, s nímž tvrzení 144 stojí a padá, není jasné, jak se dají, pokud vůbec, pomocí b omezit čísla a_i. Nevíme, zda jde o polynomiálně velký certifikát. Je třeba vymyslet novou definici prvočíselnosti.

Tvrzení 145 (definice prvočíselnosti). *Číslo $n \in \mathbf{N}, n > 1$, je prvočíslo tehdy a jen tehdy, když $n = 2$ nebo existuje $r \in \mathbf{N}, 1 < r < n$, takové, že $r^{n-1} \equiv 1 \bmod n$, ale $r^{(n-1)/q} \not\equiv 1 \bmod n$ pro všechny prvočinitele q čísla $n - 1$.*

Důkaz. Je-li $n = p > 2$ prvočíslo, stačí za r vzít jakýkoli z $\varphi(p-1)$ primitivních elementů pole $\mathbf{Z}_p$ (viz tvrzení 86 v 4.1).

Nechť n je složené a $r \in \mathbf{N}, r^{n-1} \equiv 1 \bmod n$, je libovolné. Tedy $r \perp n$ a podle tvrzení 10 máme $r^{\varphi(n)} \equiv 1 \bmod n$. Nechť $k \in \mathbf{N}$ je nejmenší exponent, pro nějž $r^k \equiv 1 \bmod n$. Patrně $k \backslash (n-1)$ a $k \backslash \varphi(n)$. Protože je n složené, $\varphi(n) < n-1$ a tedy $k < n-1$. Nechť q je libovolný prvočinitel čísla $(n-1)/k$. Dostáváme $r^{(n-1)/q} \equiv 1 \bmod n$, protože exponent je násobek k. Pro složené n požadované r neexistuje. $\diamondsuit$

Věta 146 (Pratt, 1975). *Množina prvočísel P má polynomiální certifikát. Tudíž*

$$P \in \mathbf{NP} \cap \mathbf{coNP} \ .$$

Důkaz. Certifikát R se definuje rekurzivně. Pro n probíhající přirozená čísla větší než 1 obsahuje R všechny seznamy $C(n)$ tvaru $C(2) = *$ a, pro $n > 2$,

$$C(n) = (n, r; q_1, C(q_1), q_2, C(q_2), \ldots, q_k, C(q_k)) \ ,$$

kde $r \in \mathbf{N}$, $1 < r < n$, $r^{n-1} \equiv 1 \bmod n$, $q_i \in \mathbf{N}$, $r^{(n-1)/q_i} \not\equiv 1 \bmod n$ pro $i = 1 \ldots k$ a $q_1 q_2 \ldots q_k = n-1$. Podseznamy $C(q_i)$ mají touž strukturu. R je, podle předchozího tvrzení, vskutku certifikátem prvočíselnosti n. Rekurzivní struktura je vynucena tím, že musíme certifikovat i prvočíselnost čísel q_i. Toto je jeden z certifikátů $C(67)$ prvočísla 67:

$$(67, 2; 2, *, 3, (3, 2; 2, *), 11, (11, 8; 2, *, 5, (5, 3; 2, *, 2, *))) \ .$$

Ukážeme, že R je polynomiálně velký i polynomiálně ověřitelný. Uvidíme, že na uložení seznamu $C(n)$ stačí $O(\log^2 n)$ bitů. Nechť $|C(n)|$ označuje délku slova kódujícího $C(n)$. Indukcí dokážeme nerovnost $|C(n)| < 12(\log_2 n)^2$. Pro $n = 2$ je pravdivá: $|C(2)| = |*| = 1$. Nechť $n \geq 3$ je liché a nerovnost pro čísla menší než n platí. Číslo $n-1$ má $k = \Omega(n-1) \leq \log_2 n$ prvočinitelů (s násobnostmi), mezi nimi určitě $q_1 = 2$. Na uložení čísel $n, r, q_1, \ldots, q_k$ a seznamu $C(q_1) = C(2)$ nám stačí $\lceil \log_2 n \rceil + \lceil \log_2 r \rceil + \lceil \log_2 q_1 \rceil + \cdots + \lceil \log_2 q_k \rceil + 1 \leq 7 \log_2 n$ bitů. Dvě závorky (a) a $2k+1$ oddělovačů , a ; uložíme v $2k + 3 \leq 5k \leq 5 \log_2 n$ bitech. Délka slova kódujícího $C(n)$ tak splňuje

$$|C(n)| \ \leq \ 12 \log_2 n + \sum_{i=2}^{k} |C(q_i)| \leq 12 \log_2 n + 12 \sum_{i=2}^{k} (\log_2 q_i)^2$$

$$
\begin{aligned}
&\leq \; 12\log_2 n + 12\left(\sum_{i=2}^{k} \log_2 q_i\right)^2 = 12\log_2 n + 12\left(\log_2 \frac{n-1}{2}\right)^2 \\
&< \; 12\log_2 n + 12(\log_2 n - 1)^2 \leq 12(\log_2 n)^2 \; .
\end{aligned}
$$

Načrtneme algoritmus rozpoznávající L_R a důkaz jeho polynomiálnosti. Na zkontrolování kongruence $r^{n-1} \equiv 1 \bmod n$ potřebujeme vypočítat mocninu r^{n-1} modulo n. Nechť $l = \lfloor \log_2(n-1) \rfloor$. Po l umocněních na druhou modulo n (každé zvládneme za $O(l^2)$ kroků) vypočteme l čísel $r^1, r^2, r^4, r^8, \ldots, r^{2^l} \bmod n$. Z nich v dalších nejvýše l násobeních vypočteme $r^{n-1} \bmod n$. Celkem nám stačí $O(\log^3 n)$ kroků. Obdobně postupujeme při kontrole kongruencí $r^{(n-1)/q_i} \not\equiv 1 \bmod n$. Všech $k+1$ kongruencí tedy zkontrolujeme za $O(\log^4 n)$ kroků. Na kontrolu rovnosti $q_1 q_2 \ldots q_k = n-1$ nám stačí $O(\log^3 n)$ kroků. Stejně prověříme certifikáty $C(q_1), \ldots, C(q_k)$. Výpočet podobný tomu z předchozího odstavce ukazuje, že algoritmus ověří certifikát za $O(\log^5 n)$ kroků. $\diamondsuit$

5.5 Typický počet prvočinitelů

Funkce $f: \mathbf{N} \to \mathbf{R}$ má *průměrný řád* roven funkci $g: \mathbf{R} \to \mathbf{R}$, pokud pro $x \to \infty$ platí

$$\frac{1}{x} \sum_{m \leq x} f(m) \sim g(x) \; .$$

Řekneme, že f má *normální řád* roven g, pokud pro každé $\varepsilon > 0$ a $x > x_0(\varepsilon)$ platí

$$\#\{m \in \mathbf{N}: \; m \leq x \;\&\; |f(m) - g(m)| > \varepsilon g(m)\} < \varepsilon x \; .$$

Funkce $g(x)$ sloužící k zachycení průměrného a normálního řádu je typicky rostoucí funkce daná jednoduchým analytickým předpisem. Ani jedna definice nezesiluje druhou. Snadno se sestrojí příklad aritmetické funkce, jejíž průměrný řád není jejím normálním řádem. Podobně naopak.

Nalezneme průměrné a normální řády počtu prvočinitelů $\omega(n)$ a počtu prvočinitelů s násobnostmi $\Omega(n)$ (definice viz 1.2).

Tvrzení 147 (průměrné řády ω a Ω). *Existují konstanty $c_1, c_2 \in \mathbf{R}$ takové, že pro $x \to \infty$ platí*

$$\sum_{n \leq x} \omega(n) \;\; = \;\; x \log\log x + c_1 x + O(x \log^{-1} x)$$

$$\sum_{n\le x}\Omega(n) \;=\; x\log\log x + c_2x + O(x\log^{-1}x)\ .$$

Průměrný řád obou funkcí je tedy $\log\log x$.

Důkaz. Nechť $x>0$ je pevné.

$$\begin{aligned}\sum_{n\le x}\omega(n) &= \sum_{n\le x}\sum_{p\backslash n}1\\ &= \sum_{p\le x}\left\lfloor\frac{x}{p}\right\rfloor = x\sum_{p\le x}\frac{1}{p} + O(\pi(x))\\ &= x\log\log x + c_1x + O(x\log^{-1}x)\ .\end{aligned}$$

Použili jsme větu 139 a 2 věty 141. Podobně

$$\sum_{n\le x}\Omega(n) = \sum_{p^m\le x}\left\lfloor\frac{x}{p^m}\right\rfloor = \sum_{n\le x}\omega(n) + \sum_{p^m\le x}\langle m\ge 2\rangle\left\lfloor\frac{x}{p^m}\right\rfloor\ .$$

První sumu už máme odhadnutou. Co se týče druhé,

$$\sum_{p^m\le x}\langle m\ge 2\rangle\left\lfloor\frac{x}{p^m}\right\rfloor = x\sum_{p^m\le x}\frac{\langle m\ge 2\rangle}{p^m} + O(x^{1/2}\log x)\ ,$$

protože je jen $O(x^{1/2}\log x)$ druhých a vyšších mocnin nepřesahujících x. Ovšem

$$\sum_{p^m\le x}\frac{\langle m\ge 2\rangle}{p^m} = \sum_{p^m}\frac{\langle m\ge 2\rangle}{p^m} - \sum_{p^m>x}\frac{\langle m\ge 2\rangle}{p^m}\ .$$

První suma konverguje a druhá, jak ukazuje jednoduchý integrální odhad, je řádu $O(x^{-1})$. Celkem dostáváme dokazovaný odhad pro $\sum_{n\le x}\Omega(n)$. $\diamondsuit$

Nyní dokážeme hlubší výsledek, že $\log\log x$ je i normálním řádem obou aritmetických funkcí.

Věta 148 (Hardy a Ramanujan, 1917). *Funkce* $\omega(n)$ *a* $\Omega(n)$ *mají normální řád* $\log\log n$.

Důkaz. **(Turán, 1934.)** Nechť $a(x)$ je libovolná funkce rostoucí do nekonečna. Ukážeme, že pro $x\to\infty$

$$\#\{n:\ n\le x\ \&\ |\omega(n)-\log\log n| > a(x)\sqrt{\log\log n}\ \} = o(x)\ .$$

Tím dostaneme ještě silnější výsledek, než že normální řád $\omega(n)$ je $\log\log n$. Místo $\log\log n$ lze v poslední formuli psát $\log\log x$, protože $|\log\log x - \log\log n| < \log 2$ pro všechna $n, x^{1/2} < n \le x$. Podle předchozího tvrzení

$$\sum_{n\le x}(\Omega(n)-\omega(n)) = cx + O(x\log^{-1}x)$$

pro nějakou konstantu $c \ge 0$. Sčítance v sumě jsou nezáporné. Pro velké x tak $\Omega(n)-\omega(n) > 2c/\varepsilon$ nastává pro méně než εx čísel $n \le x$ a každý normální řád $\omega(n)$ je i normálním řádem $\Omega(n)$. Důkaz stačí provést jen pro funkci $\omega(n)$.

Začneme odhadem sumy čtverců $\omega(n)$.

$$\begin{aligned}\sum_{n\le x}\omega(n)^2 &= \sum_{n\le x}\Big(\sum_p \langle p\backslash n\rangle\Big)^2 = \sum_{p\le x}\left\lfloor\frac{x}{p}\right\rfloor + \sum_{p,q}\langle p\ne q \;\&\; pq\le x\rangle\cdot\left\lfloor\frac{x}{pq}\right\rfloor\\ &= O(x\log\log x) + x\sum_{p,q}\frac{\langle p\ne q \;\&\; pq\le x\rangle}{pq} + O(x)\ .\end{aligned}$$

První sumu jsme odhadli (dost hrubě) asymptotikou 2 věty 141. Pominutím podmínky $p\ne q$ výraz $x\sum_{p,q}\ldots$ zvětšíme jen o $O(x)$, protože řada $\sum_{n=1}^{\infty}1/n^2$ konverguje. Sumu pak snadno odhadneme shora i zdola:

$$\Big(\sum_p\frac{\langle p\le x^{1/2}\rangle}{p}\Big)^2 \le \sum_{p,q}\frac{\langle pq\le x\rangle}{pq} \le \Big(\sum_p\frac{\langle p\le x\rangle}{p}\Big)^2\ .$$

Podle 2 věty 141 $\sum_{p,q}\langle pq\le x\rangle/pq = (\log\log x)^2 + O(\log\log x)$. Celkem

$$\sum_{n\le x}\omega(n)^2 = x(\log\log x)^2 + O(x\log\log x)\ .$$

Odtud a z první asymptotiky tvrzení 147 plyne, že

$$\begin{aligned}\sum_{n\le x}(\omega(n)-\log\log x)^2 &= \sum_{n\le x}\omega(n)^2 - 2\log\log x\cdot\sum_{n\le x}\omega(n) + \lfloor x\rfloor(\log\log x)^2\\ &= O(x\log\log x)\ .\end{aligned}$$

Řekněme, že výchozí $o(x)$ výsledek neplatí. To jest, existuje $\varepsilon > 0$ a posloupnost čísel (x_i) jdoucí do nekonečna tak, že více než εx_i z čísel n nepřesahujících x_i splňuje

$$|\omega(n)-\log\log x_i| > a(x_i)\sqrt{\log\log x_i}\ .$$

Pro $i = 1, 2, \ldots$ pak máme

$$\sum_{n \le x_i} (\omega(n) - \log\log x_i)^2 > \varepsilon x_i \cdot a(x_i)^2 \log\log x_i \ .$$

To ale není funkce řádu $O(x \log\log x)$ pro $x \to \infty$. Dostali jsme spor. $\diamondsuit$

Skoro všechna n tedy mají cca $\log\log n$ prvočinitelů, ať už počítáno s násobnostmi či bez nich.

Funkce $\omega(n)$ a $\Omega(n)$ mají stejný průměrný i normální řád. Funkce počtu dělitelů $d(n)$ se chová zcela jinak.

Tvrzení 149 (svérázné chování $d(n)$). *Pro každé $\varepsilon > 0$ je pro velké x počet přirozených čísel $n \le x$ nesplňujících*

$$(\log n)^{\log 2 - \varepsilon} < d(n) < (\log n)^{\log 2 + \varepsilon}$$

menší než εx.

DŮKAZ. Protože $2 \le d(p^k) = k + 1 \le 2^k$ a $d(n)$ je multiplikativní, máme nerovnosti

$$2^{\omega(n)} \le d(n) \le 2^{\Omega(n)} \ .$$

Použijeme předchozí větu a uvědomíme si, že $2^{\log\log n} = (\log n)^{\log 2}$. $\diamondsuit$

Funkce $d(n)$ se tedy skoro vždy rovná zhruba $(\log n)^{0.69}$. To však je mnohem méně, než její průměrný řád $\log n$, který odvodíme v kapitole 6. Proto musí existovat zanedbatelná menšina čísel s mimořádně velkým počtem dělitelů.

5.6 Šnirelmanova věta

Předmětem oddílu 5.6 je

Věta 150 (Šnirelman, 1930). *Existuje číslo $h \in \mathbf{N}$ takové, že každé přirozené číslo větší než 1 je součtem nejvýše h prvočísel.*

Důkaz této pozoruhodné věty má jednoduchý kombinatorický základ. Užívá však podstatně horní odhad počtu řešení rovnice $n = p + q$ (tvrzení 154). Jeho důkaz je rovněž elementární, ale poněkud náročnější (tím zajímavější) a zaujímá větší část oddílu. Začneme kombinatorikou.

Pro podmnožinu $A \subset \mathbf{N}$ a číslo $n \in \mathbf{N}$ označíme $A(n)$ počet prvků v $A \cap \{1, 2, \ldots, n\}$. *Šnirelmanova hustota* $Ш(A)$ je infimum

$$Ш(A) = \inf\{A(n)/n : \; n \in \mathbf{N}\} \; .$$

Zřejmě $0 \leq Ш(A) \leq 1$ a $Ш(A) = 1$, právě když $A = \mathbf{N}$. Pokud $1 \not\in A$, $Ш(A) = 0$. Pro každé $n \in \mathbf{N}$ platí $A(n) \geq nШ(A)$. Dále, $Ш(A) > 0$, právě když $1 \in A$ a existují $c > 0$ a n_0 tak, že $A(n)/n > c$ pro $n \geq n_0$.

Pro $A, B \subset \mathbf{N}_0$ označíme $A + B = \{a + b : \; a \in A, b \in B\}$. Vícenásobný součet množin $A_1 + \cdots + A_k$ se definuje obdobně. Pokud $A_1 = \cdots = A_k$, píšeme místo $A + A + \cdots + A$ (k sčítanců) stručněji kA. Množina $A \subset \mathbf{N}_0$ je *bazí* (přesněji, aditivní bazí řádu nejvýše h), pokud $hA = \mathbf{N}_0$ pro nějaké $h \in \mathbf{N}$. Ekvivalentně, A je bazí, pokud $0 \in A$ a pro nějaké pevné $h \in \mathbf{N}$ je každé číslo $n \in \mathbf{N}$ součtem nejvýše h prvků z $A \backslash \{0\}$ (a přesně h prvků z A).

Tvrzení 151 (Šnirelmanova nerovnost). *Nechť $A, B \subset \mathbf{N}_0$ a $0 \in A \cap B$. Pak*

$$Ш(A + B) \geq Ш(A) + Ш(B) - Ш(A) \cdot Ш(B) \; .$$

Důkaz. Označíme $Ш(A) = \alpha$ a $Ш(B) = \beta$. Nechť $A \cap \{0, 1, \ldots, n\} = \{a_0, a_1, \ldots, a_k\}$, kde $0 = a_0 < a_1 < \cdots < a_k \leq n$. Pak, pro každé $n \in \mathbf{N}$,

$$(A + B)(n) \geq A(n) + \sum_{i=0}^{k-1} B(a_{i+1} - a_i - 1) + B(n - a_k) \; ,$$

protože $A(n) = |\{a_i + 0 : \; i = 1, \ldots, k\}|$, $B(a_{i+1} - a_i - 1) = |\{a_i + b : \; b \in B, 0 < b < a_{i+1} - a_i\}|$, $B(n - a_k) = |\{a_k + b : \; b \in B, 0 < b \leq n - a_k\}|$ a tyto množiny jsou disjunktní. Takže

$$\begin{aligned}
(A + B)(n) \;&\geq\; A(n) + \beta \sum_{i=0}^{k-1} (a_{i+1} - a_i - 1) + \beta(n - a_k) = A(n) + \beta(n - k) \\
&=\; A(n) - \beta A(n) + \beta n \geq (1 - \beta)\alpha n + \beta n \\
&=\; (\alpha + \beta - \alpha\beta)n \; .
\end{aligned}$$

$\diamondsuit$

Věta 152 (Šnirelman, 1930). *Každá množina $A \subset \mathbf{N}_0$ taková, že $0 \in A$ a $Ш(A) > 0$, je bazí.*

Důkaz. Ekvivalentní tvar nerovnosti z tvrzení 151 je $1 - Ш(A + B) \leq (1 - Ш(A))(1 - Ш(B))$. Odtud indukcí plyne nerovnost

$$1 - Ш(hA) \leq (1 - Ш(A))^h \ .$$

Protože $1 - Ш(A) < 1$, pro dosti velké $h_0 \in \mathbf{N}$ máme $Ш(h_0A) \geq 1/2$. Ukážeme, že

$$(2h_0)A = h_0A + h_0A = \mathbf{N}_0 \ .$$

Nechť $n \in \mathbf{N}_0$. Množiny

$$\{i : \ 0 \leq i \leq n, i \in h_0A\} \quad \text{a} \quad \{n - j : \ 0 \leq j \leq n, j \in h_0A\}$$

mají každá $(h_0A)(n) + 1 \geq n/2 + 1$ prvků, obě dohromady alespoň $n+2$. To je ale více než má prvků množina $\{0, 1, \ldots, n\}$, v níž jsou obsaženy. Musejí se protínat, $i = n - j$ pro nějaká i a j. Takže $n = i + j \in h_0A + h_0A$. $\diamondsuit$

Zajímavé, je to ale vůbec k něčemu? Vždyť pro množinu prvočísel P podle věty 139 máme $Ш(\{1\} \cup P) = 0$ a předchozí věta se pro $A = \{0, 1\} \cup P$ nedá použít. Vtip je v tom, že se dá použít pro $A = \{0, 1\} \cup 2P$.

Tvrzení 153 ($P + P$ je hustá). *Nechť*

$$X = P + P = \{p + q : \ p \text{ a } q \text{ jsou prvočísla}\} \ .$$

Pak $Ш(\{1\} \cup X) > 0$.

To plyne z následujícího hlubokého výsledku.

Tvrzení 154 (odhad počtu řešení $n = p + q$). *Nechť $r(n)$ je počet řešení rovnice $n = p + q$, kde p a q jsou prvočísla. Pro $n = 1, 2, \ldots$ platí*

$$r(n) = \sum_{p,q} \langle n = p + q \rangle \ll \frac{n}{\log^2 n} \cdot \prod_{p \backslash n} \left(1 + \frac{1}{p}\right) \ .$$

Důkaz tvrzení 153. Podle Cauchyho nerovnosti

$$\left(\sum_{n \leq m} r(n)\right)^2 \leq \sum_{n \leq m} \langle r(n) > 0 \rangle 1^2 \cdot \sum_{n \leq m} r(n)^2 \ ,$$

takže

$$\frac{X(m)}{m} \geq \frac{1}{m} \cdot \frac{\left(\sum_{n \leq m} r(n)\right)^2}{\sum_{n \leq m} r(n)^2} \ .$$

Odhadneme zdola čitatele.

$$\sum_{n\le m} r(n) = \#\{(p,q):\ p+q\le m\} \ge \pi(m/2)^2 \gg m^2/\log^2 m$$

(podle věty 139). Čitatel je tedy $\gg m^4/\log^4 m$. Zbývá odhadnout shora jmenovatele. Podle tvrzení 154

$$\sum_{n\le m} r(n)^2 \ll \frac{m^2}{\log^4 m}\cdot \sum_{n\le m}\prod_{p\backslash n}\left(1+\frac{1}{p}\right)^2 .$$

Platí odhad (podmínka pro d_i je zkratka pro konjunkci podmínek pro d_1 a d_2)

$$\begin{aligned}
\sum_{n\le m}\prod_{p\backslash n}\left(1+\frac{1}{p}\right)^2 &\le \sum_{n\le m}\Big(\sum_{d\backslash n} 1/d\Big)^2 = \sum_{n,d_i}\frac{\langle n\le m\ \&\ d_i\backslash n\rangle}{d_1d_2}\\
&= \sum_{d_i}\frac{\langle d_i\le m\rangle}{d_1d_2}\cdot\sum_{n}\langle n\le m\ \&\ d_i\backslash n\rangle\\
&= \sum_{d_i}\frac{\langle d_i\le m\rangle}{d_1d_2}\cdot\sum_{n\le m}\langle [d_1,d_2]\backslash n\rangle\\
&\le \sum_{d_i\le m}\frac{m}{d_1d_2[d_1,d_2]}\\
&\le m\sum_{d_i\le m}(d_1d_2)^{-3/2} \le m\Big(\sum_{d=1}^{\infty} d^{-3/2}\Big)^2\\
&\ll m
\end{aligned}$$

(užili jsme nerovnost $[d_1,d_2]=d_1d_2/(d_1,d_2)\ge (d_1d_2)^{1/2}$). Jmenovatel tedy je $\ll m^3/\log^4 m$. Celkem, pro $m\ge 4$, platí

$$\frac{X(m)}{m} \gg \frac{1}{m}\cdot\frac{m^4/\log^4 m}{m^3/\log^4 m} = 1$$

a Ш$(\{1\}\cup X)>0$. ◊

Nyní už umíme dokázat, že množina prvočísel (s nulou a jedničkou) je aditivní bazí.

Důkaz věty 150. Připomínáme, že $X = P + P$ sestává z čísel, která jsou součtem dvou prvočísel. Podle věty 152 a tvrzení 153 existuje $h\in\mathbf{N}$ takové, že

$$h(\{0,1\}\cup X) = \mathbf{N}_0 .$$

Ukážeme, že každé $n \in \mathbf{N}$ větší než 1 je součtem nejvýše $2h+1$ prvočísel. Pro $n = 2$ není co dokazovat. Pro $n > 2$ vyjádříme n jako $n = 2 + (n-2)$ a $n-2$ napíšeme jako součet nejvýše $2h - 2l$ prvočísel a l jedniček. Pokud $l = 0$, jsme hotovi. Pokud $l = 1$, nahradíme $2+1$ sčítancem 3 a n máme vyjádřeno součtem nejvýše $2h - 1$ prvočísel. Pokud $l > 1$, nahradíme jedničky stejným součtem menšího počtu dvojek a trojek (např. $1+1+1+1+1 = 2+3$). V každém případě je n součtem nejvýše $2h+1$ prvočísel. $\diamondsuit$

Zbývá ovšem dokázat tvrzení 154. To nám zabere zbytek oddílu. Číslo $z \in \mathbf{R}$ buď kladné a $D \subset \mathbf{N}$ buď množina všech čtvercuprostých přirozených čísel menších než z. Nechť $g : \mathbf{N} \to (0,1]$ je úplně multiplikativní funkce splňující $g(1) = 1$ a $0 < g(n) < 1$ pro $n > 1$. Nechť $G(\lambda_d : \ d \in D)$ je kvadratická forma v $|D|$ neznámých λ_d odpovídajících číslům $d \in D$, definovaná jako

$$G = \sum_{d_1, d_2 \in D} \frac{g(d_1)\lambda_{d_1} g(d_2)\lambda_{d_2}}{g((d_1, d_2))} \ .$$

Dále pro čtvercuprosté $l \in \mathbf{N}$ označíme

$$f(l) = \sum_{d \backslash l} \frac{\mu(d)}{g(l/d)} = \frac{1}{g(l)} \sum_{d \backslash l} \mu(d) g(d) = \frac{1}{g(l)} \prod_{p \backslash l} (1 - g(p)) > 0$$

a pro $d \in D$

$$\alpha_d = \sum_l \frac{\langle dl \in D \rangle}{f(l)} \ .$$

Povšimněme si, že $f(l)$ je multiplikativní a podle Möbiovy inverzní formule (tvrzení 7 v kapitole 1)

$$\frac{1}{g(k)} = \sum_{d \backslash k} f(d) \ .$$

Lemma 155. *Pro $d \in D$ označme*

$$\lambda_d^* = \frac{\mu(d)\alpha_d}{f(d)g(d)\alpha_1} \ .$$

Pak

1. $\lambda_1^* = 1$ *a* $|\lambda_d^*| \le 1$ *pro všechna* $d \in D$.

2. *Pro každé* $k \in D$ *platí, že* $\sum_{d \in D} \langle k \backslash d \rangle \cdot g(d) \lambda_d^* = \mu(k)/(\alpha_1 f(k))$.

3. $G(\lambda_d^*:\ d\in D) = (\alpha_1)^{-1}$.

4. $\alpha_1 = \sum_{k\in D} f(k)^{-1} \geq \sum_{k<z} g(k)$.

DŮKAZ. **1.** $\mu(1)=g(1)=f(1)=1$, takže $\lambda_1^*=1$. Pro libovolné $d\in D$ máme

$$\begin{aligned}
\alpha_1 &= \sum_{k\in D}\frac{1}{f(k)} = \sum_l \langle l\backslash d\rangle \sum_{k\in D}\frac{\langle (k,d)=l\rangle}{f(k)}\\
&= \sum_l \frac{\langle l\backslash d\rangle}{f(l)}\sum_m \frac{\langle ml\in D\ \&\ (m,d/l)=1\rangle}{f(m)}\\
&\geq \sum_l \frac{\langle l\backslash d\rangle}{f(l)}\sum_m \frac{\langle md\in D\rangle}{f(m)} = \sum_m \frac{\langle md\in D\rangle}{f(m)}\sum_l \frac{\langle l\backslash d\rangle}{f(l)}\\
&= \frac{\alpha_d}{f(d)}\sum_l \langle l\backslash d\rangle f(d/l)\\
&= \frac{\alpha_d}{f(d)g(d)}\ ,
\end{aligned}$$

kde jsme v poslední úpravě použili hořejší vyjádření $1/g(k)$. Tudíž $|\lambda_d^*| = \alpha_d/(f(d)g(d)\alpha_1)\leq 1$.
2. Nechť $k\in D$. Pak

$$\begin{aligned}
\sum_{d\in D}\langle k\backslash d\rangle g(d)\lambda_d^* &= \sum_{d\in D}\langle k\backslash d\rangle g(d)\frac{\mu(d)\alpha_d}{f(d)g(d)\alpha_1}\\
&= \frac{1}{\alpha_1}\sum_l \langle kl\in D\rangle\frac{\mu(kl)\alpha_{kl}}{f(kl)}\\
&= \frac{\mu(k)}{\alpha_1 f(k)}\sum_l \langle kl\in D\rangle\frac{\mu(l)}{f(l)}\sum_m\frac{\langle klm\in D\rangle}{f(m)}\\
&= \frac{\mu(k)}{\alpha_1 f(k)}\sum_l \langle kl\in D\rangle\mu(l)\sum_m\frac{\langle klm\in D\rangle}{f(lm)}\\
&= \frac{\mu(k)}{\alpha_1 f(k)}\sum_n \frac{\langle kn\in D\rangle}{f(n)}\sum_l\langle l\backslash n\rangle\mu(l)\\
&= \frac{\mu(k)}{\alpha_1 f(k)}\ \text{(tvrzení 7)}\ .
\end{aligned}$$

3.

$$G(\lambda_d:\ d\in D) = \sum_{d_i\in D}\frac{g(d_1)\lambda_{d_1}g(d_2)\lambda_{d_2}}{g((d_1,d_2))}$$

$$
\begin{aligned}
&= \sum_{d_i \in D} \sum_{k \backslash d_i} f(k) g(d_1)\lambda_{d_1} g(d_2)\lambda_{d_2} \text{ (vyjádření } 1/g(k) \text{ výše)} \\
&= \sum_{k \in D} f(k) \sum_{d_i \in D} \langle k\backslash d_1 \ \&\ k\backslash d_2 \rangle g(d_1)\lambda_{d_1} g(d_2)\lambda_{d_2} \\
&= \sum_{k \in D} f(k) \Big(\sum_{d \in D} \langle k \backslash d \rangle g(d) \lambda_d \Big)^2 .
\end{aligned}
$$

Položíme-li $\lambda_d = \lambda_d^*$, dostaneme podle 2

$$
G(\lambda_d^* :\ d \in D) = \sum_{k \in D} f(k) \left(\frac{\mu(k)}{\alpha_1 f(k)} \right)^2 = \frac{1}{\alpha_1^2} \sum_{k \in D} \frac{1}{f(k)} = \frac{1}{\alpha_1} .
$$

4.

$$
\begin{aligned}
\sum_{k \in D} \frac{1}{f(k)} &= \sum_{k \in D} g(k) \prod_{p \backslash k} (1 - g(p))^{-1} \\
&= \sum_{k \in D} g(k) \prod_{p \backslash k} (1 + g(p) + g(p^2) + \cdots) \\
&= \sum_{k \in D} g(k) \sum_{l} \langle p \backslash l \Rightarrow p \backslash k \rangle g(l) \\
&= \sum_{k,l} \langle k \in D \ \&\ (p\backslash l \Rightarrow p \backslash k) \rangle g(kl) \\
&= \sum_{m} g(m) \sum_{k} \langle k \in D \ \&\ k \backslash m \ \&\ (p \backslash (m/k) \Rightarrow p \backslash k) \rangle \\
&\geq \sum_{m<z} g(m)
\end{aligned}
$$

(pro $m < z$ je poslední vnitřní suma vždy ≥ 1, za k lze totiž vzít čtvercuprostou část m). $\diamondsuit$

Funkce g buď jako výše. $A \subset \mathbf{N}$ buď daná konečná posloupnost. Pro $d \in \mathbf{N}$ označíme

$$
r_d = |\{a \in A :\ d \backslash a\}| - g(d)|A| .
$$

Věta 156 (Selberg, 1947). *Veličiny z, g, A a r_d buďte jako výše. Připomínáme, že $D = \{n \in \mathbf{N} :\ \mu(n) \neq 0 \ \&\ n < z\}$. Nechť*

$$
S(A, z) = \#\{a \in A :\ a \perp d \textit{ pro všechny } d \in D\} .
$$

Potom

$$
S(A, z) \leq \frac{|A|}{\sum_{k<z} g(k)} + \sum_{d<z^2} 3^{\omega(d)} |r_d| .
$$

DŮKAZ. Pro každou sadu $|D|$ reálných čísel $\lambda_d, d \in D, \lambda_1 = 1$, platí

$$\begin{aligned} S(A,z) = \sum_a \langle a \in A \;\&\; (a,d) = 1 \;\forall d \in D\rangle &\le \sum_{a\in A} \Big(\sum_{d\in D} \langle d \backslash a\rangle \lambda_d \Big)^2 \\ = \sum_{d_i \in D} \lambda_{d_1}\lambda_{d_2} \sum_{a\in A} \langle [d_1, d_2] \backslash a\rangle & \\ = \sum_{d_i \in D} \lambda_{d_1}\lambda_{d_2} (g([d_1,d_2])|A| + r_{[d_1,d_2]}) & \\ = |A| \sum_{d_i\in D} \frac{\lambda_{d_1}\lambda_{d_2} g(d_1 d_2)}{g((d_1,d_2))} + \sum_{d_i \in D} \lambda_{d_1}\lambda_{d_2} r_{[d_1,d_2]} & \\ = |A| G(\lambda_d :\; d \in D) + R \;. & \end{aligned}$$

Položíme $\lambda_d = \lambda_d^*$ (to můžeme, $\lambda_1^* = 1$). Podle 3 a 4 předešlého lemmatu máme pro první sčítanec horní odhad $|A|/\sum_{k<z} g(k)$. Odhadneme R (užíváme 1 předešlého lemmatu):

$$|R| \le \sum_{d_i \in D} |r_{[d_1,d_2]}| = \sum_d |r_d| \sum_{d_i} \langle d_i \in D \;\&\; [d_1,d_2] = d\rangle \;.$$

Zřejmě $d_1, d_2 \in D$ implikuje $d = [d_1, d_2] < z^2$ a d je čtvercuprosté. Spočítáme, kolik je pro dané čtvercuprosté $d \in \mathbf{N}$ dvojic d_1, d_2 s $[d_1, d_2] = d$. Nechť $\omega(d) = n$. Počet uvažovaných dvojic je právě počet dvojic množin (X, Y) takových, že $X \cup Y = \{1, 2, \ldots, n\}$, to jest počet dvojic (X, Z), že $\{1, 2, \ldots, n\} \supset X \supset Z$ $(Z = X \cap Y)$. Hledaný počet tedy je $(k = |X|)$ $\sum_{k=0}^n \binom{n}{k} 2^k = (2+1)^n = 3^{\omega(d)}$. Na čtvercuprostost d zapomeneme a máme horní odhad R. ♢

DŮKAZ TVRZENÍ 154. Nechť $n \in \mathbf{N}$ je pevné sudé číslo (pro liché n odhad $r(n)$ platí triviálně). Pomocí věty 156 odhadneme $r(n) = \sum_{p,q} \langle p + q = n\rangle$. Položíme $z = n^{1/8}$, $D = \{m :\; m < z \;\&\; \mu(m) \neq 0\}$ a

$$A = (m(n-m) :\; m = 1, 2, \ldots, n-1) \;.$$

Úplně multiplikativní funkce g splňuje $g(1) = 1$ a je dána svými prvočíselnými hodnotami:

$$g(p) = \begin{cases} \dfrac{2}{p} & \ldots\; p \text{ nedělí } n \\[2ex] \dfrac{1}{p} & \ldots\; p \text{ dělí } n \;. \end{cases}$$

Protože n je sudé, $0 < g(m) < 1$ pro $m > 1$. Když $z < m < n - z$ a $(m(n-m), d) > 1$ pro nějaké $d \in D$, nutně m nebo $n - m$ je složené a $n = m + (n - m)$ nepřispívá do $r(n)$. Takže

$$r(n) \leq 2n^{1/8} + S(A, z)\ .$$

Podle věty 156

$$S(A, z) \leq \frac{|A|}{\sum_{k<z} g(k)} + \sum_{d<z^2} 3^{\omega(d)} |r_d|\ .$$

Odhadneme první sčítanec. Nechť $k \in \mathbf{N}$ je libovolné a s_i jsou exponenty těch prvočísel v rozkladu k, která nedělí n. Nechť $d_n(k)$ je počet dělitelů čísla k nesoudělných s n. Pak

$$g(k) = \frac{2^{s_1+s_2+\cdots}}{k} \geq \frac{\prod(s_i+1)}{k} = \frac{d_n(k)}{k}\ .$$

Označíme $P_n = \{m \in \mathbf{N} :\ p \backslash m \Rightarrow p \backslash n\}$. Pak

$$\begin{aligned}
\frac{\sum_{k<z} g(k)}{\prod_{p\backslash n}(1-1/p)} &\geq \sum_{k<z} \frac{d_n(k)}{k} \sum_{l=1}^{\infty} \frac{\langle l \in P_n \rangle}{l} \\
&= \sum_{k<z} d_n(k) \sum_{t=1}^{\infty} \frac{\langle k \backslash t\ \&\ t/k \in P_n \rangle}{t} \\
&= \sum_{t=1}^{\infty} \frac{1}{t} \sum_{k<z} \langle k \backslash t\ \&\ t/k \in P_n \rangle d_n(k) \\
&\geq \sum_{t<z} \frac{1}{t} \sum_{k} \langle k \backslash t\ \&\ t/k \in P_n \rangle d_n(k).
\end{aligned}$$

Nechť $t = t_1 t_2$, kde $t_1 \in P_n$ a $t_2 \perp n$. Vnitřní suma obsahuje $d(t_1)$ sčítanců (k probíhá čísla $it_2, i \backslash t_1$), z nichž každý se rovná $d(t_2)$. Celkem se vnitřní suma rovná $d(t_1)d(t_2) = d(t)$ (protože $t_1 \perp t_2$). Tedy

$$\frac{|A|}{\sum_{k<z} g(k)} \leq \frac{|A| \prod_{p\backslash n}(1-1/p)^{-1}}{\sum_{t<z} d(t)/t} \ll \frac{n}{\log^2 n} \cdot \prod_{p\backslash n} \left(1 + \frac{1}{p}\right)\ ,$$

protože $|A| = n - 1$, součin $\prod_p (1 + (p^2-1)^{-1})$ konverguje a $\sum_{t<z} d(t)/t \sim \frac{1}{2} \log^2 z \gg \log^2 n$. Asymptotika pro $\sum_{t<z} d(t)/t$ vyplývá Abelovou sumací (tvrzení 18 v 1.4) z asymptotiky $\sum_{t<z} d(t) \sim z \log z$, kterou odvodíme (dosti jednoduše) v příští kapitole.

Nyní druhý sčítanec v horním odhadu $S(A,z)$. Nechť číslo d je čtvercuprosté a $d = p_1 \dots p_a q_1 \dots q_b$, kde p_i dělí n a q_i nedělí n. Zřejmě

$$m(n-m) \equiv 0 \bmod d \Longleftrightarrow \forall p \backslash d\, [m \equiv 0 \text{ nebo } m \equiv n \bmod p]\ .$$

Pro $p = p_i$ obě kongruence splývají, pro $p = q_i$ jsou různé. Podle tvrzení 5 v 1.2 existuje 2^b různých čísel $i_1, \dots, i_{2^b}$ v $\{0, 1, \dots, d-1\}$ takových, že

$$m(n-m) \equiv 0 \bmod d \Longleftrightarrow \exists j\ [m \equiv i_j \bmod d]\ .$$

Takže

$$2^b \left\lfloor \frac{n-1}{d} \right\rfloor \le |\{a \in A:\ d \backslash a\}| \le 2^b \left\lceil \frac{n-1}{d} \right\rceil\ .$$

Protože $g(d) = 2^b/d$,

$$|r_d| = |\#\{a \in A:\ d \backslash a\} - g(d)(n-1)| \le 2^b \le 2^{\omega(d)}\ .$$

Druhý sčítanec je v porovnáním s prvním zanedbatelný (užijeme nerovnost $2^{\omega(d)} \le d$ a rovnost $z = n^{1/8}$):

$$\begin{aligned} \sum_{d<z^2} 3^{\omega(d)} |r_d| &\le \sum_{d<z^2} 6^{\omega(d)} \le \sum_{d<z^2} 2^{\omega(d)\log_2 6} \\ &\le z^2 \cdot z^{2\log_2 6} = n^{(2+2\log 6/\log 2)/8} \\ &< n^{9/10}\ . \end{aligned}$$

Důkaz tvrzení 154 je dokončen (až na rest $\sum_{n<x} d(n) \sim x \log x$) a důkaz věty 150 je úplný. Pozoruhodný důkaz!

5.7 Prvočíselná věta

Následující Prvočíselná věta patří k nejznámějším výsledkům teorie čísel. V 5.7.1 ji dokážeme komplexní analýzou a v 5.7.2 elementárně.

Věta 157 (Hadamard, 1896; de La Valée Poussin, 1896). *Počet prvočísel nepřesahujících x má pro $x \to \infty$ asymptotiku*

$$\pi(x) \sim \frac{x}{\log x}\ .$$

Nejprve uvedeme její dvě klasické ekvivalentní formulace. Ekvivalence je míněna ve smyslu relativně jednoduché vzájemné převeditelnosti. Připomínáme, že Čebyševova funkce ϑ je definována sumou $\vartheta(x) = \sum_{p \le x} \log p$.

Tvrzení 158 (via Čebyševova funkce). *Nechť ϑ je Čebyševova funce. Prvočíselná věta je ekvivalentní asymptotice*

$$\vartheta(x) \sim x \ .$$

DŮKAZ. Nerovnost $\vartheta(x) \le \pi(x) \log x$ je zřejmá. Z druhé strany,

$$\begin{aligned} \vartheta(x) &\ge \sum_p \langle x^{1-\varepsilon} \le p \le x \rangle \cdot \log p \ge (1-\varepsilon)(\pi(x) - x^{1-\varepsilon}) \log x \\ &> (1-\varepsilon)\pi(x) \log x - x^{1-\varepsilon} \log x \end{aligned}$$

pro každé pevné $\varepsilon > 0$. Tedy $\pi(x) \sim x/\log x$, právě když $\vartheta(x) \sim x$. ♢

Budeme pracovat se sumatorními funkcemi

$$M(x) = \sum_{n \le x} \mu(n) \ \text{ a } \ \psi(x) = \sum_{n \le x} \Lambda(n) \ ,$$

kde μ je Möbiova funkce (viz 1.2) a Λ von Mangoldtova funkce (viz 5.3). I funkci ψ se říká Čebyševova funkce. Je jasné, že $\vartheta(x) - \psi(x) = O(x^{1/2} \log^2 x)$, protože ψ má navíc jen sčítance přes druhé a vyšší mocniny (prvočísel) nepřesahující x. Bude se nám hodit jedna transformace sum.

Tvrzení 159 (hyperbolový trik). *Funkce $f, g : \mathbf{N} \to \mathbf{C}$ mějte sumatorní funkce $F(x) = \sum_{n \le x} f(n)$ a $G(x) = \sum_{n \le x} g(n)$. Pro každé x a y, $1 \le y \le x$, platí*

$$\sum_{n \le x} \sum_{d \backslash n} f(d) g(n/d) = \sum_{n \le x/y} g(n) F(x/n) + \sum_{n \le y} f(n) G(x/n) - F(y) G(x/y) \ .$$

DŮKAZ. Dvojitá suma vlevo je vlastně součet $\sum f(k)g(l)$ přes dvojice $X = \{(k,l) \in \mathbf{N}^2 : \ kl \le x\}$. Dvě sumy vpravo jsou součty přes množiny $Y = \{(k,l) \in X : \ l \le x/y\}$ a $Z = \{(k,l) \in X : \ k \le y\}$. Vzhledem k $X = Y \cup Z$ dostaneme rovnost, když ještě odečteme sumu přes $Y \cap Z$, což je přesně poslední člen. ♢

Tvrzení 160 (via Möbiova funkce). *Nechť μ je Möbiova funkce. Prvočíselná věta je ekvivalentní limitě*

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n\le x}\mu(n)=0\ .$$

Jinak řečeno, $\pi(x)\sim x\log^{-1}x$ je ekvivalentní $M(x)=o(x)$.

DŮKAZ. Toto přeformulování leží hlouběji. Nechť platí Prvočíselná věta. Pak, podle tvrzení 158 a následné poznámky, $\psi(x)\sim x$. Pro $n\in\mathbf{N}$ platí identita

$$\mu(n)\log n=-\sum_{d\backslash n}\mu(d)\cdot\Lambda(n/d)\ .$$

Pro čtvercuprosté n platí triviálně. Pro $\mu(n)=0$ máme vlevo nulu. Nechť p je takové, že $\mathrm{ord}_p(n)>1$. Každé dva sčítance a a b vpravo odpovídající dělitelům d a pd, kde $p\perp d$, splňují $a=-b$. Pro ostatní d je sčítanec vpravo nulový. Nulu tak máme i vpravo.

Sumace přes $n\le x$ a tvrzení 6 dávají

$$\begin{aligned}\sum_{n\le x}\mu(n)\log n &= -1+\sum_{n\le x}\sum_{d\backslash n}\mu(d)\cdot(1-\Lambda(n/d))\\ &= -1+\sum_{n\le x}\mu(n)\cdot(\lfloor x/n\rfloor-\psi(\lfloor x/n\rfloor))\ .\end{aligned}$$

Podle Abelovy sumace (tvrzení 18) máme vlevo vlastně $M(x)\log x+O(x)$. Podle předpokladu, $|\lfloor x/n\rfloor-\psi(\lfloor x/n\rfloor)|<\varepsilon x/n$, jakmile $x/n>A=A_\varepsilon$. Podle lemmatu 138 je tento výraz $<Bx/n$ pro všechna x/n a absolutní konstantu B. Takže

$$\begin{aligned}|M(x)|\log x &< O(x)+\sum_{n\le x/A}\varepsilon x/n+\sum_{x/A<n\le x}Bx/n\\ &= \varepsilon x\log(x/A)+Bx\log A+O(x)\\ &< 2\varepsilon x\log x\ ,\end{aligned}$$

pro dostatečně velké x. Tedy $M(x)=o(x)$.

Pro důkaz opačné implikace potřebujeme opět (jako v důkazu tvrzení 154) průměrný řád $d(n)$, nyní ale v přesnější podobě

$$\sum_{n\le x}d(n)=x\log x+(2\gamma-1)x+O(\sqrt{x})$$

($\gamma = 0.57721\ldots$ je Eulerova–Mascheroniova konstanta). Tuto asymptotiku dokážeme poměrně jednoduše v příští kapitole.

Vyjdeme z identity $\Lambda(n) = \sum_{d\backslash n} \log(d)\cdot\mu(n/d)$, která je Möbiovou inverzí (tvrzení 7 v 1.2) identity $\sum_{d\backslash n}\Lambda(d) = \log n$ z důkazu lemmatu 136. My ale potřebujeme $\Lambda(n)-1$. Využijeme proto identitu $1 = \sum_{d\backslash n} d(d)\cdot\mu(n/d)$, která je Möbiovou inverzí definice $d(n)$. Tedy

$$\begin{aligned}\Lambda(n)-1 &= \sum_{d\backslash n}(\log d - d(d))\cdot\mu(n/d)\\ &= \sum_{d\backslash n}(\log d - d(d)+2\gamma)\cdot\mu(n/d) - 2\gamma\delta_{1n}\ .\end{aligned}$$

Označme $f(n) = \log n - d(n) + 2\gamma$. Podle (zatím nedokázaného) průměrného řádu $d(n)$ a podle tvrzení 16 z 1.4,

$$F(x) := \sum_{n\le x} f(n) = O(\sqrt{x})\ .$$

Sečtení pro $n \le x$ dává, s obratem z tvrzení 159,

$$\begin{aligned}\psi(x) - \lfloor x\rfloor &= \sum_{n\le x}\sum_{d\backslash n} f(d)\cdot\mu(n/d) - 2\gamma\\ &= \sum_{n\le x/y}\mu(n)F(x/n) + \sum_{n\le y} f(n)M(x/n) - F(y)M(x/y) - 2\gamma\ ,\end{aligned}$$

kde y, $2 < y < x$, je pevný parametr. Za předpokladu $M(x) = o(x)$ a díky $F(x) = O(\sqrt{x})$,

$$\begin{aligned}|\psi(x) - x| &< \sum_{n\le x/y}|F(x/n)| + o_y(x) + o_y(x)\\ &\ll \sqrt{x}\sum_{n\le x/y} 1/\sqrt{n} + o_y(x)\\ &\ll x/\sqrt{y} + o_y(x)\ .\end{aligned}$$

Protože tento odhad platí pro každé pevné y, z $M(x) = o(x)$ plyne Prvočíselná věta ve tvaru $\psi(x) - x = o(x)$. $\diamondsuit$

5.7.1 Newmanův analytický důkaz

Prvočíselnou větu dokážeme ve formulaci tvrzení 158. Důkaz je založen na vlastnostech *Riemannovy zeta funkce*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}\ , \quad \text{kde } s \in \mathbf{C}\ .$$

Řada konverguje absolutně a stejnoměrně v každé polorovině $\mathrm{Re}(s) > t > 1$, definuje proto v $\mathrm{Re}(s) > 1$ holomorfní funkci. Ta se dá holomorfně rozšířit na celé $\mathbf{C}$, kromě jednoduchého pólu v $s = 1$. Nám postačí rozšíření na $\mathrm{Re}(s) > 0$.

Tvrzení 161 (rozšíření $\zeta(s)$). *Funkci*

$$\zeta(s) - \frac{1}{s-1}$$

lze holomorfně rozšířit do poloroviny $\mathrm{Re}(s) > 0$.

Důkaz. V $\mathrm{Re}(s) > 1$ máme vyjádření

$$\begin{aligned}\zeta(s) - \frac{1}{s-1} &= \sum_{n=1}^{\infty} n^{-s} - \int_1^{\infty} x^{-s} dx = \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - x^{-s})\, dx \\ &= \sum_{n=1}^{\infty} F_n(s)\ .\end{aligned}$$

Funkce $F_n(s)$ jsou, podle standardních výsledků o integrálních reprezentacích, celistvé (holomorfní v $\mathbf{C}$). Dále

$$|F_n(s)| = \left| s \int_n^{n+1} \int_n^x u^{-s-1}\, du\, dx \right| \le |s| \max_{n \le u \le n+1} |u^{-s-1}| = \frac{|s|}{n^{\mathrm{Re}(s)+1}}\ .$$

Suma $\sum_n F_n(s)$ tudíž v $\mathrm{Re}(s) > 0$ konverguje absolutně a na kompaktních podmnožinách stejnoměrně. Definuje tedy v $\mathrm{Re}(s) > 0$ holomorfní funkci, která rozšiřuje $\zeta(s) - (s-1)^{-1}$. $\diamondsuit$

Je jasné, že $\zeta(s) \neq 0$ pro $\mathrm{Re}(s) > 1$. Eulerova identita z třetího důkazu v 5.1 platí totiž i v $\mathrm{Re}(s) > 1$ a nekonečný součin na levé straně nekonverguje k 0, neboť

$$\sum_p \log\left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{p,n} \frac{1}{np^{ns}} = \sum_{n=1}^{\infty} \frac{1}{n} \sum_p p^{-ns}$$

v $\mathrm{Re}(s) > 1$ absolutně konverguje.

Tvrzení 162 (nenulovost $\zeta(s)$ na $\mathrm{Re}(s)=1$). *Funkce $\zeta(s)$ je nenulová v uzavřené polorovině $\mathrm{Re}(s)\ge 1$.*

Důkaz. **(Mertens, 1898.)** Pro $\mathrm{Re}(s)>1$ to již víme, zbývá přímka $\mathrm{Re}(s)=1$. Uvažme pro $u,t\in\mathbf{R}, u>1$, a $s=u+it$ funkci

$$G(s)=G(u+it)=\zeta(u)^3\zeta(u+it)^4\zeta(u+2it)\ .$$

Podle Eulerovy identity z 5.1 a rovnosti $\mathrm{Re}(\log z)=\log|z|$

$$\begin{aligned}\log|\zeta(s)| &= \mathrm{Re}\Big(\sum_p \log(1-p^{-s})^{-1}\Big)\\ &= \mathrm{Re}\Big(\sum_p \Big(p^{-s}+\frac{p^{-2s}}{2}+\frac{p^{-3s}}{3}+\cdots\Big)\Big)\\ &= \mathrm{Re}\Big(\sum_n a_n n^{-s}\Big)\ ,\end{aligned}$$

kde čísla a_n jsou reálná a nezáporná. Pro každé $u>1$ a t tedy platí

$$\begin{aligned}\log|G(s)| &= \mathrm{Re}\Big(\sum_{n=1}^{\infty} a_n n^{-u}(3+4n^{-it}+n^{-2it})\Big)\\ &= \sum_{n=1}^{\infty} a_n n^{-u}(3+4\cos(t\log n)+\cos(2t\log n))\\ &= \sum_{n=1}^{\infty} a_n n^{-u} 2(1+\cos(t\log n))^2\\ &\ge 0\ ,\end{aligned}$$

díky identitě $\cos 2x = 2\cos^2 x - 1$.

Kdyby $\zeta(s)$ měla v $1+it_0$ kořen násobnosti $k\ge 1$, pro $u\to 1^+$ by platilo

$$G(u+it_0)\sim (u-1)^{-3}(u-1)^{4k}\zeta(u+2it_0)\to 0$$

(alespoň čtyřnásobný kořen $\zeta(s)^4$ v $s=1+it_0$ „přebije“ trojnásobný pól $\zeta(s)^3$ v $s=1$) a $\log|G(u+it_0)|\to -\infty$, což je spor. $\diamondsuit$

Tvrzení použijeme k holomorfnímu rozšíření funkce

$$F(s)=\sum_p \frac{\log p}{p^s}\ .$$

Lemma 163. *$F(s)-1/(s-1)$ se dá holomorfně rozšířit na $\mathrm{Re}(s) \geq 1$. (Tím se rozumí rozšíření do otevřené množiny obsahující $\mathrm{Re}(s) \geq 1$.)*

Důkaz. Holomorfnost v $\mathrm{Re}(s) > 1$ je zřejmá z definice. Potřebujeme nově vyjádřit $F(s)$. Pro $\mathrm{Re}(s) > 1$ dostaneme derivováním logaritmu Eulerovy identity v 5.1

$$-\frac{\zeta(s)'}{\zeta(s)} = \sum_p \frac{\log p}{p^s - 1} = F(s) + \sum_p \frac{\log p}{p^s(p^s-1)} \ .$$

Tedy

$$F(s) - \frac{1}{s-1} = -\left(\frac{\zeta(s)'}{\zeta(s)} + \frac{1}{s-1}\right) + \sum_p \frac{\log p}{p^s(1-p^s)} \ .$$

Suma definuje funkci holomorfní v $\mathrm{Re}(s) > 1/2$. Podívejme se na chování výrazu v závorce v bodě s na přímce $\mathrm{Re}(s) = 1$. Pokud $s = 1$, funkce $\zeta(s) - (s-1)^{-1}$ je holomorfní v okolí 1 (tvrzení 161) a odtud je lehké odvodit, že i $\zeta(s)'\zeta(s)^{-1} + (s-1)^{-1}$ je holomorfní v okolí 1. Pokud $\mathrm{Re}(s) = 1$, ale $s \neq 1$, jsou $\zeta(s)'$, $\zeta(s)$ i $1/(s-1)$ holomorfní v okolí s (tvrzení 161) a navíc podle předchozího tvrzení je $\zeta(s)$ ve vhodném okolí s nenulová. Funkce $\zeta(s)'\zeta(s)^{-1} + (s-1)^{-1}$ je opět holomorfní v okolí s. $F(s)-(s-1)^{-1}$ tedy můžeme holomorfně rozšířit do okolí každého bodu přímky $\mathrm{Re}(s) = 1$. ♢

Lemma 164. *Nechť $F(s)$ je jako výše a $\vartheta(x) = \sum_{p \leq x} \log p$ je Čebyševova funkce. Pro $\mathrm{Re}(s) > 1$ platí*

$$F(s) = s \int_0^\infty \vartheta(\mathrm{e}^t)\mathrm{e}^{-st}\, dt \ .$$

Důkaz.

$$\begin{aligned} s \int_0^\infty \vartheta(\mathrm{e}^t)\mathrm{e}^{-st}\, dt &= s \int_1^\infty \vartheta(x) x^{-s-1}\, dx = \sum_{n=1}^\infty \vartheta(n) \cdot s \int_n^{n+1} x^{-s-1}\, dx \\ &= \sum_{n=1}^\infty \vartheta(n)(n^{-s} - (n+1)^{-s}) = \sum_{n=1}^\infty n^{-s}(\vartheta(n) - \vartheta(n-1)) \\ &= \sum_p \frac{\log p}{p^s} \ . \end{aligned}$$

♢

Klíčovým nástrojem důkazu je výsledek z komplexní analýzy, který zdánlivě nemá cokoli společného s prvočísly. Nechť $f : [0, \infty) \to \mathbf{R}$ je omezená funkce, která je integrovatelná na každém (konečném) intervalu $[a, b]$. Výsledky o integrálních reprezentacích založené na Morerově větě (komplexní funkce spojitá v oblasti D a mající v ní nulový integrál přes hranici každého obdélníku, je v D holomorfní) nám říkají, že funkce

$$g(z) = \int_0^\infty f(t)\mathrm{e}^{-zt}\, dt$$

je holomorfní v $\mathrm{Re}(z) > 0$.

Věta 165 (Wiener a Ikehara, 1932). *Funkce $f(t)$ a $g(z)$ buďte jako výše, zejména je $f(t)$ omezená. Nechť se navíc $g(z)$ dá holomorfně rozšířit na* $\mathrm{Re}(z) \geq 0$ *(to jest do okolí každého bodu na imaginární ose). Pak integrál*

$$\int_0^\infty f(t)\, dt$$

konverguje a rovná se $g(0)$.

DŮKAZ. (**Newman, 1980.**) Pro reálné $T > 0$ položíme

$$g_T(z) = \int_0^T f(t)\mathrm{e}^{-zt}\, dt \ .$$

To je funkce holomorfní v celém $\mathbf{C}$. Máme dokázat, že $\lim_{T\to\infty} g_T(0) = g(0)$. Nechť $R > 0$ je reálné a C je oblast

$$C = C(R) = \{z \in \mathbf{C} :\ |z| < R\ \&\ \mathrm{Re}(z) > -\delta\}\ ,$$

přičemž $\delta = \delta(R) > 0$ je tak malé, že $g(z)$ je v C holomorfní. Hranici ∂C (uzavřená křivka připomínající písmeno D) rozdělíme na křivky

$$\begin{aligned} \partial C^+ &= \{z \in \partial C :\ \mathrm{Re}(z) > 0\} \ \text{ a} \\ \partial C^- &= \{z \in \partial C :\ \mathrm{Re}(z) < 0\}\ . \end{aligned}$$

Budeme též potřebovat půlkružnici

$$K = \{z \in \mathbf{C} :\ |z| = R\ \&\ \mathrm{Re}(z) < 0\}\ .$$

Křivky ∂C^- a K mají shodné koncové body. Definujeme funkci $G(z) : \mathbf{C} \to \mathbf{C}$,

$$G(z) = G(z, R, T) = \left(1 + \frac{z^2}{R^2}\right)\mathrm{e}^{zT}\ ,$$

kde $R, T > 0$ jsou reálné parametry mající shora uvedený smysl. $G(z)$ je holomorfní v celém $\mathbf{C}$. Podle Cauchyho věty (hranice ∂C je orientovaná proti směru hodinových ručiček a $G(0) = 1$)

$$g(0) - g_T(0) = \frac{1}{2\pi i} \int_{\partial C} \frac{g(z) - g_T(z)}{z} G(z)\, dz\ .$$

Poslední integrál I je součtem $I_1 + I_2 + I_3$, kde

$$\begin{aligned} I_1 &= \int_{\partial C^-} \frac{g(z)}{z} G(z)\, dz\ , \\ I_2 &= -\int_K \frac{g_T(z)}{z} G(z)\, dz \ \text{ a} \\ I_3 &= \int_{\partial C^+} \frac{g(z) - g_T(z)}{z} G(z)\, dz\ . \end{aligned}$$

V I_2 jsme křivku ∂C^- mohli zdeformovat v K beze změny integrálu, protože integrand je holomorfní v $\mathrm{Re}(z) < 0$. Postupně odhadneme $|I_1|, |I_2|$ a $|I_3|$.

Integrand v I_1 je součinem e^{zT} a funkce nezávislé na T. Nechť $M_1 = M_1(R)$ je maximální modul této funkce na křivce ∂C^-. Pak

$$|I_1| \le M_1 \int_{\partial C^-} |\mathrm{e}^{zT}|\, dz\ .$$

Pro každé $\varepsilon > 0$ existuje $\kappa > 0$ tak, že platí $|\mathrm{e}^{zT}| \le \mathrm{e}^{-\kappa T}$ na celé ∂C^- vyjma části, jejíž délka je méně než ε-zlomek celkové délky ∂C^-. Na tomto zbytku použijeme triviální odhad $|\mathrm{e}^{zT}| \le 1$. Vidíme, že pro každé pevné $R > 0$

$$\lim_{T \to \infty} |I_1| = 0\ .$$

Pro odhad $|I_2|$ použijeme konstantu $B = \sup_{t \ge 0} |f(t)|$. Pro $\mathrm{Re}(z) < 0$ máme

$$|g_T(z)| = \left| \int_0^T f(t) \mathrm{e}^{-tz}\, dt \right| \le B \int_{-\infty}^T |\mathrm{e}^{-tz}|\, dt = \frac{B\mathrm{e}^{-\mathrm{Re}(z)T}}{|\mathrm{Re}(z)|}\ .$$

Ale na kružnici $|z| = R$ platí rovnost

$$\left| \frac{G(z)}{z} \right| = \left| \frac{\mathrm{e}^{zT}(z + \overline{z})}{R^2} \right| = 2\mathrm{e}^{\mathrm{Re}(z)T} \cdot \frac{|\mathrm{Re}(z)|}{R^2}\ .$$

Takže

$$|I_2| \leq \frac{2\pi B}{R} \ .$$

Na ∂C^+ podobně odhadneme

$$|g(z) - g_T(z)| \leq B \int_T^\infty |\mathrm{e}^{-tz}| \, dt = \frac{B\mathrm{e}^{-\mathrm{Re}(z)T}}{\mathrm{Re}(z)} \ .$$

Opět, díky identitě pro $|G(z)z^{-1}|$ na $|z| = R$,

$$|I_3| \leq \frac{2\pi B}{R} \ .$$

Z $|I| \leq |I_1| + |I_2| + |I_3|$ a hořejších odhadů dostáváme pro každé $R > 0$

$$|g(0) - g_T(0)| = \frac{|I|}{2\pi} \leq \frac{|I_1|}{2\pi} + \frac{2B}{R} \ .$$

Pro dané $\varepsilon > 0$ zvolíme R tak velké, že druhý sčítanec je menší než $\varepsilon/2$. Pak pro každé dostatečně velké T je i první sčítanec menší než $\varepsilon/2$ a dohromady $|g(0) - g_T(0)| < \varepsilon$. Věta je dokázána. ♢

Lemma 166. *Nechť ϑ je Čebyševova funkce. Integrál*

$$\int_1^\infty \frac{\vartheta(x) - x}{x^2} \, dx$$

konverguje.

Důkaz. Podle lemmatu 164 v $\mathrm{Re}(z) > 0$ platí

$$\int_0^\infty \left(\frac{\vartheta(\mathrm{e}^t)}{\mathrm{e}^t} - 1 \right) \mathrm{e}^{-tz} \, dt = \frac{F(z+1)}{z+1} - \frac{1}{z} \ .$$

Na funkce $f(t) = \vartheta(\mathrm{e}^t)\mathrm{e}^{-t} - 1$ a $g(z) = F(z+1)(z+1)^{-1} - z^{-1}$ tedy můžeme aplikovat předchozí větu, pokud ovšem ověříme její předpoklady. Veličina $|f(t)|$ je omezená podle lemmatu 138. Funkce $g(z)$ má požadované holomorfní rozšíření podle lemmatu 163. Tedy $\int_0^\infty f(t) \, dt$ konverguje. Zbytek plyne substitucí $x = \mathrm{e}^t$. ♢

Důkaz věty 157. **(Newman, 1980.)** Dokážeme, že pro $x \to \infty$ platí $\vartheta(x) \sim x$. Předpokládejme pro spor, že existuje $\lambda > 1$ tak, že pro každé $y > 0$ existuje x větší než y tak, že $\vartheta(x) \geq \lambda x$. Protože ϑ je neklesající,

$$\int_x^{\lambda x} \frac{\vartheta(t) - t}{t^2}\, dt \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2}\, dt = \int_1^{\lambda} \frac{\lambda - u}{u^2}\, du = c > 0 \; .$$

To je spor s předešlým lemmatem. Podobně, kdyby existovalo $0 < \lambda < 1$ tak, že pro každé $y > 0$ existuje x větší než y tak, že $\vartheta(x) \leq \lambda x$, pak

$$\int_{\lambda x}^{x} \frac{\vartheta(t) - t}{t^2}\, dt \leq \int_{\lambda x}^{x} \frac{\lambda x - t}{t^2}\, dt = \int_{\lambda}^{1} \frac{\lambda - u}{u^2}\, du = d < 0 \; .$$

Opět spor s předešlým lemmatem. Díky tvrzení 158 je Prvočíselná věta dokázána.

5.7.2 Daboussiho elementární důkaz

Prvočíselnou větu dokážeme ve formulaci tvrzení 160. Nechť $M(t) = \sum_{n \leq t} \mu(n)$ a

$$\alpha = \limsup_{x \to \infty} \left| \frac{M(x)}{x} \right| \; .$$

Patrně $0 \leq \alpha \leq 1$. Pomocí tří odhadů v tvrzeních 167, 169 a 170 ukážeme, že $\alpha = 0$.

Nechť $y \in \mathbf{R}$ je kladné číslo. Pomocí $v_y : \mathbf{N} \to \{0, 1\}$ označíme charakteristickou funkci množiny čísel, jejichž prvočinitelé nepřesahují y (klademe $v_y(1) = 1$). Nechť

$$V_y(x) = \sum_{n \leq x} v_y(n)\mu(n) \quad \text{a} \quad V_y^*(x) = \sum_{n \leq x} v_y(n) \; .$$

Tvrzení 167 (první odhad). *Pro každé $y \geq 1$ platí nerovnost*

$$\alpha \leq \prod_{p \leq y} \left(1 - \frac{1}{p}\right) \cdot \int_1^{\infty} \frac{|V_y(t)|\, dt}{t^2} \; .$$

Důkaz. Nechť $u_y : \mathbf{N} \to \{0, 1\}$ je charakteristická funkce množiny čísel, jejichž každý prvočinitel je větší než y (i zde klademe $u_y(1) = 1$). Je jasné, že

$$\mu(n) = \sum_{d \backslash n} u_y(d)\mu(d) \cdot v_y(n/d)\mu(n/d) \; .$$

Sumací pro $n \le x$ dostaneme

$$M(x) = \sum_{n \le x} u_y(n)\mu(n)V_y(x/n) \ .$$

Nechť $1 = d_1 < d_2 < \cdots < d_q$ jsou všechna čtvercuprostá čísla d, pro něž $v_y(d) = 1$. Pro $n \in (x/d_{j+1}, x/d_j]$ platí $V_y(x/n) = V_y(d_j)$. Tedy

$$M(x) = \sum_{j=1}^{q-1} V_y(d_j) \sum_{x/d_{j+1} < n \le x/d_j} u_y(n)\mu(n) + V_y(d_q) \sum_{n \le x/d_q} u_y(n)\mu(n)$$

a

$$\alpha \le \sum_{j=1}^{q-1} |V_y(d_j)| \lim_{x\to\infty} \frac{1}{x} \sum_{x/d_{j+1} < n \le x/d_j} u_y(n) + |V_y(d_q)| \lim_{x\to\infty} \frac{1}{x} \sum_{n \le x/d_q} u_y(n) \ .$$

Podle principu inkluze a exkluze

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n \le x} u_y(n) = \prod_{p \le y} \left(1 - \frac{1}{p}\right) \ .$$

Tedy

$$\alpha \le \prod_{p \le y} \left(1 - \frac{1}{p}\right) \cdot \sum_{j=1}^{q} |V_y(d_j)| \cdot (d_j^{-1} - d_{j+1}^{-1}) \ ,$$

kde $d_{q+1} = \infty$. První odhad je dokázán, protože $V_y(t) = V_y(d_j)$ na intervalu $[d_j, d_{j+1})$ a integrál funkce t^{-2} přes něj je $d_j^{-1} - d_{j+1}^{-1}$. $\diamondsuit$

Lemma 168. *Nechť $a \ge 1$ a $M(t)$ v intervalu $[a,b]$ nemění znaménko. Potom*

$$\int_a^b \frac{|M(t)|\,dt}{t^2} \le 6 \ .$$

Důkaz. Stačí dokázat, že $|\int_1^x M(t)t^{-2}\ dt| \le 3$ pro každé $x \ge 1$. Podle Abelovy sumace $\int_1^x M(t)t^{-2}\,dt = -M(x)/x + \sum_{n\le x} \mu(n)/n$. Ale

$$\begin{aligned}
x \sum_{n \le x} \frac{\mu(n)}{n} &= \sum_{n \le x} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor + \sum_{n \le x} \mu(n) \left\{ \frac{x}{n} \right\} \\
&= \sum_{n \le x} \mu(n) \sum_{m \le x} \langle n \backslash m \rangle + A \quad (|A| \le x) \\
&= \sum_{m \le x} \sum_{n \backslash m} \mu(n) + A \\
&= 1 + A \ ,
\end{aligned}$$

podle tvrzení 6. Opravdu $|\int_1^x M(t)t^{-2}\,dt| \le (|M(x)|+1+|A|)/x \le 3$. $\diamondsuit$

Tvrzení 169 (druhý odhad). *Nechť α je jako výše a $\alpha > 0$. Pak existuje číslo $\delta \in (0,1)$ závisející jen na α a takové, že pro každé $\beta \in (\alpha, 2)$ a každé $y \ge 1$ platí nerovnost*

$$\int_1^y \frac{|V_y(t)|\,dt}{t^2} \le \delta\beta \log y + O_\beta(1)\ .$$

Důkaz. Pro $t \in [1,y]$ máme $V_y(t) = M(t)$. Nechť $\beta \in (\alpha, 2)$ je pevné. Existuje x_β tak, že $|M(t)| \le \beta t$ pro $t \ge x_\beta$. Pro interval $I = [a,b]$, $a \ge 1$, definujeme $l(I) = \log b - \log a$. Nechť (i) funkce $M(t)$ v I nemění znaménko a (ii) $M(a) = 0$ a $a \in \mathbf{N}$. Ukážeme, že pak

$$\int_I \frac{|M(t)|\,dt}{t^2} \le \frac{\beta \cdot l(I)}{2}\ , \quad \text{jakmile } l(I) \ge \frac{12}{\beta} \ \text{ nebo } l(I) \le \frac{\beta}{2+\beta}\ .$$

Pro dlouhé intervaly ($l(I) \ge 12/\beta$) to plyne hned z předchozího lemmatu a předpoklad (ii) nepotřebujeme. Nechť I je krátký interval ($l(I) \le \beta/(2+\beta)$). Graf $|M(t)|$ leží v I pod přímkou $t-a$ a integrál je proto nejvýše $(b-a)^2/(2a^2)$. (Nyní zjevně nepotřebujeme (i).) Nechť $c = b/a - 1$. Protože $l(I) = \log(1+c)$ a $\mathrm{e}^x \le 1 + 2x$ pro $x \in (0, 1/2)$, z předpokladu o $l(I)$ plyne $c \le \frac{\beta}{1+\beta/2}$. Tudíž

$$\frac{(b-a)^2}{2a^2} = \frac{c^2}{2} \le \frac{\beta}{2}\left(c - \frac{c^2}{2}\right) < \frac{\beta}{2}\log(1+c) = \frac{\beta \cdot l(I)}{2}\ .$$

Nechť $I = [a,b]$, kde $a \ge x_\beta$ a $a \in \mathbf{N}$, je interval střední velikosti ($\beta/(2+\beta) < l(I) < 12/\beta$), na němž $M(t)$ nemění znaménko a $M(a) = 0$. Z I oddělíme krátký počáteční interval J, $l(J) = \frac{\beta}{2+\beta}$, na němž integrál odhadneme hořejší nerovností. Na zbytku I použijeme triviální odhad $|M(t)| \le \beta t$. Dostaneme

$$\begin{aligned}
\int_I \frac{|M(t)|\,dt}{t^2} &\le \frac{\beta}{2}\cdot l(J) + \beta \cdot (l(I) - l(J)) = \left(1 - \frac{l(J)}{2l(I)}\right)\beta \cdot l(I) \\
&\le \left(1 - \frac{\beta^2}{48 + 24\beta}\right)\beta \cdot l(I) \\
&< \left(1 - \frac{\alpha^2}{96}\right)\beta \cdot l(I) = \delta\beta \cdot l(I)\ .
\end{aligned}$$

Protože $\alpha \leq 1$, platí tento odhad pro všechny intervaly, i pro krátké a dlouhé.

Nechť $z_\beta \in \mathbf{N}$, kde $z_\beta \geq x_\beta$, je první celočíselný nulový bod $M(t)$ za x_β. Uvážíme rozklad $\int_I |M(t)|t^{-2}\, dt = H_1 + H_2 + H_3$, kde $I = [1, y]$ a H_i jsou integrály přes intervaly $I_1 = [1, x_\beta]$, $I_2 = [x_\beta, z_\beta]$ a $I_3 = [z_\beta, y]$. Zřejmě $H_1 \leq \log x_\beta = O_\beta(1)$. I_3 rozdělíme na intervaly, které začínají celočíselnými nulovými body $M(t)$ a na nichž $M(t)$ nemění znaménko. Podle hořejšího odhadu $H_3 \leq \delta\beta \cdot l(I_3)$. Pokud $l(I_2) \geq 12/\beta$, $H_2 \leq \delta\beta \cdot l(I_2)$ podle nerovnosti pro dlouhé intervaly ($M(t)$ v I_2 nemění znaménko) a H_2 přičteme k H_3. Jinak $H_2 \leq \beta l(I_2) < 12$ a H_2 je pohlcen v $O_\beta(1)$. Celkem $\int_I |M(t)|t^{-2}\, dt \leq \delta\beta \cdot l(I) + O_\beta(1)$. $\diamondsuit$

V dalším $C = 1/c_2 \geq 1$ označuje reciprokou hodnotu konstanty z asymptotiky 3 věty 141. Platí $C = \mathrm{e}^\gamma = 1.78107\ldots$ (úloha 21), ale to nebudeme potřebovat.

Tvrzení 170 (třetí odhad). *Nechť α je jako výše a $\alpha > 0$. Pro každé $\beta \in (\alpha, 2)$ a každé $y \geq 1$ platí nerovnost*

$$\int_y^\infty \frac{|V_y(t)|\, dt}{t^2} \leq \beta(C-1)\log y + O_\beta(1)\ .$$

Důkaz třetího odhadu je nejtěžší a na okamžik ho odsuneme. Teď už je hračkou odvodit, že $\alpha = 0$.

Důkaz věty 157. **(Daboussi, 1984.)** Nechť $\alpha > 0$. Z tvrzení 167, 169, 170 a 3 věty 141 limitním přechodem $y \to \infty$ dostáváme, že existuje $\delta \in (0, 1)$ tak, že pro každé $\beta \in (\alpha, 2)$ platí nerovnost $\alpha \leq \beta(1 - (1-\delta)C^{-1})$. To je spor, protože koeficient u β je menší než 1. Proto $\alpha = 0$ a díky tvrzení 160 je Prvočíselná věta dokázána. $\diamondsuit$

Musíme ale ještě dokázat třetí odhad. Budeme potřebovat pomocnou funkci $h(y, t)$ definovanou pomocí

$$\begin{aligned} h(y,t) &= \frac{k(\log t/\log y)}{\log y}\ , \quad \text{kde} \\ k(s) &= \int_0^\infty \mathrm{e}^{f(x)-sx}\, dx\ , \quad \text{přičemž}\ \ f(x) = \int_0^x (1-\mathrm{e}^{-u})u^{-1}\, du\ , \end{aligned}$$

a tři lemmata.

Lemma 171. *Pro každé $t \geq y > 1$ platí*

$$\log t \cdot h(y,t) - \int_t^{yt} \frac{h(y,v)\, dv}{v} = 1\ .$$

DŮKAZ. Záměnou pořadí integrace jednoduchým výpočtem, s využitím definice $f(x)$, dostaneme

$$\int_s^{s+1} k(u)\, du = \int_0^\infty \mathrm{e}^{f(x)}\mathrm{e}^{-sx} f'(x)\, dx = \int_0^\infty \left(\mathrm{e}^{f(x)}\right)' \mathrm{e}^{-sx}\, dx\ .$$

Integrací per partes posledního integrálu odvodíme vztah

$$sk(s) - \int_s^{s+1} k(u)\, du = 1\ .$$

Obměníme-li tuto formuli substitucemi $s = \log t/\log y$ a $u = \log v/\log y$, dostaneme přesně dokazovanou formuli. $\diamondsuit$

Lemma 172. *Funkce $f : [y,\infty) \to \mathbf{R}$ buď kladná, spojitě diferencovatelná a klesající. Potom*

$$\begin{aligned}
\sum_{p\le y} \frac{f(pt)\log p}{p} &= \int_t^{yt} \frac{f(v)\, dv}{v} + O(f(y)) \quad \textit{pro všechna } t \ge y > 1 \\
\sum_{y/t<p\le y} \frac{f(pt)\log p}{p} &= \int_y^{yt} \frac{f(v)\, dv}{v} + O(f(y)) \quad \textit{pro všechna } t \ge 1\ .
\end{aligned}$$

DŮKAZ. Označme $M_1(y) = \sum_{p\le y} \log p/p$. Podle Abelovy sumace (tvrzení 18) se suma na levé straně první formule rovná

$$f(yt)M_1(y) - \int_1^y M_1(u) \frac{df(ut)}{du}\, du\ .$$

Asymptotika 1 věty 141 říká, že $M_1(y) = \log y + O(1)$. Nahradíme-li v posledním výrazu funkci M_1 logaritmem, způsobíme chybu velkou jen $O(f(y))$ (f je kladná a klesající). Integrál pak transformujeme zpět integrací per partes. Levá strana se tedy rovná

$$f(yt)\log y - f(ut)\log u|_1^y + \int_1^y \frac{f(ut)\, du}{u} + O(f(y)) = \int_t^{yt} \frac{f(v)\, dv}{v} + O(f(y))\ .$$

Druhá formule se dokazuje podobně. $\diamondsuit$

Lemma 173. *Nechť C a $h(y,t)$ jsou jako výše. Pro $y\to\infty$ platí asymptotika*

$$\int_1^y \left(\int_y^{yt} \frac{h(y,v)\, dv}{v} \right) \frac{dt}{t} = (C-1)\log y + O(1)\ .$$

DŮKAZ. Dokážeme ji aritmeticky. Všechny O členy jsou vzhledem k $y \to \infty$. Nechť Λ je von Mangoldtova funkce, definovaná na začátku 5.3. Pro všechna $n \in \mathbf{N}$ platí

$$v_y(n)\log n = \sum_{d \backslash n} v_y(d)\Lambda(d) \cdot v_y(n/d)$$

(malá obměna identity $\log n = \sum_{d \backslash n} \Lambda(d)$ z důkazu lemmatu 136). Sumací pro $n \le t$ dostaneme

$$\sum_{n \le t} v_y(n)\log n = \sum_{n \le t} v_y(n)\Lambda(n)V_y^*(t/n) \ ,$$

což přepíšeme jako

$$V_y^*(t)\log t = \sum_{n \le t} v_y(n)\Lambda(n)V_y^*(t/n) + \sum_{n \le t} v_y(n)\log(t/n) \ .$$

Podle definice Λ máme

$$V_y^*(t)\log t = \sum_{p \le t,y} \log p \cdot V_y^*(t/p) + \sum_{p^r} \log p \cdot V_y^*(t/p^r) + \sum_{n \le t} v_y(n)\log(t/n) \ ,$$

kde v druhé sumě sčítáme přes ty p^r, že $p \le y$, $p^r \le t$ a $r \ge 2$.

Poslední vztah vynásobíme $h(y,t)/t^2$ a zintegrujeme přes $[y, \infty)$:

$$\begin{aligned} J &= \int_y^\infty \frac{V_y^*(t)h(y,t)\log t}{t^2}\, dt \\ &= \int_y^\infty \sum_{p \le y} \frac{V_y^*(t/p)h(y,t)\log p}{t^2}\, dt + E_1 + E_2 \\ &= I + E_1 + E_2 \ , \end{aligned}$$

kde

$$\begin{aligned} E_1 &= \int_y^\infty \sum_{p^r} \frac{V_y^*(t/p^r)h(y,t)\log p}{t^2}\, dt \quad \text{a} \\ E_2 &= \int_y^\infty \sum_{n \le t} \frac{v_y(n)h(y,t)\log(t/n)}{t^2}\, dt \ , \end{aligned}$$

přičemž v E_1 sčítáme přes výše popsané mocniny prvočísel. Funkce $h(y,t)$ je klesající v t. Odtud, se substitucemi $u = t/p^r$ a $u = t/n$,

$$\begin{aligned} E_1 &\le h(y,y) \sum_{n,r \ge 2} \frac{\log n}{n^r} \cdot \int_1^\infty \frac{V_y^*(u)\, du}{u^2} \quad \text{a} \\ E_2 &\le h(y,y) \sum_n \frac{v_y(n)}{n} \cdot \int_1^\infty \frac{(\log u)\, du}{u^2} \ . \end{aligned}$$

Podle definice $h(y,y)=O(\log^{-1} y)$. Dále

$$\int_1^\infty \frac{V_y^*(u)\,du}{u^2} = \sum_n \frac{v_y(n)}{n} = \prod_{p\le y} \frac{1}{1-p^{-1}} = C\log y + O(1)\ .$$

První rovnost se dostane Abelovou sumací (zřejmě $V_y^*(u) \le (1+\log_2 u)^y$, takže $V_y^*(u)/u \to 0$ pro $u\to\infty$). Druhá je konečná forma Eulerovy identity z 5.1. Třetí plyne z 3 věty 141. Zbylé dva faktory, součet v odhadu E_1 a integrál v odhadu E_2, zjevně konvergují. Dohromady, pro $y\to\infty$,

$$E_1 = O(1) \ \text{ i } \ E_2 = O(1)\ .$$

Upravíme hořejší integrál $I = \int_y^\infty \sum_{p\le y} \ldots dt$. Přepíšeme ho jako $I = \sum_{p\le y}\int_y^\infty \ldots dt$ a v každém sčítanci provedeme substituci $t/p=u$. Sčítanec $\int_{y/p}^\infty \ldots du$ rozdělíme na $\int_{y/p}^y \ldots du + \int_y^\infty \ldots du$. Protože druhý integrační obor nezávisí na p, můžeme pro něj prohodit zpět integrál a sumu. Dostaneme

$$\begin{aligned} I &= \sum_{p\le y}\int_{y/p}^y \frac{V_y^*(u)h(y,pu)\log p}{pu^2}\,du + \int_y^\infty \frac{V_y^*(u)}{u^2}\sum_{p\le y}\frac{h(y,pu)\log p}{p}\,du \\ &= I_1 + I_2\ . \end{aligned}$$

$\sum$ a $\int$ chceme vyměnit i v I_1. Nechť $2=p_1<p_2<\cdots<p_q\le y$ jsou prvočísla nepřesahující y a $p_0=1$. Pak

$$\begin{aligned} I_1 &= \sum_{i=0}^{q-1}\int_{y/p_{i+1}}^{y/p_i} \frac{V_y^*(u)}{u^2}\sum_{p_i<p\le y}\frac{h(y,pu)\log p}{p}\,du \\ &= \int_{y/p_q}^{y} \frac{V_y^*(u)}{u^2}\sum_{y/u<p\le y}\frac{h(y,pu)\log p}{p}\,du \\ &= \int_1^y \frac{V_y^*(u)}{u^2}\sum_{y/u<p\le y}\frac{h(y,pu)\log p}{p}\,du\ . \end{aligned}$$

Rovnost mezi integrály $J = I + E_1 + E_2$ za pomoci odhadů E_1 a E_2 a rozkladu $I = I_1 + I_2$ přepíšeme jako $J - I_2 = I_1 + O(1)$. Vnitřní sumy v I_1 a I_2 přitom nahradíme integrály podle lemmatu 172. Tím způsobíme chybu $O(h(y,y)) = O(\log^{-1} y)$, která vede k celkové chybě řádu $O(1)$. Dostaneme identitu

$$\begin{aligned} &\int_y^\infty \frac{V_y^*(t)}{t^2}\left(\log t\cdot h(y,t) - \int_t^{yt}\frac{h(y,v)\,dv}{v}\right)dt \\ &= \int_1^y \frac{V_y^*(t)}{t^2}\left(\int_y^{yt}\frac{h(y,v)\,dv}{v}\right)dt + O(1)\ , \end{aligned}$$

která se díky lemmatu 171 a rovnosti $V_y^*(t) = \lfloor t \rfloor = t + O(1)$, jež platí pro $t \le y$, zjednodušuje na

$$\int_y^\infty \frac{V_y^*(t)\,dt}{t^2} = \int_1^y \left(\int_y^{yt} \frac{h(y,v)\,dv}{v} \right) \frac{dt}{t} + O(1)\ .$$

Podle hořejšího argumentu a tvrzení 15 se integrál vlevo rovná

$$\begin{aligned} &\sum_n \frac{v_y(n)}{n} - \sum_{n \le y} \frac{v_y(n)}{n} + O(1) \\ &= \prod_{p \le y} \frac{1}{1-p^{-1}} - \sum_{n \le y} \frac{1}{n} + O(1) = (C-1)\log y + O(1)\ . \end{aligned}$$

Tím je asymptotika dokázána. $\diamondsuit$

Důkaz tvrzení 170. Argument je téměř identický předchozímu důkazu, pouze místo rovnosti se dokazuje nerovnost $\le$ a veličina $V_y^*(t)$ je nahražena $V_y(t)$. Proto postupujeme rychleji. Vyjdeme z identity

$$-v_y(n)\mu(n)\log n = \sum_{d \backslash n} v_y(d)\Lambda(d) \cdot v_y(n/d)\mu(n/d)\ .$$

(Mírná obměna identity z důkazu tvrzení 160). Sumací pro $n \le t$ a malou úpravou dostaneme

$$|V_y(t)| \log t \le \sum_{n \le t} v_y(n)\Lambda(n)|V_y(t/n)| + \sum_{n \le t} v_y(n)\log(t/n)\ .$$

První sumu jdoucí fakticky přes mocniny p^r rozdělíme opět na sumu pro $r = 1$ a sumu pro $r \ge 2$. Vše vynásobíme $h(y,t)t^{-2}$ a zintegrujeme podle t přes interval $[y, \infty)$. Druhý a třetí integrál vpravo od $\le$ se stejným způsobem odhadnou a jsou $O(1)$. První integrál se stejně rozloží na součet dvou integrálů I_1 a I_2 přes $[1, y]$ a $[y, \infty)$. Přesunem I_2 vlevo od $\le$ dostáváme nerovnost

$$\begin{aligned} &\int_y^\infty \frac{|V_y(t)|}{t^2} \left(\log t \cdot h(y,t) - \int_t^{yt} \frac{h(y,v)\,dv}{v} \right) dt \\ &\le \int_1^y \frac{|V_y(t)|}{t^2} \left(\int_y^{yt} \frac{h(y,v)\,dv}{v} \right) dt + O(1)\ . \end{aligned}$$

Výraz v závorce vlevo od $\le$ je 1 (lemma 171). $V_y(t) = M(t)$ pro $t \le y$ a pro $t \ge x_\beta$ máme $|M(t)| \le \beta t$. Integrál vpravo je proto podle předchozího lemmatu nejvýše $\beta(C-1)\log y + O_\beta(1)$. Třetí odhad je dokázán.

5.8 Poznámky

5.1 Je nekonečně mnoho prvočísel. Literatura: Ribenboim [62] a Hardy a Wright [30]. Pro důkaz číslo 2 je často odkazováno do klasické cvičebnice Pólyi a Szegöho [58] (díl 2, část 8, kapitola 2, §2, úloha 94), ale podle Ribenboima ho uvádí už Goldbach v jednom dopisu Eulerovi. Ribenboimova kniha [62] obsahuje i další důkazy a mnoho informací o prvočíslech.

Je pozoruhodná souvislost mezi Fermatovými prvočísly, což jsou prvočíselná $F_n = 2^{2^n} + 1$, a jednou třídou klasických Euklidovských geometrických konstrukcí. Platí totiž, že pravidelný n-úhelník lze sestrojit za pomoci pravítka a kružítka, právě když

$$n = 2^k p_1 p_2 \dots p_r \ ,$$

kde $k \in \mathbf{N}_0$ a p_i jsou různá Fermatova prvočísla. Pro $n = 17$ konstrukci nalezl Gauss v r. 1796, pro obecné n ji popsal v *Disquisitiones Arithmeticae* v r. 1801. Opačnou implikaci (není-li n uvedeného tvaru, pravidelný n-úhelník není konstruovatelný) dokázal v r. 1837 Wantzel. Podrobnou informaci podává Stillwell [71]. Jediná známá Fermatova prvočísla jsou $3, 5, 17, 257$ a 65537. Zda existuje ještě nějaké další je palčivý otevřený problém elementární teorie čísel. Bylo dokázáno, že pro $n = 5, 6, \dots, 30$ a řadu dalších n je F_n složené. První Fermatovo číslo, jehož status není znám, je F_{31}. Viz [12] a [13].

Jak ukazuje úloha 4, Euklidův důkaz se dá poněkud zesílit. Největší potenciál však v sobě skrývá důkaz Eulerův. Sám Euler jeho modifikací uměl dokázat, že prvočísel tvaru $4n+1$ i $4n+3$ je nekonečně mnoho, viz úlohy 5 a 6. Dalekosáhlým rozvinutím jeho myšlenky Dirichlet v r. 1837 dokázal slavné zobecnění, podle něhož pro každé přirozené m každá třída zbytků modulo m nesoudělná s m obsahuje nekonečně mnoho prvočísel. Důkaz Dirichletovy věty jsme rozložili do úloh 7 až 14 (podle Serreho knihy [67]).

5.2 Dokonalá čísla a Mersennova prvočísla. Literatura: Hardy a Wright [30] a Lehmer [43]. Marin Mersenne (1588–1648) byl od r. 1611 členem řádu minoritů (minimů). Korespondencí s řadou vědců a filozofů (Fermat, Pascal, Descartes, Galileo, Huygens a mnoho dalších) zprostředkovával výměnu poznatků a idejí. Ve spisu *Cogitata Physica-Mathematica* (1644) v předmluvě vyslovil domněnku, že v oboru $q \leq 257$ je $M_q = 2^q - 1$ prvočíslo pouze pro $q = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ a 257. Jak dnes víme, tento seznam má být správně $q = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$ a 127.

Dosud bylo objeveno 38 Mersennových prvočísel. (Údaje čerpáme z internetové stránky prvočísel [2] vytvořené Ch. Caldwellem.) V předpočítačové éře bylo zjištěno, že M_q je prvočíslo pro q rovné $2, 3, 5, 7$,

> 13 (anonym 1456), 17 a 19 (Cataldi 1588), 31 (Euler 1772), 61 (Pěrvušin 1883), 89 (Powers 1911), 107 (Powers 1914) a 127 (Lucas 1876).

Jako první pro hledání Mersennových prvočísel použil počítač R. Robinson (manžel J. Robinsonové). Lucasovým–Lehmerovým testem byla dokázána prvočíselnost M_q pro q rovné

> 521, 607, 1279, 2203 a 2281 (Robinson 1952), 3217 (Riesel 1957), 4253 a 4423 (Hurwitz 1961), 9689, 9941 a 11213 (Gillies 1963), 19937 (Tuckerman 1971), 21701 (Noll a Nickel 1978), 23209 (Noll 1979), 44497 (Nelson a Slowinski 1979), 86243 (Slowinski 1982), 110503 (Colquit a Wels 1988), 132049 (Slowinski 1983), 216091 (Slowinski 1985), 756839 (Slowinski a Gage 1992), 859433 (Slowinski a Gage 1994) a 1257787 (Slowinski a Gage 1996).

Nový přelom znamenal nástup internetu. Internetový projekt GIMPS (Great Internet Mersenne Primes Search), započatý G. Woltmanem, rozděluje úlohy mezi mnoho tisíc účastníků po celém světě, jimž běží v době „nečinnosti“ počítače. Vše je založeno na starém dobrém Lucasově–Lehmerově testu. Velká čísla se násobí rychlou Fourierovou transformací. GIMPS zatím nalezl čtyři Mersennova prvočísla, pro q rovné

> 1398269 (Armengaud, Woltman, GIMPS 1996), 2976221 (Spence, Woltman, GIMPS 1997), 3021377 (Clarkson, Woltman, Kurowski, GIMPS 1998) a 6972593 (Hajratwala, Woltman, Kurowski, GIMPS 1999).

Číslo

$$2^{6972593} - 1 = 4370757441 \dots\dots\dots\dots 2924193791$$

má přes dva miliony dekadických cifer a je (v září 2000) největším známým prvočíslem. Zatím není zcela jisté, že je osmatřicátým Mersennovým prvočíslem podle velikosti, protože všechny exponenty mezi 3021377 a 6972593 nebyly dosud prověřeny. (Předchozí $M_{3021377}$ však sedmatřicáté podle velikosti je.)

Osmatřicet Mersennových prvočísel dává, podle věty 130, osmatřicet sudých dokonalých čísel. Existence lichého dokonalého čísla je otevřeným problémem, který číselné teoretiky učí pokoře. Pokud existuje, je větší než 10^{300} (Brent [9]) a má alespoň osm různých prvočinitelů (Hagis [26] a Chein [34]), z nichž některý musí přesahovat 10^6 (Hagis a Cohen [27]). Musí být dělitelné mocninou prvočísla přesahující 10^{20} (Cohen [11]) a počet jeho prvočinitelů s násobnostmi je alespň 29 (Sayers [66]). Heath-Brown [31] pro liché dokonalé N dokázal nerovnost

$$N < 4^{4^{\omega(N)}} .$$

Příbuzným pojmem jsou *spřátelená* (amicable) čísla. Jsou to taková dvě (různá) přirozená čísla m a n, že $\sigma(m) = \sigma(n) = m + n$. Jinak řečeno, součet vlastních dělitelů m se rovná n a naopak. Nejmenší spřátelená dvojice je 220 a 284 (viz úloha 17), známá již v antice. Až do Eulera byla známa jen sudá spřátelená čísla. Euler přišel s novými metodami a nalezl příklady lichých spřátelených dvojic, třeba

$$3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 = 69615 \ \text{ a } \ 3^2 \cdot 7 \cdot 13 \cdot 107 = 87633 .$$

Další informace o spřátelených číslech lze nalézt v knize [62] a článcích [7] a [8].

5.3 Čebyševovy a Mertensovy odhady. Literatura: Hlawka, Schoißengaier a Taschner [33]. Konstanta c_2 ve třetí Mertensově formuli má hodnotu $c_2 = \mathrm{e}^{-\gamma} = 0.56145\ldots$, kde $\gamma = 0.57721\ldots$ je Eulerova–Mascheroniova konstanta. Viz třeba [30] nebo [72]. Nebo to zkuste v úloze 21 dokázat sami.

Čebyšev kromě odhadu funkce $\pi(x)$ také dokázal, že pokud limita $\lim_{x\to\infty} \pi(x)/(x \log^{-1} x)$ existuje, rovná se jedné (úloha 20). Erdős a Kalmár v r. 1937 ukázali, že z platnosti Prvočíselné věty plyne, že každé její ε-zeslabení má elementární důkaz. Elementárně totiž dokázali, že pro každé $\varepsilon > 0$ platí implikace (μ je Möbiova funkce)

$$\begin{aligned} &\exists\, n \forall\, m \in \{n, n+1, \ldots, n^2\} \ \left| \frac{1}{m} \sum_{k=1}^{m} \mu(k) \right| < \varepsilon \\ &\Longrightarrow \frac{(1-\varepsilon)x}{\log x} < \pi(x) < \frac{(1+\varepsilon)x}{\log x} \ \text{ pro všechna } \ x > x(\varepsilon) . \end{aligned}$$

Jak víme (tvrzení 160), z Prvočíselné věty plyne odhad

$$\sum_{n \le x} \mu(n) = o(x) .$$

Pro každé ε tedy $n = n(\varepsilon)$ požadované v předpokladu implikace existuje. Máme-li již číslo $n(\varepsilon)$, v konečném počtu kroků snadno dokážeme, že splňuje předpoklad (množina čísel m, kterou musíme otestovat, je konečná a podmínka na m je snadno testovatelná). Výsledek Erdőse a Kalmára tak pro každé $\varepsilon > 0$ dává elementární důkaz odhadu $|\pi(x)/(x \log^{-1} x) - 1| < \varepsilon$, $x > x(\varepsilon)$. Tento důkaz je navíc uniformní v ε v tom smyslu, že existuje (zřejmý) algoritmus, který pro každé vstupní $\varepsilon > 0$ v konečném počtu kroků požadované $n(\varepsilon)$ nalezne (konečnost běhu algoritmu garantuje Prvočíselná věta). Vlastně tak máme algorimus, jehož vstupem je $\varepsilon > 0$ a výstupem elementární důkaz ε-zeslabení Prvočíselné věty. Viz Erdős [20] a Diamond a Erdős [16].

5.4 Vzorce pro prvočísla. Literatura: Ribenboim [62], Wright [77] a Papadimitriou [57]. Wright svůj vzorec zobecnil v [78]. Gandhiho formule pochází z [24]. Wrighta inspiroval Mills, který v [48] dokázal, že existuje číslo $\alpha \in \mathbf{R}$ takové, že

$$\left\lfloor \alpha^{3^n} \right\rfloor$$

je prvočíslo pro každé $n \in \mathbf{N}$. Čtenářka jistě tuší, že Millsova formule sdílí s Wrightovou stejný nedostatek: prvočísla, která „generuje“, byla předem zakódována do α. Pro výzkum vlastností prvočísel je tak naprosto bezcenná. Viz též Dudley [17].

Jones, Sato, Wada a Wiens [38] sestrojili následující celočíselný polynom Q o 26 neznámých, jehož kladné hodnoty na $\mathbf{N}_0$ jsou právě všechna prvočísla (neznámé jsou označeny všemi písmeny abecedy):

$$\begin{aligned} Q(a, b, \ldots, z) \quad = \quad & (k+2)\{1 - [wz + h + j - q]^2 \\ & -[(gk + 2g + k + 1)(h + j) + h - z]^2 \\ & -[2n + p + q + z - e]^2 \\ & -[16(k+1)^3(k+2)(n+1)^2 + 1 - f^2]^2 \\ & -[e^3(e+2)(a+1)^2 + 1 - o^2]^2 \\ & -[(a^2 - 1)y^2 + 1 - x^2]^2 \\ & -[16r^2y^4(a^2 - 1) + 1 - u^2]^2 \\ & -[n + l + v - y]^2 \\ & -[((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 \\ & -[(a^2 - 1)l^2 + 1 - m^2]^2 \\ & -[q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 \end{aligned}$$

$$
\begin{aligned}
&-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\\
&-[ai+k+1-l-i]^2\\
&-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2\}\ .
\end{aligned}
$$

Pro další informace odkazujeme do Matijaseviče [47]. Ani toto generování prvočísel nevedlo a nejspíš nepovede k obohacení našich znalostí o prvočíslech (viz [46]).

Pratt svou větu dokázal v [60]. O výpočetní složitosti pojednává třeba Papadimitriou [57] a mnoho další literatury. Zda třídy jazyků **P** a **NP** splývají je slavný otevřený „**P** versus **NP** problém“, jenž byl formulován na začátku sedmdesátých let 20. století. Vedle Riemannovy hypotézy, problému Navier–Stokesových rovnic proudění tekutin a dalších otázek je uznáván jako jedna z klíčových výzev pro matematiku a matematiky 21. století. (Problém **P** versus **NP** je například zahrnut mezi sedmi matematickými problémy, za jejichž vyřešení Clayův institut v Cambridge v Massachusets vypsal odměnu 10^6\$. Další informace na adrese [1].)

Příklad s polynomiálním certifikátem množiny S složených čísel není vůbec učebnicový, byl opravdu žit. Na zasedání Americké matematické společnosti v roce 1903 dramaticky vystoupil Frank Cole, který své kolegy beze slova, během několika minut,[1] prostým vynásobením přesvědčil, že

$$2^{67}-1=193707721\cdot 761838257287\ .$$

Číslo M_{67} je tedy složené a hořejší Mersennův seznam není opravdu dobře. Nalézt tuto faktorizaci však Coleho stálo „tři roky nedělí“.

Jsou známy velmi efektivní *pravděpodobnostní* algoritmy pro testování prvočíselnosti, které v polynomiální čase oznámí, zda vstup n je složené číslo nebo prvočíslo. Odpověď „složené“ je správná vždy, odpověď „prvočíslo“ může být s malou pravděpodobností nesprávná. Opakováním algoritmu se dá pravděpodobnost chyby libovolně snížit. Platí-li zobecněná Riemannova hypotéza, vyplývá z ní, že i deterministické (neomylné) verze těchto algoritmů pracují v polynomiálním počtu kroků. Pro další informace o algoritmické teorii čísel viz Adleman [3], Pomerance [59] a Knuth [41].

5.5 Typický počet prvočinitelů. Literatura: Hardy a Wright [30] a Alon, Spencer a Erdős [4]. Hardy a Ramanujan svou větu 148 dokazovali

[1] 27. září 2000 kolem čtvrté hodiny odpoledne jsem v pracovně na Malostranském náměstí ručním výpočtem Coleho rovnost ověřil. Ručně jsem samozřejmě spočetl i mocninu 2^{67}, totiž jako $8\cdot(65536^2)^2$. Výpočet mi trval necelé 54 minuty. Na obou stranách rovnosti stojí číslo 147573952589676412927.

v [29] dosti složitě. Turánův brilantní postup [74] byl motivován pravděpodobnostními úvahami (viz [4] pro ryze pravděpodobnostní verzi Turánova důkazu). V rukou Erdőse a dalších z nich rychle vypučela pestrobarevná zahrada pravděpodobnostní teorie čísel. Uvedeme jeden z jejích květů.

Pro každé pevné $\lambda \in \mathbf{R}$

$$\lim_{x\to\infty} \frac{1}{x} \cdot \left| \left\{ n \in \mathbf{N} : \ n \le x \ \& \ \omega(n) \ge \log\log x + \lambda\sqrt{\log\log x} \ \right\} \right| \\ = \frac{1}{\sqrt{2\pi}} \int_\lambda^\infty \mathrm{e}^{-t^2/2} \, dt \ .$$

Funkce $\omega(n)$ se tedy pro velké x na intervalu $[1, x]$ chová jako náhodná veličina, která má normální rozdělení se střední hodnotou a rozptylem $\log\log x$. Toto podstatné zesílení věty 148 dokázali v r. 1940 v [21] P. Erdős a M. Kac.

Pro další informace o průměrných a normálních řádech a o pravděpodobnostní teorii čísel doporučujeme Tenenbaumovu knihu [72].

A kolik že je různých součinů v tabulce velké násobilky? V r. 1960 P. Erdős ve svém „ruském článku“ [19] (Erdős se rád chlubil tím, že ikdyž neumí rusky, přesto napsal rusky článek) dokázal, že pro $x \to \infty$

$$|\{ab : \ a, b \in \mathbf{N} \ \& \ a, b \le x\}| = \frac{x^2}{(\log x)^{\alpha + o(1)}} \ ,$$

kde

$$\alpha = 1 - \frac{\log(\mathrm{e} \log 2)}{\log 2} = 0.08607\ldots \ .$$

5.6 Šnirelmanova věta. Literatura: Nathanson [50]. „Prvočísla jsou proto, aby se násobila. Tak proč je sčítat??“ řekl prý sovětský fyzik a nobelista Lev Landau na adresu aditivní teorie čísel (Arnold [5]).

V roce 1742 Goldbach v dopisu Eulerovi vyslovil domněnku, že každé sudé přirozené číslo větší než 2 je součtem dvou prvočísel. Euler odepsal, že domněnce věří, ale neumí ji dokázat. Dosud to neumí nikdo. Pomocí počítačů Sinisalo [68] ověřil, že domněnka platí pro všechna sudá n menší než $4 \cdot 10^{11}$. Šnirelmanova věta 150 je druhým významným výsledkem směrem k důkazu Goldbachovy hypotézy. Šnirelman ji publikoval nejprve v [69] a pak německy [70]. V důkazu nepoužil větu 156, která je pozdější, ale výsledky V. Bruna, o nichž se zmíníme za chvíli. *Šnirelmanova konstanta* je nejmenší přirozené h_0 takové, že každé $n \in \mathbf{N}$ větší než 1 je součtem nejvýše h_0 prvočísel. Šnirelman sám uměl dokázat, že $h_0 < 8 \cdot 10^5$. Ramaré [61] dokázal, že $h_0 \leq 7$. Platí-li Goldbachova hypotéza, $h_0 = 3$.

Goldbachova domněnka zjevně implikuje tzv. lichou Goldbachovu domněnku, podle níž každé liché přirozené n větší než 1 je součtem nejvýše tří prvočísel. Třetí základní výsledek ke Goldbachově hypotéze dosáhl I. M. Vinogradov v roce 1937 v [76]. Vinogradov pomocí analytické *kruhové metody* (která se zrodila v pracích Hardyho, Littlewooda a Ramanujana v letech 1918–20) dokázal, že tato slabší verze Goldbachovy hypotézy pro dostatečně velké liché n opravdu platí: existuje konstanta n_0, že každé liché $n > n_0$ je součtem nejvýše tří prvočísel. Z Vinogradovova důkazu byla získána konkrétní hodnota $n_0 = 3^{3^{15}}$. Později byla snížena na 10^{43000}. Saouter [65] ověřil lichou Goldbachovu domněnku numericky až do 10^{20}. Zinoviev [80] dokázal, že za předpokladu zobecněné Riemannovy hypotézy lze vzít $n_0 < 10^{20}$. Tím jsme s lichou Goldbachovou domněnkou dnes prakticky hotovi.

Historicky první průkopnické výsledky o Goldbachově hypotéze přinesl V. Brun, příslušník norské číselně-teoretické školy, jejichž několik vynikajících zástupců jsme už ve skriptech zmínili (Thue, Skolem, Selberg). Brun v r. 1920 v [10] dokázal, že pro každé dostatečně velké sudé n má rovnice $n = m_1 + m_2$ řešení, které splňuje $\Omega(m_1), \Omega(m_2) \leq 9$. Brunova metoda, dnes známá jako *Brunovo síto*, je elementární (avšak technicky dosti složité) zjemnění principu inkluze a exkluze. Vývoj nejrůznějších „sít“ pokračuje dodnes (ve větě 156 jsme se seznámili se *Selbergovým sítem*), viz Nathanson [50], Halberstam a Richert [28] a Motohashi [49]. Po řadě zlepšení Brunova výsledku různými autory nakonec metodami síta dokázal v r. 1966 svou pozoruhodnou větu J. R. Chen: Brunův výsledek platí i při velmi silném omezení sčítanců $\Omega(m_1) = 1$ a $\Omega(m_2) \leq 2$. (Chen svůj výsledek oznámil v [35], ale publikoval ho v úplnosti až v [36]. Překážkou byla čínská „kulturní revoluce“, jejíž dopady byly velmi nekulturní.) Jedním z posledních úspěchů sít je průlom Friedlandera a Iwaniecze [22] a [23], kteří dokázali, že existuje nekonečně mnoho prvočísel tvaru $x^2 + y^4$.

Metody síta se stejně dobře dají použít pro *problém dvojčat*, kdy se má dokázat, že existuje nekonečně mnoho prvočíselných dvojic n a $n + 2$. To nikdo dosud neumí. Brun dokázal, že nekonečně mnoho přirozených čísel n splňuje $\Omega(n), \Omega(n + 2) \leq 9$. Chenova metoda dává opět nekonečně mnoho dvojic n a $n+2$ takových, že jeden člen je prvočíslo a druhý součinem nejvýše dvou (ne nutně různých) prvočísel.

Důkaz Chenovy věty podává Ross [64] (bez důkazu některých základních tvrzení). Důkaz Vinogradovovy věty lze najít v Karacubovi [39]. Nathansonova kniha [50] obsahuje důkazy obou. O kruhové metodě si trochu povíme v příštích dvou kapitolách, základní monografie je Vaughan [75].

5.7 Prvočíselná věta. Literatura: Hlawka, Schoißengaier a Taschner [33], Newman [53] a Daboussi [14]. Důkaz v 5.7.1 náleží D. J. Newmanovi [52]. Newmanovo výrazné zjednodušení analytického důkazu Prvočíselné věty (dále PV) vzbudilo zaslouženou pozornost, viz třeba Korevaar [42], Zagier [79] nebo i Bak a Newman [6]. Důkaz v 5.7.2 podal H. Daboussi v [14]. Vraťme se však na začátek celé historie, asi o 200 let zpět.

Jako první publikoval domněnku o tvaru PV roku 1798 Legendre: $\pi(x) \sim x/(A\log x + B)$ pro nějaké konstanty A a B. O deset let později ji zpřesnil na $\pi(x) \sim x/(\log x + A(x))$, kde $A(x) \to 1.08366\ldots$ (dnes víme, že správná hodnota limity je 1). Již předtím však Gauss v letech 1792–93 vypracoval rozsáhlé tabulky prvočísel a porovnával hodnoty $\pi(x)$ s hodnotami integrállogaritmu

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t} \ .$$

Gauss předjímal moderní formulaci PV: $\pi(x) = \mathrm{li}(x) + \Delta(x)$, kde $\Delta(x)$ je malá chyba. O svých výzkumech nic nepublikoval, víme o nich jen z Gaussova dopisu astronomu Enckemu v r. 1849 (Goldstein [25]). Významným výsledkem, ikdyž v jiném směru, byla Dirichletova věta o prvočíslech v aritmetické posloupnosti z r. 1837. Dalším pokrokem byly Čebyševovy výsledky z let 1851–52.

V r. 1859 publikoval B. Riemann přelomový memoár [63], v němž odhalil úzkou souvislost mezi $\pi(x)$ a chováním zeta funkce $\zeta(s)$ v komplexním oboru. Nalezneme něm také slavnou *Riemannovu hypotézu*: pokud $\zeta(s) = 0$ pro $\mathrm{Re}(s) > 0$, platí $\mathrm{Im}(s) = 1/2$. Ta zůstává dodnes otevřená a patří k nejdůležitějším nerozhodnutým matematickým problémům. O Riemannově revolučním článku, vlastnostech $\zeta(s)$ a PV píše velmi precizně a zajímavě Edwards [18].

Po necelých 40 letech proměnili roku 1896, nezávisle na sobě, J. Hadamard (1865–1963) a Ch. de La Valée Poussin (1866–1962) Riemannovy ideje v rigorózní důkaz PV. Ukázalo se, že správná aproximace pro $\pi(x)$ je opravdu $\mathrm{li}(x)$. V prvním přiblížení platí $\mathrm{li}(x) \sim x\log^{-1} x$, ale pro přesnější aproximace $\pi(x)$ se $x\log^{-1} x$ nehodí, viz úloha 18. V r. 1899 de La Valée Poussin dokázal, že pro jistou konstantu $c > 0$

$$\pi(x) = \mathrm{li}(x) + O(x\mathrm{e}^{-c\sqrt{\log x}}) \ .$$

Roku 1901 dokázal von Koch, že Riemannova hypotéza je ekvivalentní asymptotice
$$\pi(x) = \mathrm{li}(x) + O_\varepsilon(x^{1/2+\varepsilon}) \ .$$

Současný rekord pro odhad chyby $\pi(x) - \mathrm{li}(x)$ v PV je
$$O(x\exp(-c(\log x)^{3/5}(\log\log x)^{-1/5})) \ ,$$
který dokázali v r. 1958 (nezávisle) N. M. Korobov a I. M. Vinogradov. Podrobněji se lze o historii PV dočíst v Edwardsovi [18] nebo Novákovi [55]. Další literatura o $\zeta(s)$ a PV: Tenenbaum [72], Ivič [37], Titchmarsh [73] a Karacuba a Voronin [40].

Mnozí si mysleli, že se PV elementárně, bez použití komplexní analýzy, dokázat nedá. Existoval též názor, že pokud by snad takový důkaz byl nalezen, přinesl by podstatný převrat ve znalostech o prvočíslech (viz poznámky k 9. kapitole [51]). Oba názory se ukázaly jako mylné. V r. 1948 A. Selberg a P. Erdős, nezávisle na sobě, ale ve vzájemné interakci (viz [51]), nalezli elementární důkaz PV. Selbergův důkaz a jeho varianty užívají různé verze tzv. *Selbergovy formule* popsané v úloze 22. Tyto elementární důkazy lze nalézt například v Novákovi [54], pozdějším vydání [30], v [51] nebo v Levinsonovi [44]. Daboussi se obdivuhodnou ekvilibristikou dokázal obejít bez Selbergovy formule. Hildebrand [32] dokázal PV elementárně metodami sít. Brunův krajan A. Selberg byl za své práce o prvočíslech vyznamenán r. 1950 Fieldsovou medailí.

Elementární důkazy PV se sice nedokázaly zcela vyrovnat, co do síly odhadu zbytku $\pi(x) - \mathrm{li}(x)$, analytickým, podstatně však překonaly počáteční skeptická očekávání (podrobná diskuse je v Novákovi [56]). Současný rekord odhadu zbytku v PV s elementárním důkazem je
$$O_\varepsilon(x\exp(-(\log x)^{1/6-\varepsilon}))$$
(A. F. Lavrik a A. Š. Sobirov 1973). Přehledový článek o elementárních metodách je Diamond [15].

Riemannova hypotéza zůstává i po 150 letech stále záhadná. Je dobře známo, že nulové body $\zeta(s)$ pro $\mathrm{Re}(s) \le 0$ jsou právě $-2, -4, -6, \ldots$ (triviální nuly $\zeta(s)$) a že všechny nulové body v $\mathrm{Re}(s) > 0$, kterých je nekonečně mnoho, leží uvnitř („kritického“) pásu $0 < \mathrm{Re}(s) < 1$ a jsou rozloženy symetricky vzhledem k přímkám $\mathrm{Re}(s) = 1/2$ a $\mathrm{Im}(s) = 0$. Tyto nulové body se uvažují v pořadí podle svých kladných imaginárních souřadnic. Van de Lune, te Riele a Winter [45] numericky dokázali, že prvních $1.5 \cdot 10^9$ z nich opravdu leží na přímce $\mathrm{Re}(s) = 1/2$. Další informace a odkazy poskytuje výše zmíněná literatura o $\zeta(s)$ a Bombieriho text o Riemannově hypotéze dostupný na adrese [1].

5.9 Úlohy

1. (**2**) Uvažme reprezentaci prvočísel kodifikovanými názvy čísel v češtině. Prvočíslu přiřadíme slovo nad abecedou

$$A = \{\sqcup,\ \text{a, á, b, c, č, d, e, ě, i, í, \ldots, y}\}\ ,$$

   které je jeho českým názvem. Symboly ď, é, f, g, h, ch, …, z, ž pro tento účel nepotřebujeme. Symbol $\sqcup$ označuje mezeru. Množinu P_r takto reprezentovatelných prvočísel pak lineárně uspořádáme standardním lexikografickým (slovníkovým) uspořádáním $<_l$, které je odvozeno z obvyklého abecedního pořadí symbolů v A (mezera předchází vše, písmeno s diakritikou jde po písmenu bez ní). Například

$$\text{devadesát} \sqcup \text{sedm} <_l \text{dva} \sqcup \text{tisíce} \sqcup \text{tři} <_l \text{dvacet} \sqcup \text{tři}\ ,$$

   protože e $<_l$ v a $\sqcup <_l$ c. Nalezněte nejmenší a největší prvek lineárního uspořádání $(P_r, <_l)$. (Ty existují, protože P_r je jistě konečná.)

2. (**1**) Dokažte, že pro každé $s \in \mathbf{R}$ větší než 1 platí Eulerova identita

$$\prod_p \frac{1}{1 - 1/p^s} = \sum_{n=1}^{\infty} \frac{1}{n^s}\ .$$

3. (a) (**2**) Kde je chyba v následujícím důkazu, uvedeném v jedné poměrně známé učebnici (nikoli teorie čísel)?

   Claim: The number of primes up to n is at least $\sqrt{n}$.

   Proof of the claim: If a number $i \leq n$ is not divisible by any prime smaller than $\sqrt{n}$, then i is a prime. Now, of the numbers that are less than or equal to n, at most one-half are divisible by two. Of the remaining ones, at most one-third are divisible by three. And so on for all primes up to $\sqrt{n}$. It follows that the number of primes up to n is at least $n \prod_{p \le \sqrt{n}} \frac{p-1}{p}$, with the product ranging over all primes up to $\sqrt{n}$, which is at least as large as $n \prod_{i=2}^{\lfloor \sqrt{n} \rfloor} \frac{i-1}{i} \ge \sqrt{n}$. □

(b) (**2**) Je nerovnost

$$\pi(n) \ge n \prod_{p \le \sqrt{n}} \frac{p-1}{p} \ ,$$

která byla v důkazu „odvozena“, pravdivá?

4. Modifikací Euklidova důkazu dokažte, že

   (a) (**1**) Prvočísel tvaru $4n+3$ je nekonečně mnoho.

   (b) (**2**) Prvočísel tvaru $4n+1$ je nekonečně mnoho.

5. Funkce $\chi_1, \chi_3 : \mathbf{Z} \to \{-1, 0, 1\}$ definujeme jako

$$\chi_1(n) = \begin{cases} 1 \ldots & n \equiv 1,3 \bmod 4 \\ 0 \ldots & \text{jinak} \end{cases} \quad \text{a} \quad \chi_3(n) = \begin{cases} -1 \ldots & n \equiv 3 \bmod 4 \\ 1 \ldots & n \equiv 1 \bmod 4 \\ 0 \ldots & \text{jinak} \ . \end{cases}$$

   Dále, pro $i = 1, 3$ a $s \in \mathbf{R}$, nechť

$$L(s, \chi_i) = \sum_{n=1}^{\infty} \frac{\chi_i(n)}{n^s} \ .$$

   (a) (**0**) Pro každé $s > 1$ řada $L(s, \chi_1)$ konverguje a $L(s, \chi_1) > 0$.

   (b) (**1**) Totéž platí pro $s > 0$ i pro $L(s, \chi_3)$.

   (c) (**1**) $L(s, \chi_1) \to \infty$ pro $s \to 1+$.

6. Modifikací Eulerova důkazu dokažte, že prvočísel tvaru $4n+1$ i tvaru $4n+3$ je nekonečně mnoho. Konkrétněji,

   (a) (**2**) Pro $s > 1$ mají obě $L(s, \chi_i)$ součinové vyjádření analogické Eulerově identitě v 5.1.

   (b) (**1**) Pro s jdoucí k číslu 1 zprava uvažte chování výrazů $L(s, \chi_1)/L(s, \chi_3)$ a $L(s, \chi_1)L(s, \chi_3)$.

7. Cílem úloh 7–14 je dokázat Dirichletovu větu, podle níž pro každou dvojici $a, m \in \mathbf{N}, a \perp m$, existuje nekonečně mnoho prvočísel p splňujících $p \equiv a \bmod m$. Budeme potřebovat několik vlastností charakterů.

   Připomínáme, že charakter Abelovy grupy $(G, \cdot)$ je homomorfismus χ z G do komplexní jednotkové kružnice. Nechť $\widehat{G}$ je množina všech charakterů grupy G.

   (a) (**1**) $\widehat{G}$ s operací násobení charakterů $(\chi \cdot \psi)(x) = \chi(x)\psi(x)$ tvoří Abelovu grupu, jejímž neutrálním prvkem je hlavní charakter (identická 1).

   (b) (**1**) Je-li G cyklická grupa řádu n, je i $\widehat{G}$ cyklická grupa řádu n.

   (c) (**2**) Je-li H podgrupa G, lze každý charakter $\chi \in \widehat{H}$ rozšířit na charakter grupy G.

   (d) (**1**) Je-li H podgrupa G, je podgrupa $\{\chi \in \widehat{G} : \forall x \in H\ \chi(x) = 1\}$ grupy $\widehat{G}$ izomorfní grupě $\widehat{G/H}$.

   (e) (**2**) Grupy G a $\widehat{G}$ mají týž počet prvků.

   (f) (**1**) Zobrazení $x \to (\chi \to \chi(x))$ je izomorfismus grup G a $\widehat{(\widehat{G})}$.

   (g) (**1**) Nechť $a \in G$ má řád f a $g = |G|/f$. Pak

$$\prod_{\chi \in \widehat{G}} (1 - \chi(a)x) = (1 - x^f)^g \ .$$

8. (**1**) Nechť $n = |G|$, $a \in G$ a $\psi \in \widehat{G}$. Pak

$$\sum_{x \in G} \psi(x) = \begin{cases} n \ldots & \psi \text{ je hlavní} \\ 0 \ldots & \text{jinak} \end{cases} \quad \text{a} \quad \sum_{\chi \in \widehat{G}} \chi(a) = \begin{cases} n \ldots & a = 1_G \\ 0 \ldots & a \neq 1_G \ . \end{cases}$$

9. (**2**) Nechť $0 < \alpha < \beta$ jsou dvě reálná čísla a $z \in \mathbf{C}$ je komplexní, přičemž $\mathrm{Re}(z) = x > 0$. Pak

$$|\mathrm{e}^{-\alpha z} - \mathrm{e}^{-\beta z}| \leq \left|\frac{z}{x}\right| \cdot (\mathrm{e}^{-\alpha x} - \mathrm{e}^{-\beta x}) \ .$$

10. Charakterem modulo $m \in \mathbf{N}$ rozumíme charakter χ multiplikativní grupy $G_m = (\mathbf{Z}/m\mathbf{Z})^*$ zbytků modulo m nesoudělných s m. χ chápeme jako zobrazení $\chi : \mathbf{Z} \to \mathbf{C}$, $\chi(a) = \chi(\bar{a})$ pro $a \perp m$ ($\bar{a}$ je redukce a

modulo m) a $\chi(a) = 0$ pro $(a, m) > 1$. Pro $s \in \mathbf{C}$ a χ charakter modulo m definujeme Dirichletovu L-funkci

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \; .$$

(a) (**1**) Je-li χ nehlavní, konverguje $L(s, \chi)$ pro každé $\mathrm{Re}(s) > 0$ a definuje funkci holomorfní v této polorovině.

(b) (**2**) Je-li χ hlavní, konverguje $L(s, \chi)$ pro každé $\mathrm{Re}(s) > 1$ a definuje funkci holomorfní v této polorovině. $L(s, \chi)$ se dá rozšířit na funkci $\frac{1}{s-1} + F(s)$, kde $F(s)$ je holomorfní v polorovině $\mathrm{Re}(s) > 0$.

11. Dirichletova řada

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

měj nezáporné reálné koeficienty a_n. Nechť t_0 je infimum (ve skutečnosti minimum) těch $t \in \mathbf{R}$, že $F(t)$ konverguje.

(a) (**1**) $F(s)$ definuje v $\mathrm{Re}(s) > t_0$ holomorfní funkci.

(b) (**3**) Tato funkce má v t_0 singularitu (nedá se holomorfně rozšířit do žádného okolí t_0).

12. Nechť $m \in \mathbf{N}$ a $s \in \mathbf{C}$.

(a) (**2**) V $\mathrm{Re}(s) > 1$ platí

$$\prod_{\chi} L(s, \chi) = \prod_{p \text{ nedělí } m} (1 - p^{-f(p)s})^{-g(p)} \; ,$$

kde χ probíhá $\varphi(m)$ charakterů modulo m, $f(p)$ je řád p v G_m (nejmenší $f \in \mathbf{N}$ takové, že $p^f \equiv 1 \bmod m$) a $g(p) = |G_m|/f(p) = \varphi(m)/f(p)$.

(b) (**3**) S pomocí funkce

$$\zeta_m(s) = \prod_{\chi} L(s, \chi)$$

dokažte, že pro každý nehlavní charakter χ modulo m máme $L(1, \chi) \neq 0$.

13. Nechť χ je charakter modulo m, $s \in \mathbf{R}$ je větší než 1 a

$$f_\chi(s) = \sum_p \frac{\chi(p)}{p^s} \ .$$

(a) (**2**) Je-li χ hlavní, pak $f_\chi(s) \to \infty$ pro $s \to 1^+$.

(b) (**2**) Je-li χ nehlavní, je $f_\chi(s)$ pro $s \to 1+$ omezená.

14. (**2**) Pro $a, m \in \mathbf{N}, a \perp m$, a $s \in \mathbf{C}$ s $\mathrm{Re}(s) > 1$ definujeme veličiny

$$p(a,m) = \{p:\ p \equiv a \bmod m\} \ \ \text{a} \ \ g_a(s) = \sum_{p \in p(a,m)} \frac{1}{p^s} \ .$$

Dokažte identitu

$$g_a(s) = \frac{1}{\varphi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s) \ .$$

Z ní a z předchozích výsledků odvoďte Dirichletovu větu: $p(a,m)$ je nekonečná.

15. (**2**) Dokažte, že pro každé a a m jako výše pro $s \to 1^+$ platí

$$g_a(s) \sim \frac{1}{\varphi(m)} \log \frac{1}{s-1} \ .$$

16. (**2**) Nechť $N = p_1^{a_1} \dots p_r^{a_r}$ je prvočíselný rozklad (hypotetického) lichého dokonalého čísla. Dokažte, že všechny exponenty a_i kromě jednoho jsou sudé a zbylý exponent, řekněme a_1, splňuje $p_1 \equiv a_1 \equiv 1 \bmod 4$.

17. (**1**) Ověřte, že čísla

$$2^n(3 \cdot 2^{n-1} - 1)(3 \cdot 2^n - 1) \ \ \text{a} \ \ 2^n(9 \cdot 2^{2n-1} - 1)$$

jsou spřátelená, pokud tři čísla v závorkách jsou prvočísla. Nalezněte tři hodnoty n, pro něž to nastává.

18. (**3**) Dokažte, že asymptotika

$$\pi(x) = \frac{x}{\log x} + O(x \log^{-3} x)$$

neplatí.

19. (**2**) Když p^k dělí $\binom{2m}{m}$, pak $p^k \le 2m$. Dokažte a odvoďte z toho, že $\pi(x) \gg x \log^{-1} x$.

20. (**2**) Dokažte implikaci

$$\lim_{x\to\infty} \frac{\pi(x)}{x \log^{-1} x} = c \ \text{ existuje } \Longrightarrow c = 1 \ .$$

21. (**3**) Dokažte, že

$$\lim_{x\to\infty} \log x \cdot \prod_{p\le x} \left(1 - \frac{1}{p}\right) = \mathrm{e}^{-\gamma} \ ,$$

kde $\gamma = \lim_{n\to\infty}(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n) = 0.57721\ldots$ je Eulerova–Mascheroniova konstanta.

22. (**4**) Dokažte elementárně asymptotiku

$$\sum_{p\le x} \log^2 p + \sum_{pq\le x} \log p \cdot \log q = 2x \log x + O(x) \ .$$

Literatura

[1] `www.claymath.org`

[2] `www.utm.edu/research/primes/`

[3] L. M. Adleman, Algorithmic number theory - The complexity contribution, 88–113. In: ??? (ed.), *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994),* IEEE Comput. Soc. Press, Los Alamitos, CA 1994.

[4] N. Alon, P. Erdős and J. Spencer, *The Probabilistic Method,* John Wiley & Sons, New York 1992.

[5] V. I. Arnold, Will mathematics survive? Report on the Zürich Congress, *Math. Intell.,* **17** (1995), 6–10.

[6] J. Bak and D. J. Newman, *Complex Analysis,* Springer, New York 1997.

[7] S. Battiato and W. Borho, Are there odd amicable numbers not divisible by three?, *Math. Comp.,* **50** (1988), 633–637.

[8] W. Borho and H. Hoffmann, Breeding amicable numbers in abundance, *Math. Comp.,* **46** (1986), 281–293.

[9] R. P. Brent, Improved techniques for odd perfect numbers, *Math. Comp.,* **57** (1991), 857–868.

[10] V. Brun, Le crible d'Eratosthène et le théorème de Goldbach, *Skrifter utgit av Videnskapsselskapet i Kristiania, I. Matematisk-Naturvidenskabelig Klasse,* **1** (1920), 1–36.

[11] G. L. Cohen, On the largest component of an odd perfect number, *J. Aust. Math. Soc., Ser. A,* **42** (1987), 280–286.

[12] R. Crandall, J. Doenias, C. Norrie and J. Young, The twenty-second Fermat number is composite, *Math. Comp.,* **64** (1995), 863–868.

[13] R. Crandall, E. Mayer and J. Papadopoulos, The twenty-fourth Fermat number is composite, *Math. Comp.,* **??** (200?), ???–???.

[14] H. Daboussi, Sur le théorème des nombres premiers, *C. R. Acad. Sci. Paris, Ser. I,* **298** (1984), 161–164.

[15] H. G. Diamond, Elementary methods in the study of the distribution of prime numbers, *Bull. Amer. Math. Soc.,* **7** (1982), 553–589.

[16] H. G. Diamond and P. Erdős, On sharp elementary prime number estimates, *Enseign. Math. II. Sér.,* **26** (1980), 313–321.

[17] U. Dudley, History of a formula for primes, *Amer. Math. Monthly,* **76** (1969), 23–28.

[18] H. M. Edwards, *Riemann's Zeta Function,* Academic Press, New York 1974.

[19] P. Erdős, Ob odnom asimptotičeskom něravenstve v těorii čisel, *Věstnik Leningr. Univ.,* **15** (1960), 41–49.

[20] P. Erdős, On some of my favourite theorems, 97–132. In: D. Miklós, V. T. Sós and T. Szőnyi (ed.), *Combinatorics, Paul Erdős Is Eighty. Vol. 2,* János Bolyai Mathematical Society, Budapest 1996.

[21] P. Erdős and M. Kac, The Gaussian law of errors in the theory of additive number theoretic functions, *Amer. J. Math.,* **62** (1940), 738–742.

[22] J. Friedlander and H. Iwaniecz, The polynomial $x^2 + y^4$ captures its primes, *Ann. of Math. (2),* **148** (1998), 945–1040.

[23] J. Friedlander and H. Iwaniecz, Asymptotic sieve for primes, *Ann. of Math. (2),* **148** (1998), 1041–1065.

[24] J. M. Gandhi, Formulae for the nth prime, 96–106. In: ??? (ed.), *Proceedings of the Washington State University Conference on Number Theory,* Pullman, Washington 1971.

[25] L. J. Goldstein, A history of the prime number theorem, *Amer. Math. Monthly,* **80** (1973), 599–615. [Oprava na str. 1115.]

[26] P. Hagis, Outline of a proof that every odd perfect number has at least 8 prime factors, *Math. Comp.,* **35** (1980), 1027–1032.

[27] P. Hagis, Jr. and G. L. Cohen, Every odd perfect number has a prime factor which exceeds 10^6, *Math. Comp.,* **67** (1998), 1323–1330.

[28] H. Halberstam and H.-E. Richert, *Sieve methods,* Academic Press, London 1974.

[29] G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number n, *Quart. J. Math.,* **48** (1917), 76–92.

[30] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* Oxford University Press, Oxford 1945. [Tato klasická učebnice se dočkala od r. 1938 celkem 5 vydání, posledního v roce 1979.]

[31] D. R. Heath-Brown, Odd perfect numbers, *Math. Proc. of the Cambridge Philos. Soc.,* **115** (1994), 191–196.

[32] A. Hildebrand, The prime number theorem via the large sieve, *Mathematika,* **33** (1986), 23–30.

[33] E. Hlawka, J. Schoissengaier and R. Taschner, *Geometric and Analytic Number Theory,* Springer, Berlin 1991.

[34] J. E. Z. Chein, *An odd perfect number has at least 8 prime factors*, Ph.D. thesis, Pennsylvania State University 1979.

[35] J. R. Chen, On the representation of a large even integer as the sum of a prime and the product of at most two primes, *Kexue Tonbao,* **17** (1966), 385–386.

[36] J. R. Chen, On the representation of a larger even integer as the sum of a prime and the product of at most two primes, *Sci. Sinica,* **16** (1973), 157–176.

[37] A. Ivič, *The Riemann Zeta-function,* John Wiley, New York 1985.

[38] J. P. Jones, D. Sato, H. Wada and D. Wiens, Diophantine representation of the set of prime numbers, *Amer. Math. Monthly,* **83** (1976), 449–464.

[39] A. A. Karacuba, *Osnovy Analitičeskoj Těorii Čisel,* Mir, Moskva 1983. [Anglický překlad: A. A. Karatsuba, *Basic Analytic Number Theory,* Springer, Berlin 1993.]

[40] A. A. Karatsuba and S. M. Voronin, *The Riemann Zeta-function,* W. de Gruyter, Berlin 1992. [Původně rusky 1994.]

[41] D. E. Knuth, *The Art of Compuer Programming. Volume 2. Seminumerical Algorithms,* Addison-Wesley, Reading, MA 1998. [Třetí doplněné vydání, první v r. 1969, druhé v r. 1981.]

[42] I. Korevaar, On Newman's quic way to the prime number theorem, *Math. Intell.,* **4** (1982), 108–115.

[43] D. H. Lehmer, On Lucas's test for the primality of Mersennes's numbers, *J. London Math. Soc.,* **10** (1935), 162–165.

[44] N. Levinson, A motivated account of an elementary proof of the prime number theorem, *Amer. Math. Monthly,* **76** (1969), 225–245.

[45] J. van de Lune, H. J. J. te Riele and D. T. Winter, On the zeros of the Riemann zeta function in the critical strip, IV, *Math. Comp.,* **46** (1986), 667–681.

[46] Yu. Matijasevich, My collaboration with Julia Robinson, *Mathem. Intell.,* **14** (1992), 38–45. [Addendum ibidem 1993, 75.]

[47] Yu. V. Matiyasevich, *Hilbert's Tenth Problem,* The MIT Press, Cambridge, MA 1993.

[48] W. H. Mills, A prime-representing function, *Bull. Amer. Math. Soc.,* **53** (1947), 604.

[49] Y. MOTOHASHI, *Lectures on sieve methods and prime numbers theory,* Springer, Berlin 1983.

[50] M. NATHANSON, *Additive Number Theory. The Classical Bases,* Springer, Berlin 1996.

[51] M. NATHANSON, *Elementary Methods in Number Theory,* Springer, Berlin 2000.

[52] D. J. NEWMAN, Simple analytic proof of the prime number theorem, *Amer. Math. Monthly,* **87** (1980), 693–696.

[53] D. J. NEWMAN, *Analytic Number Theory,* Springer, Berlin 1998.

[54] B. NOVÁK, *Vybrané Partie z Teorie Čísel,* Státní pedagogické nakladatelství, Praha 1972. [Skripta MFF UK.]

[55] B. NOVÁK, O osmém Hilbertově problému, *Pokroky mat., fyz. a astr.,* **18** (1973), 9–17.

[56] B. NOVÁK, O elementárním důkazu prvočíselné věty, *Čas. pro pěstování mat.,* **100** (1975), 71–84.

[57] CH. H. PAPADIMITRIOU, *Computational Complexity,* Addison-Wesley, Reading, MA 1994.

[58] G. PÓLYA AND G. SZEGÖ, *Problems and Theorems in Analysis. Volume 1 and 2,* Springer, Berlin 1972 and 1976. [Oba díly vyšly poprvé německy v roce 1925.]

[59] C. POMERANCE, A tale of two sieves, *Notices Amer. Math. Soc.,* **43** (1996), 1473–1485. [Český překlad: C. POMERANCE, Vyprávění o dvou sítech, *Pokroky mat., fyz. a astr.,* **43** (1998), 9–29.]

[60] V. R. PRATT, Every prime has a succint certifikate, *SIAM J. Comput.,* **4** (1975), 214–220.

[61] O. RAMARÉ, On Šnirel'man's constant, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.,* **22** (1995), 645–706.

[62] P. RIBENBOIM, *The New Book of Prime Number Records,* Springer, New York 1996.

[63] B. RIEMANN, Über die Anzahl der Primzahlen unter einer gegebenen Grösse, *Monatsberichte der Berliner Akademie,* **???** (1859), 671–680.

[64] P. M. ROSS, On Chen's theorem that each large even number has the form $p_1 + p_2$ or $p_1 + p_2p_3$, *J. London Math. Soc. (2),* **10** (1975), 500–506.

[65] Y. SAOUTER, Checking the odd Goldbach conjecture up to 10^{20}, *Math. Comp.,* **67** (1998), 863–866.

[66] M. D. SAYERS, *An improved lower bound for the total number of factors of an odd perfect number*, MA thesis, NSW Inst. Tech. 1986.

[67] J.-P. SERRE, *A Course in Arithmetics,* Springer, Berlin 1996. [První vydání v r. 1973.]

[68] M. K. SINISALO, Checking the Goldbach conjecture up to $4 \cdot 10^{11}$, *Math. Comp.,* **61** (1993), 931–934.

[69] L. G. SHNIREL'MAN, On the additive properties of integers, *Izv. Donskogo Politechn. Inst. v Novočerkaske,* **14** (1930), 3–27.

[70] L. G. SHNIREL'MAN, Über additive Eigenschaften von Zahlen, *Math. Ann.,* **107** (1933), 649–690.

[71] J. STILLWELL, *Elements of Algebra,* Springer, Berlin 1994.

[72] G. TENENBAUM, *Introduction to Analytic and Probabilistic Number Theory,* Cambridge University Press, Cambridge, UK 1995.

[73] E. C. TITCHMARSH, *The Theory of the Riemann Zeta-function,* The Clarendon Press, New York 1986. [Vydání z r. 1951 aktualizoval D. R. Heath-Brown.]

[74] P. TURÁN, On a theorem of Hardy and Ramanujan, *J. London Math. Soc.,* **9** (1934), 274–276.

[75] R. C. VAUGHAN, *The Hardy–Littlewood Method,* Cambridge University Press, Cambridge, UK 1997. [Druhé vydání, první v r. 1981.]

[76] I. M. VINOGRADOV, Representation of an odd number as the sum of three primes, *Dokl. Akad. Nauk SSSR,* **15** (1937), 291–294.

[77] E. M. WRIGHT, A prime-representing function, *Amer. Math. Monthly,* **58** (1951), 616–618.

[78] E. M. WRIGHT, A class of representing functions, *J. London Math. Soc.,* **29** (1954), 63–71.

[79] D. ZAGIER, Newman's short proof of the prime number theorem, *Amer. Math. Monthly,* **104** (1997), 705–708.

[80] D. ZINOVIEV, On Vinogradov's constant in Goldbach's ternary problem, *J. Number Theory,* **65** (1997), 334–358.