Vojtěch Jarník
Tři sovětské knihy o analytické theorii čísel

Časopis pro pěstování matematiky, Vol. 76 (1951), No. 1, 35--65

Persistent URL: http://dml.cz/dmlcz/116997

Časopis pro pěstování matematiky, roč. 76 (1951)

RECENSE KNIH A ČLÁNKŮ

Tři sovětské knihy o analytické theorii čísel.

V. JARNÍK, Praha.

(Referát o přednášce konané dne 23. X. 1950 v Matematické obci pražské.)

Po vítězném ukončení Velké vlastenecké války vyšly v Sovětském Svazu tři knihy, nevelké rozsahem, ale velmi významné svým obsahem. Jejich autory jsou *N. G. Čudakov*, akademik *I. M. Vinogradov* a jeho čínský žák a spolupracovník *Loo Keng Hua*. Tyto knihy tvoří zároveň jakýsi celek. Kniha *Vinogradovova* vykládá autorovy methody, které tak převratně působily v analytické theorii čísel, kniha *Huova* pak vykládá o řešení složitého problému (t. zv. problému Waring-Goldbachova), při němž je nutno kombinovati různé methody Vinogradovovy a na některých místech je doplniti. Kniha *Čudakovova* pak je první knihou ve světové literatuře, která systematicky vykládá od samého počátku základy, na nichž spočívají právě nejvýznamnější části Vinogradovových prací, totiž ty, které se zabývají aditivní theorií prvočísel. Považuji proto tento referát za vhodnou příležitost, abych čtenáře nejenom informoval o těchto knihách, nýbrž i o naukách v nich projednávaných, a to způsobem obšírnějším, než bývá zvykem.

I. *Н. Г. Чудаков:* **Введение в теорию L-функций Дирихле.** (*N. G. Čudakov*: **Úvod do theorie Dirichletových L-funkcí.**) ОГИЗ, Moskva-Leningrad 1947, str. 203, cena 7 r., tiráž 5000 exemplářů.

Jedním z nejzákladnějších problémů analytické theorie prvočísel je vyšetřování asymptotického průběhu funkce $\pi(x)$ pro $x \to +\infty$; při tom $\pi(x)$ značí počet prvočísel, jež nejsou větší než x; tedy $\pi(2) = 1$, $\pi(3) = \pi(4) = 2$, $\pi(5) = \pi(6) = 3$, $\pi(7) = \ldots = \pi(10) = 4$ atd. Je známo, že

$$\pi(x) \sim \frac{x}{\log x}, \text{ t. j. že } \lim_{x \to +\infty} \frac{\pi(x) \log x}{x} = 1.$$

Tuto slavnou „prvočíselnou větu" dokázali r. 1896 nezávisle na sobě *Hadamard* a *de la Vallée-Poussin*.

Funkci $\pi(x)$ lze tedy v prvním přiblížení aproximovati funkcí $\frac{x}{\log x}$. Ale lépe se dá funkce $\pi(x)$ aproximovati funkcí $\operatorname{li} x = \int_2^x \frac{\mathrm{d}t}{\log t} + c$[1]) $\left(\text{jest ovšem } \operatorname{li} x \sim \frac{x}{\log x}\right)$.

Platí totiž: položíme-li

$$\pi(x) = \operatorname{li} x + R(x), \tag{1}$$

[1]) Při tom c je jistá konstanta; na její hodnotě nám zde nezáleží.

potom existují kladná čísla C, μ tak, že je

$$|R(x)| < Cx\mathrm{e}^{-\mu\sqrt{\log x}} \text{ pro všechna } x > 1. \tag{2}$$

(Je zvykem, psáti tento vztah s použitím známého symbolu O ve tvaru

$$\pi(x) = \mathrm{li}x + O(x\mathrm{e}^{-\mu\sqrt{\log x}}).)^{2}) \tag{3}$$

Studium funkce $\pi(x)$ je možno dále prohloubiti: Jednak je možno studovati nepravidelnosti v rozdělení prvočísel, t. j. sledovati „oscilace" funkce $R(x)$ (je na př. známo, že pro některá libovolně velká x nabývá $R(x)$ jak kladných tak záporných hodnot velikosti

$$|R(x)| > \text{konst.}\, x^{\frac{1}{2}}(\log x)^{-1}\log\log\log x),$$

dále je možno hledati odhady pro rozdíl $p_{n+1} - p_n$ dvou po sobě jdoucích prvočísel a konečně je možno snažit se o zostření nerovnosti (2). Všechny tyto otázky, a vedle nich ještě jiné, byly vyšetřovány v mnoha pracích. V posledních 15 letech poskytly znamenité výsledky *Vinogradovovy*, týkající se trigonometrických součtů, nové možnosti při vyšetřování druhé a třetí ze zmíněných tří otázek. Na př. právě *Čudakov* podal podstatné příspěvky k těmto problémům. Nebudu se však těmito věcmi zde zabývati (několik slov o zostření odhadu (2) řeknu na konci referátu o Čudakovově knize).

Zaveďme nyní toto zobecnění funkce $\pi(x)$. Buďte k, l dvě přirozená čísla, $0 < l \leqq k$. Označme znakem $\pi(x, k, l)$ počet prvočísel $p \leqq x$, ležících v aritmetické posloupnosti

$$l, l + k, l + 2k, l + 3k, l + 4k, \ldots \tag{4}$$

Mají-li čísla l, k společného dělitele $d > 1$, jsou všechna čísla $l + nk$ dělitelna číslem d, a tedy posloupnost (4) obsahuje nejvýše jedno prvočíslo. Avšak jsou-li l, k nesoudělná, potom posloupnost (4) obsahuje nekonečně mnoho prvočísel, jak již r. 1837 dokázal *Dirichlet*. Počet čísel l $(0 < l \leqq k)$, nesoudělných s daným číslem k, označme $\varphi(k)$. Jak dokázali *de la Vallée-Poussin* a *Landau*, platí pro $\pi(x, k, l)$ odhad obdobný vztahům (1), (2): *Jsou-li l, k nesoudělná, $0 < l \leqq k$, je*

$$\pi(x, k, l) = \frac{1}{\varphi(k)}\mathrm{li}x + R_{k,l}(x), \tag{5}$$

kde

$$|R_{k,l}(x)| < C_k x\mathrm{e}^{-\mu_k\sqrt{\log x}} \tag{6}$$

pro všechna $x > 1$; při tom C_k, μ_k jsou kladná čísla, závislá pouze na k.[3]) Z (5), (6) je vidět rovnoměrné rozdělení prvočísel mezi $\varphi(k)$ posloupností (4), které odpovídají různým hodnotám l (nesoudělným s k); na každou z nich připadá přibližně stejný počet prvočísel $p \leqq x$, je-li x dosti velké. Vzorce (1), (2) jsou speciálním případem vzorců (5), (6) pro $k = l = 1$.

Ale nerovnost (6) není ještě zcela uspokojující. Právě ve své fenomenální práci o Goldbachově problému potřeboval *Vinogradov* studovati současně několik funkcí $\pi(x, k, l)$ (při téže hodnotě x, ale pro různá k, l), při čemž počet vyšetřovaných hodnot k, l byl velmi veliký při velkém x. Vzorec (6), jehož pravá strana způsobem blíže neznámým závisí na k, neměl proto pro něj cenu. Ale na štěstí platí vedle vzorce (6) ještě tento ostřejší odhad: *Zvolme libovolné* (sebe větší) *číslo M. Potom pro všechna k, l, x, která vyhovují podmínkám*[4])

$$[l, k] = 1, \; 0 < l \leqq k < (\log x)^M, \tag{7}$$

---

[2]) Tento odhad dokázal *de la Vallée-Poussin* r. 1899.

[3]) Formuli (6) dokázal *Landau* 1909. Před ním *de la Vallée-Poussin* dokázal pouze $\pi(x, k, l) \sim \dfrac{x}{\varphi(k)\log x}$ pro $x \to +\infty$.

[4]) Znakem $[l, k]$ budu značiti největšího společného dělitele čísel k, l.

platí nerovnost

$$|R_{k,l}(x)| < C_M x e^{-\mu_M \sqrt{\log x}}, \tag{8}$$

kde C_M, μ_M *jsou kladná čísla, závislá pouze na* M (tedy nezávislá na x, k, l). Tento výsledek je bezprostředním důsledkem prací *Pageových* a *Siegelových*, a obsahuje ovšem odhad (6) (stačí zvoliti k pevné).

Důkazy odhadů (2) a (6) byly už v literatuře dobře přístupny: viz na př. pro nerovnost (2) velmi pěknou knížku *A. E. Inghama*, The distribution of prime numbers (Cambridge Tracts in Mathem. and Math. Physics 30, 1932), o které jsem napsal recensi v tomto Časopise, roč. **67**, (1937—8) str. D54—D56; tato kniha vyšla též rusky (А. Е. Ингам, Распределение простых чисел, ОНТИ 1936); obecnější nerovnost (6) je dokázána na př. u *E. Landaua*, Vorlesungen über Zahlentheorie, II. svazek (Leipzig, Hirzel, 1927); viz moji recensi této knihy v Časopise, roč. **57**, (1927—8) str. 62—63.

Avšak obecnější, a právě v poslední době tak důležitý odhad (8) byl dosud přístupný pouze studiem řady ne snadných pojednání, roztroušených po časopisech. Je velkou zásluhou *N. G. Čudakova*, že svou novou knihu zaměřil — mimo jiné — právě k tomu, aby čtenáře dovedl od prvních počátků theorie Dirichletových L-funkcí spolehlivě až k této větě.

Pokusím se nyní stručně vylíčiti, co to jsou Dirichletovy L-funkce a jak souvisí s problémem rozložení prvočísel v aritmetické posloupnosti (4); při tom vylíčím obsah *Čudakovovy* knihy. První kapitola je věnována klasické theorii charakterů, která však je zde podána novým, elementárním a velmi vhodným způsobem.

Charakterem nazýváme funkci (obecně komplexní) $\chi(n)$, definovanou pro všechna celá n, jež má tyto tři vlastnosti: Funkce $\chi(n)$ není rovna nule identicky (t. j. pro všechna celá n); pro všechna celá m, n je $\chi(mn) = \chi(m)\chi(n)$; funkce χ má celočíselnou kladnou periodu. Nejmenší kladná perioda se nazývá *základním modulem* funkce χ; všechny kladné periody jsou pak násobky základního modulu. Ty kladné periody, které nejsou dělitelny žádným prvočíslem neobsaženým v základním modulu, nazývá *Čudakov moduly* charakteru χ.

Je-li na př. 18 základním modulem, jsou moduly všechna čísla $2^a 3^b$ ($a = 1, 2, 3, \ldots$; $b = 2, 3, 4, \ldots$). Číslo 180 je periodou, ale není modulem. Ježto $\chi(n) = \chi(1 \cdot n) = \chi(1)\chi(n)$, je vždy $\chi(1) = 1$. Nechť má nyní charakter χ modul k. Je-li $[k, n] \neq 1$, je $\chi(n) = 0$. Je-li $[k, n] = 1$, je podle Fermatovy věty $n^{\varphi(k)} \equiv 1 \pmod{k}$, tedy $(\chi(n))^{\varphi(k)} = \chi(n^{\varphi(k)}) = \chi(1) = 1$.

Všechny od nuly různé hodnoty charakteru χ jsou tedy $\varphi(k)$-té odmocniny z 1. To vede k tomuto třídění charakterů: charakter se nazývá *hlavním* (znak: χ_0), nenabývá-li jiných hodnot než 0, 1; charakter je *druhého druhu*, je-li reálný, ale ne hlavní, t. j. nabývá-li tří různých hodnot 0, 1, —1; charakter je *třetího druhu*, jestliže nabývá také imaginárních hodnot.

Druhá kapitola knihy je věnována Dirichletovým řadám, t. j. řadám tvaru

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}, \tag{9}$$

[5])

kde a_n jsou komplexní konstanty, $s = \sigma + it$ je komplexní proměnná (označení s pro komplexní proměnnou a σ, t pro její reálnou a imaginární část budeme stále užívati); $n^s = e^{s \log n}$, kde $\log n$ je reálný logaritmus. Nejznámější Dirichletovou řadou je t. zv. Riemannova funkce

[5]) V prvním paragrafu jsou studovány ještě obecnější řady.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{10}$$

Tato řada je absolutně konvergentní pro $\sigma > 1$; funkce ζ dá se však analyticky pokračovati do celé komplexní roviny, a má jedinou singularitu v bodě $s = 1$, totiž pól prvního řádu. Zobecněním funkce ζ jsou právě Dirichletovy L-funkce, definované takto: Je-li χ libovolný charakter, položme

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{11}$$

To je opět funkce komplexní proměnné s; řada konverguje absolutně pro $\sigma > 1$, a funkci $L(s, \chi)$ lze analyticky pokračovati do celé roviny. Je-li χ hlavní charakter, liší se $L(s, \chi)$ pouze nepodstatně od $\zeta(s)$. Jestliže však χ není hlavní charakter, potom pro každé n jest $\chi(n + 1) + \chi(n + 2) + \ldots + \chi(n + k) = 0$ (kde k je modul charakteru χ); následkem toho se jednotliví členové v řadě (11) vykompensují do té míry, že pól v bodě $s = 1$ zmizí, a funkce $L(s, \chi)$ je celistvá.

Funkce ζ vyhovuje funkční rovnici

$$\zeta(1 - s) = 2(2\pi)^{-s} \Gamma(s) \cos\tfrac{1}{2}\pi s \,.\, \zeta(s), \tag{12}$$

a podobně platí pro t. zv. primitivní charaktery (co to je, nebudu vykládati) vztah, který určuje $L(1 - s, \overline{\chi})$ pomocí $L(s, \chi)$ (při tom $\overline{\chi}$ je charakter komplexně sdružený k χ). Toto vše (a ještě trochu více) je obsahem druhé kapitoly.

Abych osvětlil smysl třetí a čtvrté kapitoly, ukáži, jak souvisí funkce (10), (11) s prvočísly. V půlrovině $\sigma > 1$ platí vztah, známý již *Eulerovi*:

$$\zeta(s) = \prod_p (1 + p^{-s} + p^{-2s} + p^{-3s} + \ldots) = \prod_p (1 - p^{-s})^{-1} \tag{13}$$

(násobí se přes všechna prvočísla p); logaritmujeme-li nekonečný součin a potom derivujeme, obdržíme

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{p^{-s}}{1 - p^{-s}} \log p = \sum_p \log p \,.\, (p^{-s} + p^{-2s} + p^{-3s} + \ldots). \tag{14}$$

Formálně obdržíme (13), (14) triviálním výpočtem; oprávněnost těchto operací pak plyne z absolutní konvergence příslušných řad. Definujme funkci $\Lambda(n)$ takto: Je-li n číslo tvaru p^m (p prvočíslo, m přirozené číslo), budiž $\Lambda(n) = \log p$; v ostatních případech budiž $\Lambda(n) = 0$. Potom lze (14) napsati ve tvaru

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \quad (\text{pro } \sigma > 1). \tag{15}$$

Je známo, že limita $\lim_{T \to +\infty} \frac{1}{2\pi i} \int_{a-Ti}^{a+Ti} \frac{y^s}{s}\, ds$ je rovna nule pro $0 < y < 1$ a rovna jedné pro $y > 1$; při tom je $a > 0$ a integruje se přes úsečku $\sigma = a$, $-T \leqq t \leqq T$ (rovnoběžnou s imaginární osou). Budiž x libovolné necelé kladné číslo.[6]) Zvolíme-li $a > 1$, násobíme (15) výrazem $\frac{1}{2\pi i} \frac{x^s}{s}$ a integrujeme od $a - Ti$ do $a + Ti$, zjistíme snadno, že můžeme přejíti k limitě člen po členu, a obdržíme

[6]) Ani celá x nečiní zvláštních obtíží.

$$-\frac{1}{2\pi i}\lim_{T\to+\infty}\int_{a-Ti}^{a+Ti}\frac{x^s}{s}\frac{\zeta'(s)}{\zeta(s)}\,ds=\sum_{n\leq x}\Lambda(n)=$$
$$=\sum_{p\leq x}\log p+\sum_{p\leq x^{\frac{1}{2}}}\log p+\sum_{p\leq x^{\frac{1}{3}}}\log p+\dots \tag{16}$$

Snadno se ukáže, že všechny součty vpravo až na první dávají součet řádu nejvýše $x^{\frac{1}{2}}\log x$; je tedy pravá strana v (16) rovna

$$\sum_{p\leq x}\log p+O(\sqrt{x}\log x), \tag{17}$$

kde symbol $O(f(x))$ značí funkci, která je v absolutní hodnotě menší než $c\,f(x)$, kde c je vhodně zvolená konstanta. Ukáže se dále, že výraz (17) je pro $x\to+\infty$ téhož řádu jako x, takže člen $O(\sqrt{x}\log x)$ je pro náš asymptotický problém bez významu. Dále se velmi snadno ukáže, že každý náš poznatek o velikosti funkce $\Sigma\log p$ vede k obdobnému poznatku (přibližně téže přesnosti) o velikosti funkce $\Sigma\,1=\pi(x)$ (levá strana je ovšem součet tolika jedniček, kolik je prvočísel až do čísla x). Tedy: *Místo asymptotického vyšetřování funkce $\pi(x)$ můžeme vyšetřovati integrál na levé straně rovnice* (16). Tím je ukázáno, jaká je souvislost mezi funkcí $\pi(x)$ a funkcí $\zeta(s)$.

Buďte nyní dána dvě nesoudělná čísla k, l $(0<l\leq k)$ a zabývejme se funkcí $\pi(x,k,l)$, která udává počet prvočísel $p\leq x$ v aritmetické posloupnosti (4). Jak isolovati ona prvočísla, která leží v této posloupnosti?

K tomu nám pomohou právě L-funkce, jak už poznal Dirichlet. Je známo, že k číslu k existuje právě $\varphi(k)$ charakterů s modulem k. Vezměme jeden z nich, $\chi(n)$, a sestrojme funkci

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}. \tag{18}$$

Vzhledem ke vztahu $\chi(mn)=\chi(m)\,\chi(n)$ můžeme prováděti s funkcí $L(s,\chi)$ přesně tytéž operace, které jsme prováděli v rovnicích (13), (14), (15), (16), (17) s funkcí $\zeta(s)$; pouze místo n^{-s}, p^{-ms} se všude vyskytne

$$\chi(n)\,.\,n^{-s},\quad(\chi(p))^m\,p^{-ms}=\chi(p^m)\,.\,(p^m)^{-s}.$$

Nakonec vyjde, podobně jako v (16), (17), rovnice

$$-\frac{1}{2\pi i}\lim_{T\to+\infty}\int_{a-Ti}^{a+Ti}\frac{x^s}{s}\frac{L'(s,\chi)}{L(s,\chi)}\,ds=\sum_{p\leq x}\chi(p)\log p+O(\sqrt{x}\log x). \tag{19}$$

Z theorie charakterů je však známo: Jsou-li l, n dvě celá čísla, $[l,k]=1$, a sestrojíme-li součet

$$S(n)=\frac{1}{\varphi(k)}\sum_{\chi}\overline{\chi}(l)\,\chi(n),$$

při čemž se sčítá přes všechny charaktery χ o modulu k (v počtu $\varphi(k)$), potom je $S(n)=1$ pro $n\equiv l\pmod k$, ale $S(n)=0$ ve všech ostatních případech. Tedy: Jestliže rovnici (19) násobím číslem $\overline{\chi}(l):\varphi(k)$ a sečtu přes všechny charaktery χ o modulu k, dostanu vpravo právě

$$\Sigma\log p+O(\sqrt{x}\log x), \tag{20}$$

kde součet se vztahuje na všechna prvočísla $p\leq x$, ležící v posloupnosti (4). Dove-

du-li přibližně vypočísti tento součet, dovedu opět již velmi snadno vypočísti přibližně číslo $\pi(x, k, l)$ (podobně jako u výrazu (17)). Celý náš úkol se tedy redukuje na úkol: *Vypočísti přibližně integrál v* (19) *pro* $x \to \infty$. Při tom a je libovolné číslo větší než 1 (limita v (19) nezávisí na a).

K přibližnému výpočtu integrálu v (19) postupuji pak takto: Budiž x nějaké číslo „hodně velké". Zvolím T „velké" a číslo a blízko jedné (ukazuje se na př. vhodným, voliti

$$T = e^{\sqrt{\log x}}, \quad a = 1 + \frac{1}{\log x}).$$

Zvolme nějakou křivku C_1 v rovině komplexní proměnné s, danou rovnicí

$$\sigma = \varphi(t), \tag{21}$$

kde $\frac{1}{2} < \varphi(t) < 1$. Sestrojme uzavřenou křivku C, skládající se z úsečky

$$\sigma = a, \quad -T \leqq t \leqq T \tag{22}$$

z oblouku $C_1(T)$ křivky C_1:

$$\sigma = \varphi(t), \quad -T \leqq t \leqq T \tag{23}$$

a ze dvou „vodorovných" úseček U_1, U_2, spojujících krajní body úsečky (22) s krajními body $C_1(T)$:

$$\varphi(T) \leqq \sigma \leqq a, \ t = T; \ \varphi(-T) \leqq \sigma \leqq a, \ t = -T$$

(načrtněte si to!). Jestliže tato křivka C neprochází žádným nulovým bodem funkce $L(s, \chi)$, je

$$-\frac{1}{2\pi i}\int_{a-Ti}^{a+Ti} \frac{x^s}{s}\frac{L'(s,\chi)}{L(s,\chi)}\,ds = \frac{1}{2\pi i}\int_{C_1(T)} + \frac{1}{2\pi i}\int_{U_1} - \frac{1}{2\pi i}\int_{U_2} + \mathbf{S}, \tag{24}$$

kde $\mathbf{S}$ je součet residuí funkce $-\frac{x^s}{s}\frac{L'(s,\chi)}{L(s,\chi)}$ uvnitř křivky C. Ježto funkce $L' : L$ má pól 1. řádu s residuem m v každém bodě, jenž je nulovým bodem m-tého řádu funkce L (při čemž pól řádu n-tého funkce L jest interpretovati jako „nulový bod řádu $-n$"), vidíme, že $\mathbf{S}$ obsahuje především člen δx pocházející od pólu funkce L v bodě $s = 1$ (při tom $\delta = 1$, je-li charakter χ hlavní, $\delta = 0$, není-li χ hlavní: neboť potom bod $s = 1$ není pólem). Dále obsahuje $\mathbf{S}$ součet

$$-\sum_{\gamma}\frac{x^\gamma}{\gamma}, \tag{24a}$$

kde se sčítá přes všechny nulové body γ funkce L, ležící uvnitř C (každý se bere tolikrát, kolik činí jeho násobnost). Lze dokázati, že v půlrovině $\sigma \geqq 1$ je stále $L(s, \chi) \neq 0$ (jedinou vážnou obtíž, překonanou již *Dirichletem*, působí nehlavní reálné charaktery v bodě $s = 1$). Píši-li tedy v (24a) $\gamma = \alpha + \beta i$, je $\alpha < 1$. Ježto $|x^\gamma| = x^\alpha$, hraje v součtu $\mathbf{S}$ roli hlavního členu člen x (vystupující ovšem pouze v případě, kdy χ je hlavní charakter). Nahradím-li tedy levou stranu v (24) číslem δx, dopustím se chyby, která je dána součtem

$$\frac{1}{2\pi i}\int_{C_1(T)} \frac{x^s}{s}\frac{L'(s,\chi)}{L(s,\chi)}\,ds + \frac{1}{2\pi i}\int_{U_1} - \frac{1}{2\pi i}\int_{U_2} - \sum_{\gamma}\frac{x^\gamma}{\gamma}. \tag{25}$$

Jde nyní o to, voliti funkci $\varphi(t)$, t. j. křivku $C_1(T)$ tak, abychom mohli výraz (25) co nejvýhodněji odhadnouti. Integrály přes „krátké" úsečky U_1, U_2 nebudou činiti obtíží, jakmile zvládneme integrál přes $C_1(T)$. Zabývejme se proto jen prvním a posledním členem v (25). Ježto na křivce $C_1(T)$ je $\sigma = \varphi(t)$ a tedy $|x^s| = x^{\varphi(t)}$, bude

pro odhad integrálu přes $C_1(T)$ výhodno, bude-li $\varphi(t)$ co možná malé, t. j. bude-li křivka $C_1(T)$ ležeti pokud možná daleko „vlevo" od přímky $\sigma = 1$. Ale zde se naskytuje hned další obtíž: Posuneme-li čáru $C_1(T)$ příliš daleko doleva, může se státi, že mezi touto čarou a přímkou $\sigma = 1$ bude ležeti příliš mnoho nulových bodů γ funkce $L(s, \chi)$, což by nám znemožnilo odhad součtu $\Sigma x^\gamma : \gamma$. Je tedy naším úkolem:

A) Nalézti funkci $\varphi(t)$ (co nejmenší) tak, aby neexistoval buďto žádný nulový bod nebo jen málo nulových bodů v oblasti $\sigma > \varphi(t)$.

K tomu se ovšem druží ještě další problém:

B) Nalézti funkci $\varphi(t)$ současně tak, abychom na křivce $C_1(T)$ dostali výhodný odhad funkce $L'(s, \chi) : L(s, \chi)$ — neboť jinak bychom nemohli odhadnout integrál přes $C_1(T)$.

Ale tento problém B) bude rozřešen, jakmile rozřešíme problém A). Platí totiž tato věta (Carathéodoryova): Je-li $f(s)$ regulární v kruhu $|s - s_0| < R$, a vyhovuje-li reálná část funkce f v tomto kruhu nerovnosti $\boldsymbol{R}\, f(s) \leqq U$ (kde U je nějaká konstanta), potom v kruhu $|s - s_0| < r$ (kde $0 < r < R$) je

$$|f'(s)| \leqq \frac{2R}{(R-r)^2}\,(U - \boldsymbol{R}\, f(s_0)). \tag{26}$$

Mám-li nyní kruh o středu $s_0 = 1 + \frac{1}{\log x} + it_0$ a o poloměru $R < \frac{1}{2}$, potom velmi snadno dostanu odhad (zdola i shora) pro

$$\boldsymbol{R} \log L(s_0, \chi) = \log|L(s_0, \chi)|;$$

za druhé dostanu snadno odhad shora pro $|L(s, \chi)|$ v kruhu[7]) $|s - s_0| < R$, a tedy i odhad shora pro

$$\log|L(s, \chi)| = \boldsymbol{R} \log L(s, \chi).$$

Jestliže v tomto kruhu je $L(s, \chi) \neq 0$, je v něm $\log L(s, \chi)$ regulární, a aplikací věty Carathéodoryovy na funkci $f(s) = \log L(s, \chi)$ dostanu z (26) odhad pro $|L'(s, \chi) : L(s, \chi)|$ v každém menším koncentrickém kruhu. Tedy problém B) bude řešen, najdu-li vhodný obor, v němž $L(s, \chi)$ nemá nulových bodů, t. j. rozřeším-li problém A). (Vypadá to asi takto: Nemá-li $L(s, \chi)$ nulových bodů vpravo od křivky $\sigma = \varphi_1(t)$, potom stačí funkci $\varphi_1(t)$ nahradit funkcí $\varphi(t)$ o něco málo větší, aby byl splněn vedle požadavku A) i požadavek B). Při tom dokonce nevadí, je-li vpravo od křivky $\sigma = \varphi_1(t)$ dostatečně malý počet nulových bodů — potom ovšem je nutno trochu upravit použití Carathéodoryovy věty.)

Zbývá tedy řešiti problém A), t. j. nalézti co nejmenší funkci $\varphi(t)$ tak, aby v oboru $\sigma \geqq \varphi(t)$ leželo jenom „málo" kořenů funkcí $L(s, \chi)$. Tomuto problému je věnována 3. kapitola *Čudakovovy* knihy; při jeho řešení se opět vydatně užívá Carathéodoryovy věty. Při *pevném* k byl tento problém řešen již dávno (důkaz lze si přečísti v citované knize Landauově). Výsledek je tento: Budiž k přirozené číslo; potom existuje kladné číslo $c(k)$, závislé pouze na k, s touto vlastností: Je-li χ libovolný charakter o modulu k, potom všechny nulové body funkce $L(s, \chi)$ leží vlevo od křivky

$$\sigma = 1 - \frac{c(k)}{\log(|t| + 3)}. \tag{27}$$

To značí: každý nulový bod $\sigma + it$ této funkce vyhovuje nerovnosti

$$\sigma < 1 - \frac{c(k)}{\log(|t| + 3)}. \tag{28}$$

[7]) Pokud tento kruh neobsahuje body, blízké bodu $s = 1$.

Z tohoto výsledku jest již možno odvoditi odhad (6) (a tedy i odhad (2)). Nelze z něho však odvoditi odhad (8), pokud nezjistíme, jakým způsobem závisí $c(k)$ na k, po příp. dokud nenahradíme nerovnost (28) jinou nerovností, v níž by závislost na čísle k byla explicite vytčena. Takovou nerovnost odvodil *Page*; jeho výsledek je velmi zajímavý:

Existuje číslo $c > 0$ (nezávislé už vůbec na ničem, t. j. tak zvaná „absolutní konstanta") s těmito dvěma vlastnostmi:

Budiž k libovolné přirozené číslo; vyšetřujme všechny možné funkce $L(s, \chi)$, patřící ke všem možným charakterům o modulu k (počet těchto funkcí je $\varphi(k)$). Potom platí:[8])

1. Všechny nereálné nulové body $\sigma + it$ všech těchto funkcí vyhovují nerovnosti

$$\sigma \leqq 1 - \frac{c}{\log(k(|t| + 3))}. \tag{29}$$

2. Také všechny reálné nulové body σ všech těchto funkcí vyhovují nerovnosti (29) (kde ovšem $t = 0$), t. j. nerovnosti

$$\sigma \leqq 1 - \frac{c}{\log 3k}, \tag{30}$$

s jedinou možnou výjimkou. Obšírně: Mezi všemi uvažovanými funkcemi $L(s, \chi)$ (při daném k) existuje nejvýše jedna (označme ji $L(s, \chi_1)$), u níž existuje reálný nulový bod σ_1, vyhovující nerovnosti

$$\sigma_1 > 1 - \frac{c}{\log 3k}; \tag{31}$$

takový nulový bod σ_1 existuje pak u funkce $L(s, \chi_1)$ jen jeden, je nutně jednoduchý a příslušný charakter χ_1 je nutně druhého druhu.

Tomuto nulovému bodu σ_1 (existuje-li) budeme říkati *výjimečný nulový bod* (příslušný k danému číslu k).

Zvolíme-li za křivku $C_1(T)$ v (25) křivku

$$\sigma = 1 - \frac{c'}{\log(k(|t| + 3))}, \quad -T \leqq t \leqq T, \tag{32}$$

kde volím vhodně $c' > 0$, $c' < c$, podaří se nám snadno odhadnouti integrály v (25). Pokud se pak týče posledního členu v (25), který se vztahuje na nulové body funkce $L(s, \chi)$, ležící vpravo od křivky (32), potom tento člen odpadá, není-li χ právě oním „výjimečným" charakterem χ_1, kdežto pro $\chi = \chi_1$ může tento člen býti roven $-x^{\sigma_1} : \sigma_1$. Ježto, jak jsme si rozvážili, je hlavním členem v celém výpočtu výraz x, pocházející od pólu funkce $L(s, \chi_0)$ (χ_0 je hlavní charakter) v bodě 1, jde o to, zjistit, že člen x^{σ_1} je podstatně nižšího řádu než x, aby nás při konečném odhadu „zbytku" $R_{k,1}(x)$ v (8) nerušil. Není tedy vyhnutí: také pro σ_1 musíme hledati odhad analogický odhadu (30), ovšem méně přesný. *Page* odvodil tuto nerovnost:

Pro $k > 1$ je

$$\sigma_1 < 1 - c_1 k^{-\frac{1}{2}} (\log k)^{-2}, \tag{33}$$

kde $c_1 > 0$ je jistá „absolutní konstanta". *Siegel* pak dokázal: Ke každému $\varepsilon > 0$ existuje číslo $c(\varepsilon) > 0$ (závislé pouze na ε) tak, že pro každé přirozené k je

$$\sigma_1 < 1 - c(\varepsilon)\, k^{-\varepsilon}. \tag{34}$$

[8]) Tento výsledek s nepatrnou modifikací platí i tehdy, uvažujeme-li současně všechny charaktery se všemi moduly od 1 až do k.

Ježto pro $0 < \varepsilon < \frac{1}{2}$ a pro dosti velká k je

$$1 - \frac{c}{\log 3k} < 1 - \frac{c(\varepsilon)}{k^{\varepsilon}} < 1 - \frac{c_1}{k^{\frac{1}{4}} \log^2 k},$$

je *Siegelova* nerovnost ovšem horší než nerovnost (30) (platná pro „nevýjimečné" reálné nulové body σ), ale lepší než *Pageova* nerovnost (33). Přes to nelze nerovnost (33) jen tak beze všeho zahoditi, a to pro tento velmi zajímavý rozdíl mezi (33) a (34): Provádíme-li důkaz nerovnosti (33) a provedeme-li při tom všechny odhady až do numerických podrobností, můžeme nalézti *numerickou* hodnotu c_1 tak, že pro ni platí nerovnost (33). Naproti tomu všechny dosud známé důkazy *Siegelovy* věty jsou ryze existenční a nedávají možnosti, určiti číslo $c(\varepsilon)$. Tak na př. pro $\varepsilon = \frac{1}{4}$ nedovedeme udati žádné číslo $c(\frac{1}{4}) > 0$ tak, aby pro každé k bylo $\sigma_1 < 1 - c(\frac{1}{4})\, k^{-\frac{1}{4}}$ (pokud ovšem výjimečný nulový bod existuje); víme pouze, že takové číslo $c(\frac{1}{4}) > 0$ existuje.

To, co jsem právě vyložil o poloze nulových bodů funkcí $L(s, \chi)$, je hlavním obsahem třetí kapitoly *Čudakovovy* knihy. V první části čtvrté kapitoly používá pak *Čudakov* těchto výsledků k důkazu vzorce (8).[9]) V druhé části čtvrté kapitoly užívá *Čudakov* těchto výsledků k odvození slavné věty *I. M. Vinogradova* o *Goldbachově* domněnce; o této věci však zde nebudu mluvit, ježto o ní obšírněji pojednám při zprávě o knize *Vinogradovově*.

Pro lepší přehlednost jsem nevyslovil všechny výsledky v nejostřejší formě: čtenář proto najde u *Čudakova* o něco více, než je zde uvedeno. Původní *Siegelův* důkaz vzorce (34) spočíval na hlubokých pojmech a větách z theorie algebraických těles. Důkaz, podaný *Čudakovem*, je sice složitý, ale vystačí s běžnými prostředky analysy. Po publikaci *Čudakovovy* knihy vyšla krátká práce *T. Estermanna*,[10]) obsahující velmi jednoduchý a elementární důkaz *Siegelovy* věty, která tedy nikterak neleží tak „hluboko", jak se dosud zdálo.

Čtenář si snad uvědomil, že další pokrok ve zlepšení odhadů (2), (6), (8) spočívá ve zlepšení našich znalostí o nulových bodech funkcí $L(s, \chi)$ (při odhadu (2) jde pouze o funkci $\zeta(s)$), t. j. ve zlepšení odhadů (28), (29), (33), (34). Pro funkci $\pi(x)$ (t. j. pro odhad (2)) učinil r. 1921 první krok v tomto směru *J. E. Littlewood* (viz na př. citovanou knihu *Landauovu*). Ale teprve fundamentální výsledky *I. M. Vinogradova* o trigonometrických součtech umožnily další podstatný pokrok. O těchto věcech *Čudakovova* kniha nemluví; doufejme, že je najdeme v slibovaném 2. díle této knihy.

Čudakovova kniha je vzornou, dokonale promyšlenou a propracovanou monografií, která se od začátku až do konce dobře čte. Tiskových chyb (a snad i drobných nedopatření) je poměrně dost, ale kniha je psána tak přesně a srozumitelně, že je čtenář ihned objeví a snadno si je opraví.

Požadavky na předběžné znalosti čtenáře jsou mírné. Vedle běžných znalostí z integrálního počtu a z theorie analytických funkcí (pouze základní věci) se požadují první elementy theorie čísel;[11]) pouze na dvou místech se opírá *Čudakov* o citovanou knihu *Inghamovu*.[12])

---

[9]) Na základě *Siegelovy* nerovnosti (34).

[10]) On *Dirichlet's L*-functions, Journal of the London Math. Soc. **23**, 275 až 279 (1948).

[11]) V rozsahu knihy *I. M. Vinogradova*, Основы теории чисел; viz moji recensi této knížky v Časopise 74 (1949), str. D88—D89. Mezitím vyšlo již 5. vydání.

[12]) Jde o snadný theorém A na str. 57, a o obtížnější theorém B na str. 112, jehož důkaz lze nalézti na př. též u *E. Landaua*, Vorlesungen über Zahlentheorie I, věta 225. [Formule pro c_n je u Landaua (který píše a_n); zbytek si čtenář snadno doplní.]

II. *И. М. Виноградов:* **Метод тригонометрических сумм в теории чисел** (*I. M. Vinogradov, Methoda trigonometrických součtů v theorii čísel*). Práce matematického ústavu V. A. Stěklova XXIII (1947), Moskva-Leningrad, vydavatelstvo Akademie Nauk SSSR, str. 109, cena 9 r., tiráž 2000 exemplářů.

Obsah knihy je rozvržen stejně jako v knize téhož autora „Nová methoda v analytické theorii čísel" (Práce mat. úst. V. A. Stěklova X, 1937).[13]) Od r. 1937 zdokonalil *Vinogradov* své methody, a tak srovnání obou knih umožňuje sledovati pokrok, kterého bylo v té době dosaženo.

Abych uvedl čtenáře do problematiky této knihy, začnu s t. zv. *Waringovým* problémem. *Waring* vyslovil r. 1770 tuto domněnku: Ke každému přirozenému číslu $n > 1$ existuje číslo r (závislé na n) takové, že každé přirozené číslo N lze vyjádřit jako součet r „n-tých mocnin", t. j. ve tvaru

$$N = x_1^n + x_2^n + \ldots + x_r^n \quad (x_i \geqq 0, \text{ celá}). \tag{35}$$

Pro $n = 2$ rozřešil tento problém již *Lagrange*: Zde je možno položiti $r = 4$, t. j. každé přirozené číslo N lze psáti ve tvaru $N = x_1^2 + x_2^2 + x_3^2 + x_4^2$ ($x_i \geqq 0$ celá). Pro obecné n byla *Waringova* domněnka dokázána až r. 1909 *Hilbertem*. Tím ovšem problém nebyl uzavřen, neboť vzniká ještě otázka po nejmenším možném r (při daném n) a otázka, na kolik různých způsobů lze číslo N vyjádřiti ve tvaru (35) při daných hodnotách n, r. Celkem jde tedy o tyto tři hlavní otázky:

I. *Dokázati Waringovu domněnku.*

II. Označme (při daném n) znakem $G(n)$ nejmenší číslo r, pro které všechna přirozená N až na konečný počet se dají psát ve tvaru (35).[14]) Existuje-li číslo $G(n)$, je tím současně řešen úkol I. Vzniká nyní problém, *jak určiti nebo aspoň odhadnouti číslo* $G(n)$.

III. Označme (při daných n, r, N) znakem $W(N) = W_{n,r}(N)$ počet řešení rovnice (35) v celých nezáporných číslech $x_1, \ldots, x_r$, t. j. počet vyjádření čísla N ve tvaru (35).

Klademe si za úkol, *nalézti přibližné vyjádření výrazu* $W_{n,r}(N)$ (při daných n, r) *pro velká* N. Zjistíme-li při tom, že (při daných n, r) je $W_{n,r}(N) > 0$ pro všechna dostatečně velká N, je tím zřejmě dokázána nerovnost $G(n) \leqq r$, t. j. je tím podán příspěvek k řešení problému II.

Je tedy patrno, že problém III zasahuje nejhlouběji, a začněme tedy tímto problémem. K jeho řešení použili na počátu dvacátých let *Hardy* a *Littlewood* s velkým úspěchem methody, kterou při jiném problému aditivní theorie čísel po prvé zavedli do matematiky *Hardy* a *Ramanujan* (vynikající indický matematik) r. 1914. Formální základ této methody převzal *Vinogradov*, ale v jejím provedení (a zde je ovšem hlavní obtíž) použil zcela nových myšlenek, které mu umožnily neobyčejné zlepšení dřívějších výsledků. Jen pro srovnání uvádím toto o problému II: *Hardy* a *Littlewood* dokázali, že

$$\limsup_{n\to\infty} \frac{G(n)}{n \cdot 2^{n-2}} \leqq 1; \tag{36}$$

Vinogradov naproti tomu již v r. 1934 dokázal, že

$$\limsup_{n\to\infty} \frac{G(n)}{n \log n} \leqq 6, \tag{37}$$

[13]) Viz můj referát o této knize v Časopise, roč. 67 (1937—8), str. D303—D306.

[14]) Místo „všechna přirozená N až na konečný počet" bychom mohli říci „všechna přirozená N vůbec"; tím bychom místo čísla $G(n)$ dostali číslo (po případě jiné) $g(n) \geqq G(n)$. Ale číslo $G(n)$, nepřihlížející k event. konečnému počtu „výjimečných" hodnot N, se jeví důležitějším.

a číslo 6 později ještě snížil. Naproti tomu lze na několika řádcích dokázati, že $G(n) > n$, a tedy

$$\liminf_{n\to\infty} \frac{G(n)}{n} \geqq 1. \tag{38}$$

Srovnání výsledků (36), (37) ukazuje, jak nesrovnatelně lepší je (pro velká n) odhad (37) než odhad (36), a srovnání (37), (38) ukazuje, jak blízko už je odhad (37) skutečné (dosud pro větší n neznámé) hodnotě $G(n)$.

Vraťme se však od problému II k problému III. Pokusím se vylíčiti v nejhrubších rysech, na čem spočívá methoda vyšetřování tohoto problému, při čemž se budu přidržovati postupu *Vinogradovova*. Buďte r, n daná přirozená čísla; ježto případ $n = 2$ je znám (problém II je na př. řešen rovnicí $G(2) = 4$),[15] budu stále předpokládati $n \geqq 3$. Užitečná nám bude tato samozřejmá poznámka: Je-li b celé číslo, je

$$\int_0^1 e^{2\pi i b\alpha}\, d\alpha = 0 \text{ pro } b \neq 0, \quad \int_0^1 e^{2\pi i b\alpha}\, d\alpha = 1 \text{ pro } b = 0. \tag{39}$$

Je-li x reálné číslo, označíme znakem $[x]$ největší celé číslo, jež není větší než x, takže na př. $[7] = 7$, $[7{,}3] = 7$. Dále položíme $\{x\} = x - [x]$ (t. zv. zbytek čísla x modulo 1), na př. $\{7\} = 0$, $\{7{,}3\} = 0{,}3$. Vždy je $0 \leqq \{x\} < 1$. Buďte nyní r, n daná přirozená čísla. Má-li se nějaké přirozené číslo N vyjádřit ve tvaru (35), musí býti $x_i^n \leqq N$, t. j. $x_i \leqq P$, kde zde i v dalším klademe

$$P = [N^{\frac{1}{n}}]. \tag{40}$$

Odtud je téměř ihned patrno, že platí toto: Položíme-li

$$L(\alpha) = \sum_{x=0}^{P} e^{2\pi i \alpha x^n}, \tag{41}$$

jest

$$W_{n,r}(N) = \int_0^1 L^r(\alpha)\, e^{-2\pi i \alpha N}\, d\alpha. \tag{42}$$

Neboť pravá strana je rovna součtu všech integrálů (pro zjednodušení píši $\exp x$ místo e^x)

$$\int_0^1 \exp(2\pi i(x_1^n + x_2^n + \ldots + x_r^n - N)\,\alpha)\, d\alpha, \tag{43}$$

kde $x_1, \ldots, x_r$ probíhají všechna čísla celá od 0 do P. Mezi integrály (43) je však podle (39) právě tolik jedniček, kolikrát je $x_1^n + \ldots + x_r^n - N = 0$, kdežto ostatní integrály jsou rovny nule. Podotkněme ještě, že integrand v (42) má periodu 1; můžeme proto místo integračních mezí 0, 1 vzít integrační meze a, $a + 1$ (a jakékoliv reálné číslo).

V součtu (41) je každý člen v absolutní hodnotě roven 1; tedy je $|L(\alpha)| \leqq P + 1$, a pro celistvé α je právě $L(\alpha) = P + 1$. Snadno bychom vypočetli $L(\frac{1}{2})$, $L(\frac{2}{3})$ a obecně $L\left(\frac{a}{q}\right)$ při daném racionálním $\alpha = \frac{a}{q}$ (a, q celá); ovšem pro velká q by výsledek byl nepřehledný a neměl by ceny. Ale přece nám tato poznámka ukazuje cestu: Dané číslo α se snažíme aproximovat zlomkem $\frac{a}{q}$ s nepříliš velkým q a očekáváme, že $L(\alpha)$ se dá přibližně nějak vyjádřit. K tomu cíli zvolíme číslo $\tau > 1$ (jak zvolíme toto

[15]) Problém III pro $n = 2$ řešil *Hardy*.

číslo, ukážeme za chvíli) a připomeneme tuto známou větu z theorie diofantických aproximací: Je-li $\tau > 1$, potom ke každému reálnému α existují celá čísla a, q tak, že je

$$0 < q \leqq \tau, \quad \left|\alpha - \frac{a}{q}\right| < \frac{1}{q\tau}, \quad [a, q] = 1.^{16}) \tag{44}$$

Lze tedy psáti $\alpha = \frac{a}{q} + z$, kde $|z| < \frac{1}{q\tau}$. Počítejme nyní součet $L\left(\frac{a}{q} + z\right)$. Sčítací index x ($x = 0, 1, 2, \ldots, P$) pišme ve tvaru $x = qt + s$, kde s probíhá čísla $0, 1, \ldots, q - 1$, a při pevném s probíhá t celá čísla, vyhovující podmínce

$$0 \leqq qt + s \leqq P, \text{ t. j. } -\frac{s}{q} \leqq t \leqq \frac{P - s}{q}. \tag{45}$$

Vzhledem k tomu, že funkce $\exp 2\pi i\alpha$ má periodu 1, máme

$$L\left(\frac{a}{q} + z\right) = \sum_{s=0}^{q-1} \sum_{t} \exp\left(2\pi i \frac{a}{q}(qt + s)^n + 2\pi i z(qt + s)^n\right) = \sum_{s=0}^{q-1} e^{2\pi i \frac{a}{q} s^n} . D_s(z), \tag{46}$$

kde

$$D_s(z) = \sum_{0 \leqq qt+s \leqq P} \exp(2\pi i z(qt + s)^n). \tag{47}$$

Abychom přibližně spočetli $D_s(z)$, připomeneme tuto větu VAN DER CORPUTOVU: Jestliže $m < m_1$ jsou celá čísla, a jestliže reálná funkce $f(t)$ v intervalu $\langle m, m_1\rangle$ vyhovuje nerovnostem $0 \leqq f'(x) \leqq \frac{1}{2}$, $f''(x) \geqq 0$, je

$$\sum_{t=m}^{m_1} \exp(2\pi i f(t)) = \int_{m}^{m_1} \exp(2\pi i f(t))\, dt + 2\Theta, \tag{48}$$

kde znakem Θ budeme zde i příště značiti čísla s absolutní hodnotou $\leqq 1$ (různá Θ nebudeme navzájem rozlišovati indexy).

Rovnice (48) platí ovšem i tehdy, když v ní místo f píšeme $-f$ (přechod k číslům komplexně sdruženým). Aplikujme tuto větu na $D_s(z)$, kladouce $f(t) = |z|(qt + s)^n$. Abychom mohli této věty užít, musí býti $f'(t) = qn|z|(qt + s)^{n-1} \leqq \frac{1}{2}$; ježto zde $|z|$ může nabývati všech hodnot $< \frac{1}{q\tau}$ a $qt + s$ všech hodnot až do P, dostáváme podmínku $qn \cdot \frac{1}{q\tau} P^{n-1} \leqq \frac{1}{2}$; nejmenší přípustná hodnota pro τ je tedy

$$\tau = 2nP^{n-1}. \tag{49}$$

Zvolme τ tímto způsobem. Užitím VAN DER CORPUTOVY věty dostáváme z (47) ihned (substitucí $qt + s = v$)

$$D_s(z) = \frac{1}{q}\psi(z) + 4\Theta, \text{ kde } \psi(z) = \int_0^P e^{2\pi i z v^n}\, dv, \tag{50}$$

načež z (46) plyne

$$L\left(\frac{a}{q} + z\right) = \psi(z)\frac{S_{a,q}}{q} + 4\Theta q, \text{ kde } S_{a,q} = \sum_{s=0}^{q-1} e^{2\pi i \frac{a}{q} s^n}. \tag{51}$$

---

[16]) Znakem $[a, q]$ značíme největšího společného dělitele.

První člen vpravo je součinem dvou činitelů: první z nich, $\psi(z)$, nemá nic společného s theorií čísel a nezávisí na a, q; druhý činitel zase má ráz vysloveně číselně theoretický, závisí na celých číslech a, q, ale nezávisí na z.

Zřejmě $|S_{a,q}| \leqq q$; ale dá se dokonce dokázati (což je rozhodující pro další úspěch), že

$$|S_{a,q}| \leqq cq^{1-\frac{1}{n}}, \tag{52}$$

kde číslo c závisí pouze na n, a nikoliv na a, q.[17]) Integrál $\psi(z)$ se bez obtíží odhadne, načež pro první člen v (51) dostaneme s pomocí (52) odhad

$$\left|\psi(z)\frac{S_{a,q}}{q}\right| < cq^{-\frac{1}{n}}\,\mathrm{Min}(P, |z|^{-\frac{1}{n}}). \tag{53}$$

Pro hodnoty $|z|$, blízké hodnotě $\frac{1}{q\tau}$ [18]) $\left(\text{na př. pro } \frac{1}{2q\tau} < |z| < \frac{1}{q\tau}\right)$ vychází odtud

$$\left|\psi(z)\frac{S_{a,q}}{q}\right| < c\tau^{\frac{1}{n}} = c_1 P^{1-\frac{1}{n}},$$

(viz (49)). Kdyby tedy bylo $q > P^{1-\frac{1}{n}}$, mohl by ve formuli (51) člen $4\Theta q$ (o němž nevíme nic více, než že je v absolutní hodnotě nejvýše roven $4q$) převládnouti řádově nad „hlavním" členem $\psi(z)\, S_{a,q} q^{-1}$, a vzorec (51) by asi neměl mnoho ceny. Budeme proto vzorce (51) v dalším užívati jen tehdy, je-li

$$0 < q \leqq P^{1-\frac{1}{n}}. \tag{54}$$

Učiňme nyní důsledky z toho, co jsme dosud řekli. Dána jsou přirozená čísla $n \geqq 3, r$.

Je-li N jakékoliv přirozené číslo, položme

$$P = [N^{\frac{1}{n}}],\ \tau = 2nP^{n-1}.$$ [19])

Ke každému reálnému α existují potom celá čísla a, q tak, že platí (44). Jinými slovy: Sestrojím-li ke každé dvojici čísel a, q s podmínkami

$$0 < q \leqq \tau,\ [a, q] = 1 \tag{55}$$

interval

$$I_{a,q} = \left(\frac{a}{q} - \frac{1}{q\tau}, \frac{a}{q} + \frac{1}{q\tau}\right), \tag{56}$$

potom tyto intervaly pokrývají celou číselnou osu.[20]) Speciálně $I_{0,1} = \left(-\frac{1}{\tau}, \frac{1}{\tau}\right)$, $I_{1,1} = \left(1 - \frac{1}{\tau}, 1 + \frac{1}{\tau}\right)$. Počet vyjádření čísla N ve tvaru (35) je dán vzorcem (42); abychom netrhali intervaly $I_{0,1}$, $I_{1,1}$ volme místo integračního intervalu $(0, 1)$ v (42) interval $\left(-\frac{1}{\tau}, 1 - \frac{1}{\tau}\right)$ (to smíme). Tento nový integrační interval je zřejmě obsažen ve sjednocení všech intervalů $I_{a,q}$, pro něž platí

$$0 \leqq a < q \leqq \tau,\ [a, q] = 1. \tag{57}$$

---

[17]) Znak $c, c_1, \ldots$ znamená až do konce vždy čísla, která závisí nejvýše jen na n a na r; různé hodnoty c často nerozlišuji.

[18]) Pamatujme, že $|z|$ může nabývati všech hodnot menších než $\frac{1}{q\tau}$.

[19]) Zajímat nás budou ovšem hlavně velké hodnoty N.

[20]) Ovšem: částečně se tyto intervaly překrývají.

Z těchto intervalů $I_{a,q}$ nazveme *základními* intervaly ty, pro něž platí

$$0 < q \leqq P^{1-\frac{1}{n}}. \tag{58}$$

Snadno se ukáže, že žádné dva základní intervaly nemají společných bodů. Označme znakem M množinu všech bodů, která zbude, když z intervalu $\left(-\frac{1}{\tau}, 1-\frac{1}{\tau}\right)$ odstraníme všechny základní intervaly. Rozdělím-li nyní integrační interval $\left(-\frac{1}{\tau}, 1-\frac{1}{\tau}\right)$, a označím znakem $H_{a,q}$ integrál funkce $L^r(\alpha)\,\mathrm{e}^{-2\pi i\alpha N}$ přes interval $I_{a,q}$, a znakem H'' integrál přes množinu M, dostávám z (42)

$$W_{n,r}(N) = H' + H'', \text{ kde } H' = \sum_{q=1}^{\left[P^{1-\frac{1}{n}}\right]} \sum_{a=0}^{q-1}{}' H_{a,q}. \tag{59}$$

Při tom Σ' značí, že se sčítá pouze přes čísla a nesoudělná s q. Předpokládejme v dalším $r \geqq 2n+1$ (proč, uvidíme za chvíli). Potom se ze vzorců (51), (53) snadno zjistí, že neuděláme příliš velkou chybu, vynecháme-li v (51) člen $4\Theta q$, takže pro $H_{a,q}$ máme v prvním přiblížení výraz[21])

$$\mathrm{e}^{-2\pi i N\frac{a}{q}} \left(\frac{S_{a,q}}{q}\right)^r \int_{-\frac{1}{q\tau}}^{\frac{1}{q\tau}} \psi^r(z)\,\mathrm{e}^{-2\pi i N z}\,\mathrm{d}z. \tag{60}$$

V tomto integrálu udělám zase jen „malou" chybu, jestliže v něm integruji od $-\infty$ do $+\infty$ $\left(\text{místo od } -\frac{1}{q\tau} \text{ do } \frac{1}{q\tau}\right)$, a tento integrál (závislý už jenom na N) má hodnotu (jak se zjistí po jistých obtížích čistě početního rázu)

$$\frac{\left(\Gamma\left(1+\frac{1}{n}\right)\right)^r}{\Gamma\left(\frac{r}{n}\right)} N^{\frac{r}{n}-1} + o\left(N^{\frac{r}{n}-1}\right), \tag{61}$$

při čemž znakem $o(f(N))$ značím jakoukoliv funkci, která je „nižšího řádu" než $f(N)$, t. j. jakoukoliv funkci $g(N)$, pro kterou je $\lim_{N\to+\infty} \frac{g(N)}{f(N)} = 0$. Dosadíme-li do (59) za $H_{a,q}$ přibližný výraz (60), při čemž za integrál dosadíme (61), a provedeme-li podrobně odhad chyby, které se při tom dopustíme, dostaneme z (59) snadno

$$W_{n,r}(N) = \frac{\left(\Gamma\left(1+\frac{1}{n}\right)\right)^r}{\Gamma\left(\frac{r}{n}\right)} N^{\frac{r}{n}-1} \sum_{q=1}^{\left[P^{1-\frac{1}{n}}\right]} A_q(N) + o\left(N^{\frac{r}{n}-1}\right) + H'', \tag{62}$$

kde

$$A_q(N) = \sum_{a=0}^{q-1}{}' \left(\frac{S_{a,q}}{q}\right)^r \mathrm{e}^{-2\pi i\frac{a}{q}N}. \tag{63}$$

---

[21]) Integrační proměnnou α lze v intervalu $I_{a,q}$ psáti ve tvaru $\frac{a}{q} + z$, kde z probíhá interval $\left(-\frac{1}{q\tau}, \frac{1}{q\tau}\right)$.

Položme

$$\mathbf{S}(N) = \mathbf{S}(N, r, n) = \sum_{q=1}^{\infty} A_q(N) \tag{64}$$

(z (51), (63) je vidět, že tato řada, které se říká „singulární řada", závisí pouze na N, n, r); v důsledku nerovnosti (52) a podmínky $r \geqq 2n + 1$ ihned zjistíme, že tato nekonečná řada má konvergentní „majorantu" nezávislou na N

$$c \sum_{q=1}^{\infty} q \,.\, q^{-\frac{r}{n}} \leqq c \sum_{q=1}^{\infty} q^{-1-\frac{1}{n}}.$$

Tedy je $\mathbf{S}(N, r, n) < c_1$, kde c_1 závisí (jak jsme se smluvili) jen na r, n, nikoliv na N. Jestliže tedy v (62) nahradíme konečný součet nekonečnou řadou, dopustíme se opět chyby řádu $o\left(N^{\frac{r}{n}-1}\right)$, takže celkem máme výsledek (pro $r \geqq 2n + 1$)

$$W_{n,r}(N) = \frac{\left(\Gamma\left(1 + \frac{1}{n}\right)\right)^r}{\Gamma\left(\frac{r}{n}\right)} N^{\frac{r}{n}-1} \mathbf{S}(N, r, n) + o\left(N^{\frac{r}{n}-1}\right) + H''. \tag{65}$$

Abychom pokročili dále, je nutno předpokládati $r \geqq 4n$. V tomto případě se totiž číselně theoretickými úvahami dá zjistit: existuje $c_2 > 0$ tak, že pro všechna N je

$$0 < c_2 < \mathbf{S}(N, r, n) < c_1 \text{ (pro } r \geqq 4n). \tag{66}$$

Je tedy vidět toto: *Jestliže dokážeme* (pro jistou dvojici čísel n, r ($r \geqq 4n \geqq 12$)), *že je také*

$$H'' = \int_M L^r(\alpha)\, \mathrm{e}^{-2\pi i \alpha N}\, \mathrm{d}\alpha = o\left(N^{\frac{r}{n}-1}\right), \tag{67}$$

potom lze v (65) vynechati H'' a vidíme, že pro tuto dvojici n, r je problém III vyřešen: První člen v (65) je kladný, je podle (66) *přesně* řádu $N^{\frac{r}{n}-1}$, a tedy pro velká N daleko převýší zbývající člen $o\left(N^{\frac{r}{n}-1}\right)$; odtud je speciálně vidět, že pro velká N je $W_{n,r}(N) > 0$, takže máme $G(n) \leqq r$, což je příspěvek k řešení problému II.

Zbývá tedy poslední a *hlavní* úkol: dokázati vztah (67). Jestliže až dosud bylo možno říci, že *Vinogradov* — přes mnohá zjednodušení a zlepšení — vycházel z *Hardyho* a *Littlewooda*, je jeho postup při důkazu vztahu (67) zcela původní a jeho methoda nesrovnatelně mocnější než methody jeho předchůdců. Jest ovšem

$$|H''| \leqq \int_M |L(\alpha)|^r\, \mathrm{d}\alpha. \tag{68}$$

Víme, že každý bod z M leží v některém z intervalů $I_{a,q}$ ($0 < q \leqq \tau = 2nP^{n-1}$). Víme dále, že M neobsahuje žádný bod ze „základních" intervalů $I_{a,q}$, t. j. těch, pro něž $q \leqq P^{1-\frac{1}{n}}$. Tedy: Každý bod $\alpha \in M$ leží v některém (aspoň v jednom) intervalu $I_{a,q}$, kde $P^{1-\frac{1}{n}} < q \leqq \tau$. Obšírně:

Ke každému α množiny M existují celá čísla a, q tak, že jest

$$[a, q] = 1, \quad \left|\alpha - \frac{a}{q}\right| < \frac{1}{q\tau} \leqq \frac{1}{q^2}, \tag{69}$$

při čemž

$$0 < a < q,\ P^{1-\frac{1}{n}} < q \leqq \tau = 2nP^{n-1}. \tag{70}$$

Hardy a *Littlewood* se opřeli o tuto důležitou větu *Weylovu* z r. 1921: Budiž $f(x) = \alpha x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ polynom s reálnými koeficienty. Buďte a, q čísla, pro něž je

$$[a, q] = 1,\ \left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}. \tag{71}$$

Budiž Q přirozené číslo. Potom pro každé $\varepsilon > 0$ platí

$$\left|\sum_{x=0}^{Q} \exp(2\pi i f(x))\right| < \mathrm{d}(n, \varepsilon)\, Q^{1+\varepsilon} q^{\varepsilon} \left(\frac{1}{Q} + \frac{1}{q} + \frac{q}{Q^n}\right)^{\frac{1}{2^{n-1}}}, \tag{72}$$

kde $\mathrm{d}(n, \varepsilon)$ je jisté číslo, závislé pouze na n, ε, tedy nezávislé na Q, a, q a na koeficientech $\alpha, \alpha_1, \ldots, \alpha_n$.

Dosadím-li sem $Q = P$, $f(x) = \alpha x^n$, kde α je nějaký bod z M, a vezmeme-li za a, q čísla s vlastnostmi (69), (70), vidíme, že pro každé $\alpha \in M$ je

$$|L(\alpha)| < d_1(n, \varepsilon)\, P^{1+\varepsilon+(n-1)\varepsilon} \left(P^{-1} + P^{-1+\frac{1}{n}} + P^{n-1-n}\right)^{\frac{1}{2^{n-1}}} < \\ < d_2(n, \varepsilon)\, P^{1+n\varepsilon} \cdot P^{\left(-1+\frac{1}{n}\right)\cdot 2^{-n+1}}. \tag{73}$$

Podstatné je zde ovšem to, že celkový exponent při P, t. j. $1 - \frac{n-1}{n} \cdot 2^{-n+1} + n\varepsilon$ je menší než 1, zvolíme-li ε dosti malé.

Ježto pro velká N je $P \sim N^{\frac{1}{n}}$, a ježto množina M má míru menší než 1, dostaneme užitím (73) z nerovnosti (68) ihned

$$|H''| < \mathrm{d}(n, r, \varepsilon)\, N^{\frac{r}{n} - r\frac{n-1}{n^2}\cdot 2^{-n+1} + \varepsilon r}. \tag{74}$$

Ježto ε můžeme voliti libovolně malé, je viděti toto: Zvolíme-li r tak velké, že $r \cdot \frac{n-1}{n^2} 2^{-n+1} > 1$, bude $H'' = o(N^{\frac{r}{n}-1})$, a náš problém bude vyřešen. Na př. stačí vzíti

$$r \geqq n \cdot 2^n, \tag{75}$$

načež bude vskutku

$$n \cdot 2^n \cdot \frac{n-1}{n^2} \cdot 2^{-n} \cdot 2 = 2\frac{n-1}{n} > 1.$$

Tím je tedy dokázáno, že v rovnici (65) lze vynechati H'', je-li $r \geqq n \cdot 2^n$; tím je tedy pro tyto hodnoty r rozřešen problém III a zároveň dokázána nerovnost $G(n) \leqq n \cdot 2^n$. Je vhodno poznamenati, že *Hardy* a *Littlewood* vhodnou úpravou důkazu ukázali, že místo (75) stačí slabší nerovnost

$$r \geqq (n-2)\, 2^{n-1} + 5, \tag{75a}$$

a že nerovnost pro $G(n)$ ještě nad to zostřili.

Na čem nyní spočívá *Vinogradovův* úspěch? Představme si, že bychom zjistili, že pro každé $\alpha \in M$ platí nerovnost tvaru

$$|L(\alpha)| < \mathrm{d}_3(n) \cdot P^{1-\lambda} \leqq \mathrm{d}_3(n)\, N^{\frac{1-\lambda}{n}}, \tag{76}$$

kde $d_3(n)$ a $\lambda > 0$ jsou čísla závislá jen na n (nezávislá na α a na P).[22]) Za druhé, že bychom zjistili, že pro jisté celé číslo $s > 0$ je

$$\int_0^1 |L(\alpha)|^{2s} \, \mathrm{d}\alpha < d_4(n, s) \, P^{2s-\mu}, \tag{77}$$

kde $\mu > 0$ stejně jako d_4 závisí jen na n, s. Kdybychom nyní položili $r = 2s + k$ (k celé kladné), dostali bychom z (68), (76)

$$|H''| \leqq d_3{}^k(n) \, N^{\frac{k-\lambda k}{n}} \int_M |L(\alpha)|^{2s} \, \mathrm{d}\alpha; \tag{78}$$

ježto pak M je částí intervalu (0, 1), dává (77) ihned

$$H'' = O\left(N^{\frac{k-\lambda k+2s-\mu}{n}}\right). \tag{79}$$

Ježto $k + 2s = r$, je exponent $\frac{r}{n} - \frac{\lambda k + \mu}{n}$; jestliže tedy $\lambda k + \mu > n$, t. j. $k > \frac{n-\mu}{\lambda}$, bude $H'' = o(N^{\frac{r}{n}-1})$. Tedy problém III bude řešen, jestliže

$$r > 2s + \frac{n-\mu}{\lambda}. \tag{80}$$

Je vidět, že tato nerovnost bude tím výhodnější, čím bude λ v (76) větší a dále, čím bude $2s - \frac{\mu}{\lambda}$ menší. Pro ilustraci uvedu jeden příklad. Vynikající čínský matematik *Hua* dokázal, že

$$\int_0^1 |L(\alpha)|^{2^n} \, \mathrm{d}\alpha < d_5(n, \varepsilon) \, P^{2^n - n + \varepsilon} \tag{81}$$

pro každé $\varepsilon > 0$. Položím-li tedy $r = 2^n + 1$,[23]) a použiji jakéhokoliv odhadu tvaru (76), kde $\lambda > 0$ (stačí na př. *Weylův* odhad (73)), obdržím ihned

$$H'' = O(P^{1-\lambda+2^n-n+\varepsilon}) = O\left(N^{\frac{r}{n}-1-\frac{\lambda-\varepsilon}{n}}\right) = o\left(N^{\frac{r}{n}-1}\right)$$

(zvolím-li $\varepsilon < \lambda$), takže podmínku (75a) lze nahraditi pro $n \geqq 4$ slabší (a tedy výhodnější) podmínkou

$$r \geqq 2^n + 1. \tag{81a}$$

Výkon *Vinogradovův* spočívá pak v tom, že si předně uvědomil důležitost vztahů tvaru (77) pro náš problém, a za druhé, že odvodil velmi ostré nerovnosti tvaru (76) a (77). Jako ilustraci uvedu aspoň toto: Ježto je zřejmě $|L(\alpha)| \leqq P + 1$, je celý smysl nerovnosti (76) skryt v čísle λ; mohli bychom říci, že číslo λ měří „účinnost" vzorce (76). *Weylova* formule (73) ukazuje, že za λ můžeme položiti kterékoliv číslo menší než $2\frac{n-1}{n} \cdot \frac{1}{2^n}$. Kdežto *Vinogradov* dokázal, že za λ můžeme (je-li $n \geqq 12$) položiti hodnotu

$$\lambda = \frac{1}{3n(n-1)\log(12n^2)}. \tag{82}$$

---

[22]) Tohoto druhu je na př. *Weylův* odhad (73).

[23]) T. j. $2s = 2^n$, $k = 1$.

Tedy pro velká n je *Vinogradovova* formule nesrovnatelně přesnější než *Weylova* (stačí srovnati řád funkce 2^n a funkce $n^2 \log n$). *Vinogradovovy* důležité výsledky o nerovnosti (77) nebudu ani uváděti — čtenář by si bez podrobného výkladu nemohl vytvořiti jasnou představu o jejich významu. Jen zase pro ilustraci uveďme toto: Dosadíme-li do (68) za $|L(\alpha)|$ podle (76) s hodnotou (82), obdržíme, že jest $H'' = o(N^{\frac{r}{n}-1})$, jakmile

$$\frac{r(1-\lambda)}{n} < \frac{r}{n} - 1, \text{ t. j. } r > \frac{n}{\lambda},$$

t. j. jakmile

$$r > 3n^2(n-1)\log(12n^2) \text{ (pro } n \geqq 12). \tag{83}$$

Pravá strana je pro velká n řádu $n^3 \log n$. Zde jsme nepoužili vůbec vzorce typu (77); s použitím tohoto vzorce dostal *Vinogradov* výhodnější nerovnost (s pravou stranou řádu $n^2 \log n$), jak za chvilku uvidíme (viz vzorec (86)). Toto zlepšení vzorce (86) proti (83) ukazuje význam vzorců typu (77).

Společným základem *Vinogradovových* důkazů nerovností (76), (77) je velmi elementární, ale při tom nesmírně duchaplný a obtížný odhad integrandu $|L(\alpha)|^{2s}$ ve vzorci (77). Je totiž zřejmě

$$|L(\alpha)|^{2s} = \sum_{x_1,\ldots,x_s=0}^{P} \sum_{y_1,\ldots,y_s=0}^{P} \exp(2\pi i\alpha(x_1^n + \ldots + x_s^n - y_1^n - \ldots - y_s^n)). \tag{84}$$

Výraz (84) je tedy součtem několika členů tvaru $\exp 2\pi i\alpha a_m$, kde a_m jsou celá čísla. Podle (39) je potom integrál v (77) roven součtu tolika jedniček, kolik z čísel a_m je rovno nule. Ale zjistit nebo aspoň odhadnout rozumným způsobem počet čísel a_m, rovných nule, se zde nezdařilo. Proto *Vinogradov* místo *rovnosti* (84) dokazuje vhodnou *nerovnost* podobného tvaru

$$|L(\alpha)|^{2s} \leqq \sum_{m=1}^{M} \exp(2\pi i\alpha b_m), \tag{85}$$

kde opět b_m jsou celá čísla. Integrujeme-li tuto nerovnost, obdržíme nerovnost

$$\int_0^1 |L(\alpha)|^{2s}\,d\alpha \leqq K,$$

kde K je počet oněch b_m, jež jsou rovna nule. Vtip je v tom, že *Vinogradov* sestrojil takovou nerovnost (85), ve které číslo K lze vhodně odhadnout. Konstrukce nerovnosti (85) je vlastně největším výkonem *Vinogradovovým* v tomto problému.[24]) Důkaz je obdivuhodným spojením jednoduché základní myšlenky s omračující technickou virtuositou. Podobná věta, ale o něco méně účinná, byla obsažena již v citované knize z r. 1937, a je zajímavo toto: ačkoliv se mnozí vynikající matematikové celého světa intensivně zabývali *Vinogradovovými* methodami a podali mnoho důležitých modifikací i aplikací, přece nehnuli s tímto ústředním bodem; a teprve *Vinogradovu* samotnému se podařilo (bylo to v době války) nahraditi svoji starší methodu dokonalejší methodou, jež je vyložena v této knize. Při veškeré své složitosti a duchaplnosti je tato methoda ryze „elementární"; používá vlastně jen známých nerovností

[24]) Je to vlastně lemma na str. 58—59; abych čtenáři usnadnil porozumění, uvádím místo tohoto lemmatu vlastně jeho jednu aplikaci, totiž myšlenkový pochod při důkazu jiného lemmatu (str. 73).

$$\left(\sum_{i=1}^{k} a_i b_i\right)^2 \leqq \sum_{i=1}^{k} a_i^2 \cdot \sum_{i=1}^{k} b_i^2; \quad \left(\sum_{i=1}^{k} a_i\right)^m \leqq k^{m-1} \sum_{i=1}^{k} a_i^m;$$

$$(a_1 a_2 \ldots a_k)^{\frac{1}{k}} \leqq \frac{1}{k}(a_1 + \ldots + a_k) \quad (a_i \geqq 0, b_i \geqq 0; m \text{ přirozené číslo}).$$

Tolik o nerovnosti (77). Pokud se týče nerovnosti (76), převádí *Vinogradov* tento problém vtipným obratem opět na nerovnost podobného typu jako je (77), pouze s n-rozměrným integrálem místo jednoduchého, takže může použíti v podstatě téže methody.

Po nalezení čísel λ, s, μ v (76), (77) je potom, jak jsme už viděli, problém III řešen, jestliže platí (80). Po dosazení příslušných hodnot dostává tak *Vinogradov* tento výsledek: *Je-li*

$$n \geqq 12, \quad r \geqq [10n^2 \log n],^{25}) \tag{86}$$

je $H'' = o(N^{\frac{r}{n}-1})$, *a tedy problém III je pro tyto hodnoty vyřešen.* Speciálně tedy máme

$$G(n) \leqq 10n^2 \log n \text{ pro } n \geqq 12. \tag{87}$$

Jestliže však se omezíme na problém II, t. j. na odhad čísla $G(n)$, můžeme jíti ještě dále. *Vinogradov* potom totiž nevyšetřuje *všechna* řešení $x_1, \ldots, x_r$ rovnice (35), nýbrž jenom některá, vyhovující vhodným podmínkám. Jestliže se ukáže, že při určitém r je počet těchto řešení pro všechna dosti velká N různý od nuly, plyne odtud $G(n) \leqq r$ (ježto neberu *všechna* řešení, vzdávám se tím ovšem řešení problému III). Methoda důkazu, velmi důmyslná a originální, je podstatně jednodušší než v problému III: obtížné problémy, týkající se nerovností (76), (77), jsou zde nahrazeny úvahami mnohem jednoduššími. Tímto způsobem už v knize z r. 1937 bylo dokázáno, že

$$G(n) < 6n(\log n + 1) \text{ pro } n \geqq 16 \tag{88}$$

(odtud plyne (37)), nyní pak *Vinogradov* dokazuje, že

$$G(n) < n(3 \log n + 11) \text{ pro } n \geqq 3 \tag{89}$$

(ale přiznám se, že jedno místo důkazu je mně dosud nejasné).

Tolik o *Waringovu* problému. Je patrno, jak velkou roli v něm hrají „trigonometrické" (nebo „exponenciální") součty

$$S(Q) = S(\alpha, \alpha_1, \ldots, \alpha_n, Q) = \sum_{x=0}^{Q} \exp(2\pi i f(x)), \tag{90}$$

kde

$$f(x) = \alpha x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n. \tag{91}$$

Pro $Q = P$, $f(x) = \alpha x^n$ přechází tento součet ve funkci $L(\alpha)$ (viz (41)). Ale tyto součty jsou důležité i v docela jiných otázkách. Vezměme jednu z nich, t. zv. *rovnoměrné rozdělení modulo 1.* Budiž dán polynom (91) a dvě čísla β, γ ($0 \leqq \beta < \gamma \leqq 1$). Čísla $\{f(0)\}, \{f(1)\}, \{f(2)\}, \ldots$, t. zv. zbytky čísel $f(0), f(1), f(2)$ modulo 1,[26]) leží v intervalu $\langle 0, 1)$. Pro libovolné přirozené Q označme znakem $N_{\beta,\gamma}(Q)$ počet oněch čísel Q-členné posloupnosti

$$\{f(0)\}, \{f(1)\}, \{f(2)\}, \ldots, \{f(Q)\}, \tag{92}$$

---

[25]) Dřívější výsledek, otištěný v knize z r. 1937, se liší od tohoto hlavně tím, že místo n^2 obsahuje n^3.

[26]) Zopakujme: $\{5\} = 0$, $\{5{,}1\} = 0{,}1$; $\{5{,}8\} = 0{,}8$; $\{6\} = 0$.

která leží v intervalu $\langle \beta, \gamma)$. Jestliže pro každou volbu čísel β, γ je

$$\lim_{Q \to +\infty} \frac{N_{\beta,\gamma}(Q)}{Q} = \gamma - \beta, \tag{93}$$

říkáme (z důvodů zřejmých), že posloupnost

$$f(0)\ f(1), f(2), f(3), \ldots \tag{94}$$

je rovnoměrně rozdělena modulo 1. Názorně se to dá říci také tak, že komplexní čísla

$$\exp(2\pi i\, f(x)) \quad (x = 0, 1, 2, \ldots)$$

jsou rovnoměrně rozdělena na jednotkové kružnici. Následkem toho — jak se snadno ukáže — platí pro každou rovnoměrně rozdělenou posloupnost (94) nejenom triviální odhad $|S(Q)| \leqq Q + 1$, nýbrž dokonce

$$S(Q) = o(Q).^{27}) \tag{95}$$

Z rovnoměrné rozdělenosti posloupnosti (94) plyne, jak je téměř ihned patrno, také rovnoměrná rozdělenost každé posloupnosti $m f(0), m f(1), \ldots$, kde m je libovolné přirozené číslo, a tedy podle (95) též

$$S_m(Q) = o(Q) \text{ pro } m = 1, 2, 3, \ldots, \tag{95a}$$

kde

$$S_m(Q) = \sum_{x=0}^{Q} \exp(2\pi i m\, f(x)). \tag{95b}$$

A nyní je důležité, že podmínky (95a) jsou nejenom nutné, nýbrž i postačující k tomu, aby posloupnost (94) byla rovnoměrně rozdělena. To dokázal r. 1916 *Weyl*, zakladatel systematické theorie rovnoměrného rozdělení.[28]) Dá se nyní očekávati, že každý odhad, který kvantitativně zostří rovnice (95a), dovolí také kvantitativně zostřit rovnici (93). Ježto pak *Vinogradov* našel velmi ostré odhady výrazů $S_m(Q)$ (jako vzorek jsme uvedli vzorec (76) s hodnotou (82)), dá se očekávati, že z těchto jeho odhadů vyplyne zostření rovnice (93). Vskutku našel *Vinogradov* na př. tuto větu (necituji ji ani v plné ostrosti ani v plné obecnosti): Budiž $f(x) = \alpha x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ polynom, $n \geqq 12$. Budiž Q přirozené číslo; buďte a, q celá nesoudělná čísla taková, že

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}, \quad 1 < q \leqq Q. \tag{96}$$

Potom pro libovolná β, γ $(0 \leqq \beta < \gamma \leqq 1)$ jest

$$\left|\frac{N_{\beta,\gamma}(Q)}{Q} - (\gamma - \beta)\right| < c q^{-\frac{1}{3(n-1)^2 \log 12n(n-1)}} \log Q.^{29}) \tag{96a}$$

Na př. jestliže je

$\alpha = \sqrt{d}$, $d > 0$ racionální, α iracionální,

---

[27]) Jednotliví členové tohoto součtu se vzhledem k rovnoměrnému rozdělení na jednotkové kružnici do značné míry vykompensují — to je velmi názorné.

[28]) Avšak první speciální výsledek v tomto směru náleží, tuším, *W. Sierpińskému.*

[29]) c zde závisí pouze na n, t. j. nezávisí na $\alpha, \alpha_1, \ldots, \alpha_n, a, q, Q$. Činitel $\log Q$ (který vadí ovšem jenom tehdy, když q je velmi malé v poměru ke Q) u *Vinogradova* není, ale patrně jde o nedopatření.

potom je známo, že existuje konstanta $0 < c(\alpha) < 1$ tak, že v každém intervalu $(c(\alpha)\, Q,\, Q)$ — je-li Q dosti velké — existuje číslo q a k němu příslušné a tak, že platí (96). Lze tedy vzíti q „téhož řádu" jako Q, a z (96a) je patrno, že pro všechna $Q > c_1(n, \alpha)$ je

$$\left| \frac{N_{\beta,\gamma}(Q)}{Q} - (\gamma - \beta) \right| < c_2(n, \alpha)\, Q^{-\frac{1}{3(n-1)^2 \log 12n(n-1)}} . \log Q.$$

Je patrno, že tato nerovnost dává informaci o tom, jak rychle levá strana konverguje k nule pro $Q \to +\infty$.

Ještě jeden problém vyšetřuje *Vinogradov*. Zabývali jsme se právě otázkou, jak jsou rozdělena čísla (92) v celém intervalu $\langle 0, 1)$. Jednodušší je problém, který se zabývá jen těmi čísly $\{f(x)\}$, která jsou blízko nule nebo jedničce, t. j. těmi hodnotami x, pro něž $f(x)$ je velmi blízko nějakému *celému* číslu y. Jde tedy o otázku, nalézti celé číslo $x > 0$ (a k němu příslušné celé y) tak, aby rozdíl $|f(x) - y|$ byl pokud možno malý.[30]) Uvedu jen jeden výsledek: Budiž $n > 4$, β reálné,

$$[a, q] = 1,\ q > 0,\ \left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}.$$

Potom existují celá x, y tak, že

$$|\alpha x^n - \beta - y| < c_1 q^{-\varrho},\ 0 < x < q^{\frac{2}{n}}, \tag{97}$$

při čemž c_1 závisí pouze na n, a ϱ je rovno

$$\varrho = \frac{1}{4n^2} \cdot \frac{\log n}{\log(n+1) \log(n \log n + n)}.$$

Odtud plyne zřejmě

$$|\alpha x^n - \beta - y| < c_1 x^{-\frac{1}{2} n\varrho}, \tag{98}$$

kde exponent $\frac{1}{2} n\varrho$ je pro velká n asymptoticky roven $\frac{1}{8n \log n}$.

Celkem se má tento problém (co do obtížnosti, co do methody i co do přesnosti výsledků) k problému rovnoměrného rozdělení asi tak, jako problém II k problému III ve *Waringově* problému. (Všimněte si na př., že se v (96a), (86) vpravo vyskytují výrazy řádu $n^2 \log n$, kdežto v (98), (89) výrazy řádu $n \log n$.) Ve vzorcích (76), (90), (97) a pod. byl $f(x)$ mnohočlen (někdy dokonce speciální, αx^n nebo $\alpha x^n - \beta$). Obdobné výsledky lze však odvoditi i pro obecnější funkce f.

Prozatím jsem vylíčil obsah prvních osmi kapitol *Vinogradovovy* knihy: Kap. I — pomocné věty; kap. II — „singulární řada" $\mathfrak{S}(N)$; kap. III — integrál H' v (59); kap. IV — vzorec (89); kap. V — vzorec (97) a pod.; kap. VI — odhady trigonometrických součtů $\sum_{x=0}^{Q} \exp(2\pi i f(x))$ a pod.; kap. VII — problém III; kap. VIII — rovnoměrné rozdělení modulo 1.

Vinogradovova kniha obsahuje ještě tři další kapitoly. V nich hlavní pozornost je věnována t. zv. *Goldbachovu* problému. Jde o domněnku, která vznikla r. 1742 z korespondence mezi *Goldbachem* a *Eulerem*:

I. *Každé sudé číslo $N > 4$ je součtem dvou lichých prvočísel.* Na př. $6 = 3 + 3$, $8 = 5 + 3$, $10 = 5 + 5 = 7 + 3 = 3 + 7$ atd. Ze správnosti této domněnky by plynula správnost další domněnky:

[30]) Lépe řečeno: jde o otázku, jak malým lze učiniti tento rozdíl, je-li předepsáno, že x nemá překročiti jistou hranici.

II. *Každé liché číslo $N > 7$ je součtem tří lichých prvočísel.* Vskutku: stačí použíti domněnky I na sudé číslo $N - 3 > 4$.

Ještě o něco slabší je domněnka:

III. *Každé liché číslo až na konečný počet výjimek je součtem tří lichých prvočísel.*[31])

A konečně ještě slabší domněnka:

IV. *Existuje přirozené číslo r tak, že každé celé číslo $N > 1$ je součtem nejvýše r prvočísel.*

V r. 1930 sovětský matematik *Šnirelman* dokázal domněnku IV. *Landau* nazval tuto jeho práci „jedním z největších pokroků v theorii čísel, které zažil". Ale již v r. 1923 se zabývali *Hardy* a *Littlewood* domněnkou III a dokázali: domněnka III je správná, jestliže nulové body *Dirichletových* L-funkcí $L(s, \chi)$ mají jistou (dosud nedokázanou) vlastnost. *Hardy* a *Littlewood* tedy prostě převedli domněnku III na jinou nedokázanou domněnku. Situace nevypadala nikterak nadějně, pokud se domněnky III týče. A proto vzbudila ohromný rozruch práce *Vinogradovova*, který r. 1937 domněnku III vskutku dokázal. Methoda *Hardy-Littlewoodova* i *Vinogradovova* vycházejí obě z podobných základů jako methoda k řešení *Waringova* problému, kterou jsem vyložil před chvílí. Mohu proto jistě nyní postupovati stručněji.

Budiž N libovolné celé kladné číslo; označme znakem $I(N)$ počet vyjádření čísla N ve tvaru

$$N = p_1 + p_2 + p_3 \quad (p_i \text{ lichá prvočísla}). \tag{99}$$

Položme

$$S(\alpha) = \sum_{3 \leqq p \leqq N} e^{2\pi i \alpha p}, \tag{100}$$

kde se sčítá přes všechna lichá prvočísla $p \leqq N$ (písmeno p bude stále značit prvočíslo). Potom je — podobně jako v (42)) —

$$I(N) = \int_0^1 S^3(\alpha)\, e^{-2\pi i \alpha N}\, d\alpha; \tag{101}$$

neboť integrál vpravo je součtem integrálů tvaru

$$\int_0^1 \exp(2\pi i \alpha (p_1 + p_2 + p_3 - N))\, d\alpha, \tag{102}$$

a podle (39) je tento integrál roven 1, platí-li (99), kdežto v ostatních případech je integrál (102) roven nule. Je vidět, že součet (100) je *formálně* jednodušší než (41), ježto místo x^n je v něm p^1, ale *zásadně* obtížnější, ježto se v něm sčítá přes *prvočísla* a ne přes celá čísla.

Postupujeme nyní podobně jako při *Waringově* problému, ale normování čísla τ a definice „základních intervalů" bude poněkud jiná — ježto se nesčítá přes celá čísla, nýbrž přes prvočísla. Pro jednoduchost položme $\log N = \varrho$. Všimněme si vzorců (5), (8) pro funkci $\pi(x, k, l)$ (to je počet prvočísel $p \equiv l \pmod k$), jež jsou $\leqq x$). Ježto funkce $e^{-\mu\sqrt{\log x}}$ ($\mu > 0$) konverguje k nule (pro $x \to +\infty$) zřejmě rychleji, než kterákoliv mocnina $\log^{-h} x = e^{-h \log\log x}$, je patrno toto (píši-li v (5), (7), (8) N, ϱ, q, a místo x, $\log x$, k, l):

[31]) Jinak řečeno: Existuje přirozené číslo N_0 tak, že každé liché číslo $N > N_0$ je součtem tří lichých prvočísel.

Jsou-li h, B jakákoliv (sebe větší) kladná čísla, potom pro

$$[a, q] = 1, \ 0 \leqq a < q \leqq \varrho^h \ ^{32}) \tag{103}$$

je

$$\pi(N, q, a) = \frac{1}{\varphi(q)} \int_2^N \frac{\mathrm{d}x}{\log x} + O\left(\frac{N}{q\varrho^B}\right); \tag{104}$$

při tom znak O značí funkci, jejíž absolutní hodnota je menší než $c(h, B)\, Nq^{-1}\varrho^{-B}$, kde $c(h, B) > 0$ *závisí pouze na* h, B. *V tomto smyslu budeme rozuměti symbolu* O *i v dalším.*

Zvolme nyní nějak pevně číslo $h > 4$, a položme $\tau = N\varrho^{-3h}$. *Základním intervalem* $I_{a,q}$ nazvu interval

$$I_{a,q} = \left(\frac{a}{q} - \frac{1}{\tau}, \ \frac{a}{q} + \frac{1}{\tau}\right), \tag{105}$$

jestliže

$$[a, q] = 1, \ 0 < q \leqq \varrho^{3h} \tag{106}$$

(ve *Waringově* problému jsme měli $\frac{1}{q\tau}$ místo $\frac{1}{\tau}$ — na tom činiteli q zde mnoho nezáleží, ježto q podle (106) je poměrně malé). Volme v (101) opět integrační interval $(-\frac{1}{\tau}, 1 - \frac{1}{\tau})$ místo $(0, 1)$ a označme znakem M množinu, která zbude, když z integračního intervalu odstraníme základní intervaly. Ke každému $\alpha \in M$ existuje tedy dvojice celých nesoudělných čísel a, q tak, že

$$0 < a < q, \ \varrho^{3h} < q \leqq \tau, \ \left|\alpha - \frac{a}{q}\right| < \frac{1}{q\tau} \leqq \frac{1}{q^2}. \tag{107}$$

Rozdělím opět integrál (101) na dva díly (stejně jako v (59))

$$I(N) = H' + H'', \ H' = \sum_{q=1}^{[\varrho^{3h}]} \sum_{a=0}^{q-1}{}' H_{a,q}, \tag{108}$$

kde $H_{a,q}$ je integrál přes interval $I_{a,q}$, H'' je integrál přes množinu M. Všimněme si napřed integrálu přes M. Zde leží hlavní zásluha *Vinogradovova*: Podařilo se mu pro $\alpha \in M$ dokázati nerovnost obdobnou nerovnosti (76), což byla věc zásadně nová, ježto teď se sčítá přes *prvočísla*. Nám stačí tento tvar jeho věty: Je-li $\alpha \in M$, je

$$S(\alpha) = O(N\varrho^{2-h}). \tag{109}$$

Nyní už snadno odhadneme H'':

$$|H''| \leqq \int_M |S(\alpha)|^3 \, \mathrm{d}\alpha \leqq c(h, B)\, N\varrho^{2-h} \int_0^1 |S(\alpha)|^2 \, \mathrm{d}\alpha =$$

$$= c(h, B)\, N\varrho^{2-h} \sum_{3 \leqq p_1, p_2 \leqq N} \int_0^1 \mathrm{e}^{2\pi \mathrm{i}\alpha(p_1 - p_2)} \, \mathrm{d}\alpha;$$

ale poslední integrál je roven 1 pro $p_1 = p_2$, jinak je roven nule. Poslední součet je tedy roven prostě $\pi(N) - 1 = O(N\varrho^{-1})$ (prvočíslo 2 nepočítáme), takže

$$H'' = O(N^2\varrho^{1-h}). \tag{109*}$$

---

^{32}) Zde je jedno, píši-li $0 \leqq a < q$ nebo $0 < a \leqq q$; neboť $a = 0$ a $a = q$ je přípustno jen pro $q = 1$.

Vidíme, že zde odpadají obtíže s integrály typu (77) — to je proto, že zde máme $n = 1$.

Naznačme teď, jak se vypočte $H_{a,q}$. Musíme vypočísti $S(\alpha)$, když α leží v $I_{a,q}$, t. j. když α má tvar

$$\alpha = \frac{a}{q} + z, \quad |z| < \frac{1}{\tau}, \quad 0 \leqq a < q \leqq \varrho^{3h}, \quad [a, q] = 1. \tag{110}$$

Sumační interval $(2, N\rangle$[33]) rozdělme na intervaly

$$(M_0, M_1\rangle, (M_1, M_2\rangle, \ldots, (M_{k-1}, M_k\rangle,$$

kde

$$M_0 = 2, \quad M_k = N, \quad M_{i+1} - M_i = N\varrho^{-9h}$$

(poslední interval může býti kratší). Počet těchto intervalů je řádově roven ϱ^{9h}. Budiž j libovolné z čísel $0, 1, \ldots, q - 1$, nesoudělné s q, a označme

$$S_{i,j}(\alpha) = \sum_p e^{2\pi i x p}, \tag{111}$$

kde se sčítá přes ona prvočísla p intervalu $M_{i-1} < p \leqq M_i$, která leží v posloupnosti $j, j + q, j + 2q, \ldots$ Je zřejmo, že

$$S(\alpha) = \sum_{j=0}^{q-1}{}' \sum_{i=1}^{k} S_{i,j}(\alpha) + R, \tag{112}$$

kde R je součet těch členů $\exp(2\pi i \alpha p)$, kde p není nesoudělno s q, t. j. kde p je obsaženo v q, takže jistě $p \leqq q$; tedy

$$|R| \leqq q \leqq \varrho^{3h}. \tag{113}$$

Počítejme nyní

$$S_{i,j}(\alpha) = \sum_p e^{2\pi i \alpha p} = \sum_p e^{2\pi i \frac{a}{q} p} \cdot e^{2\pi i z p}. \tag{114}$$

Zde $p = j + mq$ (q celé), a tedy $\exp\left(2\pi i \frac{a}{q} p\right) = \exp\left(2\pi i \frac{a}{q} j\right)$. Tedy

$$S_{i,j}(\alpha) = e^{2\pi i \frac{a}{q} j} \sum_p e^{2\pi i z p}. \tag{115}$$

Počet členů v posledním součtu je zřejmě roven $\pi(M_i, q, j) - \pi(M_{i-1}, q, j)$, a to je podle (104) přibližně rovno

$$\frac{1}{\varphi(q)} \int_{M_{i-1}}^{M_i} \frac{dx}{\log x},$$

při čemž výraz s O je zanedbatelný (jak se zjistí z toho, že B lze voliti jakkoliv velké). Dále: p leží mezi M_{i-1} a M_i, takže

$$|zp - zM_i| \leqq \frac{1}{\tau} |M_i - M_{i-1}| \leqq \frac{N}{\tau \varrho^{9h}} = \frac{1}{\varrho^{6h}}. \tag{116}$$

Ježto tento výraz je velmi malý, můžeme v prvním přiblížení v (115) všechna čísla $\exp(2\pi i z p)$ nahraditi jediným číslem $\exp(2\pi i z M_i)$, takže v prvním přiblížení je $S_{i,j}(\alpha)$ rovno

[33]) Sčítá se přes $p \geqq 3$, t. j. přes $p > 2$.

$$\frac{1}{\varphi(q)}\, e^{2\pi i \frac{a}{q} j} \int_{M_{i-1}}^{M_i} e^{2\pi i z M_i}\, \frac{dx}{\log x}. \tag{117}$$

Schválně jsem konstantní výraz $\exp(2\pi i z M_i)$ dal za znamení integrační. Neboť integrační proměnná x opět leží mezi M_{i-1}, M_i, takže stejně jako v (116) plyne $|zM_i - zx| \leqq \varrho^{-6h}$, a zase bez velké újmy na přesnosti mohu místo zM_i psáti zx, takže pro $S_{i,j}(\alpha)$ dostanu přibližně hodnotu

$$\frac{1}{\varphi(q)}\, e^{2\pi i \frac{a}{q} j} \int_{M_{i-1}}^{M_i} e^{2\pi i z x}\, \frac{dx}{\log x}. \tag{118}$$

Sečtením přes $i = 1, \ldots, k$ dostanu pro $\sum_{i=1}^{k} S_{i,j}(\alpha)$ přibližný výraz

$$\frac{1}{\varphi(q)}\, e^{2\pi i \frac{a}{q} j}\, \psi(z), \text{ kde } \psi(z) = \int_{2}^{N} e^{2\pi i z x}\, \frac{dx}{\log x}. \tag{119}$$

Při tom $\psi(z)$ nezávisí na a, q, j, kdežto první činitel zase nezávisí na N, z. Ještě máme sčítati výraz (119) přes j. Známá elementární věta z algebry praví, že

$$\sum_{j=0}^{q-1}{}' e^{2\pi i \frac{a}{q} j} = \mu(q) \text{ (pro } [a, q] = 1), \tag{120}$$

kde $\mu(q)$ je *Möbiova* funkce takto definovaná: $\mu(1) = 1$; je-li q součinem s *různých* prvočísel, je $\mu(q) = (-1)^s$; je-li však q dělitelno druhou mocninou nějakého prvočísla, je $\mu(q) = 0$. Sečtením v (119) podle j dostanu (viz (112); zbytek R neruší vzhledem k (113)) pro $S(\alpha)$ přibližné vyjádření

$$\frac{\mu(q)}{\varphi(q)}\, \psi(z). \tag{121}$$

Umocním-li na třetí, násobím $\exp\left(-2\pi i \left(\frac{a}{q} + z\right) N\right)$ a integruji, dostávám přibližné vyjádření pro $H_{a,q}$ (ježto $\mu^3(q) = \mu(q)$):

$$\frac{\mu(q)}{\varphi^3(q)}\, e^{-2\pi i \frac{a}{q} N}\, \Phi(z), \quad \Phi(z) = \int_{-\frac{1}{\tau}}^{\frac{1}{\tau}} \psi^3(z)\, e^{-2\pi i z N}\, dz. \tag{122}$$

Pro integrál $\Phi(z)$ dostanu bez velkých obtíží přibližnou hodnotu $\frac{1}{2} N^2 \varrho^{-3}$.

Dosadím-li za $H_{a,q}$ do (108) hodnotu (122) a za H'' odhad (109*) a vyšetřím chybu, které se tím dopustím, dostanu celkem

$$I(N) = \sum_{q=1}^{[\varrho^{3h}]} \frac{\mu(q)}{\varphi^3(q)} \cdot \sum_{a=0}^{q-1}{}' e^{-2\pi i \frac{a}{q} N} \cdot \tfrac{1}{2} N^2 \varrho^{-3} + o(N^2 \varrho^{-3}). \tag{123}$$

Zavedu-li do (123) místo konečného součtu nekonečnou řadu

$$\mathfrak{S}_1(N) = \sum_{q=1}^{\infty} \frac{\mu(q)}{\varphi^3(q)} \cdot \sum_{a=0}^{q-1}{}' e^{-2\pi i \frac{a}{q} N} \tag{123*}$$

(jejíž konvergence se snadno dokáže), obdrží se ihned

$$I(N) = \tfrac{1}{2} \frac{N}{\log^3 N} \mathfrak{S}_1(N) + o\left(\frac{N}{\log^3 N}\right). \tag{124}$$

Součet řady $\mathfrak{S}_1(N)$ se dokonce snadno vypočte; jest

$$\mathfrak{S}_1(N) = \prod_p \left(1 + \frac{1}{(p-1)^3}\right) \cdot \prod_p{}'' \left(1 - \frac{1}{p^2 - 3p + 3}\right), \tag{125}$$

kde první součin se vztahuje na všechna prvočísla p, druhý pak na ona prvočísla p, jež jsou děliteli čísla N. Odtud je ihned patrno, že pro všechna *lichá* N leží $\mathfrak{S}_1(N)$ mezi dvěma pevnými kladnými čísly; je totiž

$$\tfrac{1}{2} < \mathfrak{S}_1(N) \leqq \prod_p \left(1 + \frac{1}{(p-1)^3}\right).^{34})$$

Odtud je vidět: Je-li N liché a dostatečně veliké, převáží v (124) vpravo první člen nad druhým, a tedy je $I(N) > 0$. Tím je dokázána domněnka III. Současně dává (124) přibližné vyjádření $I(N)$ pro velká N.

Teď musím však poprositi čtenáře za prominutí: Pro větší přehlednost jsem o důkazu domněnky III referoval podle knihy z r. 1937, kde se *Vinogradov* opíral o odhad (8), plynoucí ze *Siegelovy* nerovnosti (34). V knize z r. 1947 užívá *Vinogradov* pouze výsledků *Pageových*. To vede k malé formální komplikaci, kterou jsem chtěl čtenáři ušetřit. Avšak současně má vyloučení věty *Siegelovy* z důkazu jeden důležitý důsledek. Viděli jsme, že *Siegelova* věta je čistě existenční (nedovoluje numerické odhady), kdežto věty *Pageovy* mohou býti sledovány až k numerickému výpočtu. Lze tedy touto methodou stanoviti vskutku číslo N_0 takové, že každé liché číslo $N > N_0$ je součtem tří lichých prvočísel. Stačí potom prověřiti všechna lichá čísla od 9 do N_0, abychom zjistili, zda je správná také domněnka II. Jeden z žáků *Vinogradovových* vskutku takové N_0 našel; vyšla však hodnota tak velká, že prověření všech čísel až do N_0 se ukázalo prakticky nemožným. Domněnka I pak dosud vzdoruje všem pokusům o důkaz.

V kapitole XI podává *Vinogradov* důkaz věty o rovnoměrném rozdělení čísel

$$2\alpha,\ 3\alpha,\ 5\alpha,\ \ldots,\ p\alpha,\ \ldots$$

modulo 1. Jde tedy o rozložení čísel $\{p\alpha\}$ (kde p probíhá všechna prvočísla) v intervalu $\langle 0, 1)$. Proti problémům dříve projednávaným (posloupnost (94)) je zde *formální* zjednodušení v tom, že jde o polynom 1. stupně αx, ale *podstatné* ztížení v tom, že x místo všech přirozených čísel probíhá pouze prvočísla. Výsledek nebudu uváděti.

---

[34]) Pro *sudé* N je $\mathfrak{S}_1(N) = 0$, ježto v druhém součinu v (125) je člen $1 - \frac{1}{2^2 - 3 \cdot 2 + 3} = 0$.

Podotýkám, že jsem neuváděl výsledky ani v plné obecnosti, ani v plné ostrosti; tak na př. odhad $o(N^{\frac{r}{n}-1})$ v (67) lze vždy nahraditi ostřejším odhadem $O(N^{\frac{r}{n}-1-\delta})$, kde δ je jisté kladné číslo, závislé pouze na r, n. Podobně je tomu v mnoha jiných uvedených výsledcích.

Požadavky na *znalosti* čtenáře, které klade kniha *Vinogradovova*, jsou velmi mírné. Požadují se vskutku pouze běžné znalosti integrálního počtu (asi v rozsahu prvního dvouletí na našich universitách). Jedině věty o $\pi(x, k, l)$ (rozdělení prvočísel v aritmetických posloupnostech) se uvádějí bez důkazu. Ale tuto mezeru[35]) si může čtenář vyplniti právě z knihy *Čudakovovy*.

Ovšem na schopnosti matematického myšlení (a především myšlení funkčního a na živý cit pro poměrnou závažnost různých funkcí při kvantitativních odhadech) klade kniha značné nároky. *Vinogradov* často neprobírá explicitně triviální odhady a soustředí se na hlavní věci. Domnívám se, že je to v této tak složité látce správný postup: podrobné probírání všech detailů by úplně setřelo čtenáři rozdíl mezi hlavním a vedlejším: čtenář by poznal, že všechno je správné, ale nevěděl by, jak na to někdo mohl přijít. Ovšem skrývá tento způsob jisté nebezpečí, a to i pro autora: že si totiž drobnost, kterou přenechal k úvaze čtenáři, sám podrobně nepromyslil. A tak proklouzlo i velkému *Vinogradovovi* v této knize několik nedopatření, z nichž některá mají vliv (na štěstí ne podstatný) i na výsledky. Na př. v důkazu věty 1 na str. 63 se hned z počátku vynechává člen řádu $P^{1-\varrho}$; nemůže tedy (na př. pro $m = 1$) tento důkaz dávati výsledek $S \ll P^{1-\varrho t}$, kde $t > 1$. Toto nedopatření pak má vliv v kap. VIII. Tiskové chyby se v knize vyskytují, ale není jich nijak nadměrně mnoho. Ale to jsou vše výhrady spíše formální, týkající se obtíží čtenáře při studiu této knihy. Neobyčejná závažnost method i výsledků a výrazný způsob podání (za zmínku stojí i zajímavá a poučná předmluva) činí z této knihy snad nejdůležitější knižní publikaci z oboru theorie čísel v posledních 10 letech.

III. *Хуа Ло-Кен:* **Аддитивная теорня простых чисел** (*Loo-Keng Hua: Additivní theorie prvočísel*). Vydavatelstvo Akademie Nauk SSSR, Moskva-Leningrad 1947. Práce matematického institutu V. A. Stěklova XXII. Str. 179, tiráž 2000, cena 13 r.

Předem podotýkám, že rukopis této knihy byl napsán již r. 1941; jeho vydání se zpozdilo v důsledku války. Proto se tato kniha opírá o starší methody *Vinogradovovy* a ne o jeho poslední methodu, vzniklou až v r. 1942. Užitím této novější methody by se automaticky zlepšily některé její výsledky. Ježto jsem čtenáře již obšírně uvedl do problematiky otázek, jež se zde řeší, mohu zde jistě postupovat stručněji.

Kniha se skládá z 12 kapitol a dodatku; prvních devět je věnováno t. zv. *Waring-Goldbachovu* problému. *Waringův* problém jednal o vyjádření čísla N ve tvaru

$$N = x_1^n + x_2^n + \ldots + x_r^n \quad (x_i \geqq 0 \text{ celá}).$$

Nyní budeme nadto požadovati, aby x_i byla prvočísla (takže pro $n = 1$, $r = 3$ by problém přešel v *Goldbachův* problém ve tvaru II nebo III). Ale ještě obecněji místo x^n vezmu libovolný polynom

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n \quad (a_0 > 0), \tag{126}$$

který pro celá x nabývá celých hodnot (tuto vlastnost má každý polynom s celými koeficienty, ale také na př. polynom $\frac{1}{2}x^2 + \frac{1}{2}x = \frac{1}{2}x(x+1)$). Ptáme se pak po počtu vyjádření čísla N ve tvaru

$$N = f(p_1) + f(p_2) + \ldots + f(p_r) \quad (p_i \text{ prvočísla}). \tag{127}$$

[35]) Jejímž vyplněním by se rozsah knihy zdvojnásobil.

Počet těchto vyjádření označme opět $W(N)$ (závisí na N, na r a na polynomu f). Je vidět, že se zde kombinují obtíže problému *Waringova* (n-té mocniny) i *Goldbachova* (jde o prvočísla), a k tomu ještě to, že nejde o speciální polynom x^n, nýbrž o obecný polynom $f(x)$. Položme

$$\mathbf{T}(\alpha) = \sum_{p \leqq P} \exp(2\pi i \alpha f(p)), \quad P = [N^{\frac{1}{n}}]. \tag{128}$$

(Sčítá se přes prvočísla.) Potom analogicky jako v (42) je

$$W(N) = \int_0^1 \mathbf{T}^r(\alpha)\, e^{-2\pi i N \alpha}\, d\alpha. \tag{129}$$

Zvolíme opět vhodné τ, označíme znakem $I_{a,q}$ interval

$$I_{a,q} = \left(\frac{a}{q} - \frac{1}{q\tau}, \frac{a}{q} + \frac{1}{q\tau}\right), \tag{130}$$

a rozdělíme integrál v (129) na dva integrály:

$$W(N) = H' + H'', \tag{131}$$

kde H' je součet integrálů přes „základní" intervaly $I_{a,q}$ (s „malými" hodnotami q — viz příslušné omezení pro q v (54) pro *Waringův* a v (106) pro *Goldbachův* problém), H'' je pak integrál přes zbytek M intervalu (0, 1). Opět se propočtou integrály přes základní intervaly — a tím integrál H' — kdežto H'' se pouze odhadne.

K odhadu H'' se jednak musí odhadnout $\mathbf{T}(\alpha)$ pro $\alpha \in M$ (to je těžký problém: jde o polynom n-tého stupně, a současně se sčítá přes prvočísla), kterýžto odhad provedl *Vinogradov* (a je v knize *Huově* vyložen v kap. VI). Ale protože tento odhad je málo přesný (jde o obtížný problém sčítání přes *prvočísla*), musí se opět sáhnout (podobně jako v (77)) k integrálům tvaru

$$\int_0^1 |\mathbf{T}(\alpha)|^{2s}\, d\alpha.^{36}) \tag{132}$$

Štěstí je, že u tohoto integrálu už nevadí, že se sčítá jen přes prvočísla. Neboť tento integrál je zřejmě roven součtu všech integrálů tvaru

$$\int_0^1 \exp(2\pi i \alpha (f(p_1) + \ldots + f(p_s) - f(p_{s+1}) - \ldots - f(p_{2s}))\, d\alpha,$$

čili (podle (39)): (132) se rovná počtu řešení rovnice

$$f(p_1) + \ldots + f(p_s) - f(p_{s+1}) - \ldots - f(p_{2s}) = 0, \tag{133}$$

kde p_i probíhají prvočísla $\leqq P$. A zcela podobně: píši-li

$$T(\alpha) = \sum_{x=0}^{P} \exp(2\pi i \alpha f(x)), \tag{134}$$

je

$$\int_0^1 |T(\alpha)|^{2s}\, d\alpha \tag{135}$$

roven počtu řešení rovnice (133), kde však nyní p_i probíhají nejenom prvočísla, nýbrž

---

[36]) Při *Goldbachově* problému jsme tento integrál (tam bylo $s = 1$, $n = 1$) „náhodou" snadno vypočetli (viz výpočet před formulí (109*).

všechna celá nezáporná čísla $\leqq P$, takže (135) je aspoň tak velký jako (132), a místo (132) můžeme odhadovati (135), kde už o žádná prvočísla nejde. Tento integrál se tedy odhaduje methodami, jimiž se vyšetřuje integrál (77) ve *Waringově* problému. Jakási zajímavá komplikace vzniká ještě z toho, že definice čísla τ a definice základních intervalů, která se hodí pro problémy s prvočísly (zde tedy pro odhad $\boldsymbol{T}(\alpha)$) je jiná než ta, která se hodí pro problémy s libovolnými celými čísly (zde tedy pro odhad integrálu (135)); srovnej na př. (54) (*Waringův* problém) a (106) (*Goldbachův* problém), kde horní hranice pro číslo q, příslušné základním intervalům, se podstatně liší (jednou $P^{1-\frac{1}{n}}$, po druhé ϱ^{3h}, t. j. řádově $\log^{3h}P$). Ale nakonec všechno dobře dopadne, a dostaneme, že platí: Je-li buďto

$$n \geqq 1, \; r \geqq 2^n + 1 \; ^{37}) \tag{136}$$

nebo

$$n \geqq 14, \; r \geqq n^3(\log n + 2{,}2 \log\log n),^{38}) \tag{137}$$

je (viz (129))

$$W(N) = a_0^{-\frac{r}{n}} \frac{\Gamma^r\left(\frac{1}{n}\right)}{\Gamma\left(\frac{r}{n}\right)} \mathbf{S}(N) \frac{N^{\frac{r}{n}-1}}{\log^r N} + o\left(\frac{N^{\frac{r}{n}-1}}{\log^r N}\right), \tag{138}$$

kde $\mathbf{S}(N)$ je opět jistá „singulární řada" podobného typu jako (64). Ale po cestě k tomuto výsledku potkáme ještě několik obtíží. O jedné z nich se zmíním. Ve *Waringově* problému jsme se setkali s výrazem $S_{a,q}$ (viz (51)), pro nějž jsme potřebovali odhad (52). O něco obecněji se vyskytne zde

$$S(q, f) = \sum_{x=1}^{q} \exp\left(2\pi i \frac{f(x)}{q}\right),^{39})$$

kde $f(x)$ je polynom $a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x$ s celými koeficienty, při čemž největší společný dělitel $[a_0, a_1, \ldots, a_{n-1}, q] = 1$. Pro tento součet dokazuje *Hua* v kap. I odhad analogický k (52): Ke každému $\varepsilon > 0$ existuje $c(n, \varepsilon)$ tak, že

$$|S(q, f)| < c(n, \varepsilon)\, q^{1-\frac{1}{n}+\varepsilon};$$

je-li $q = p^m$, lze dokonce klásti $\varepsilon = 0$. Pro $q = p$ dokázal tuto větu *Mordell*, přechod k případu $q = p^m$ provedl *Hua*, načež přechod k obecnému q už je snadný. Je zajímavé, že důkaz případu $q = p$ i přechod od $q = p$ k $q = p^m$ jsou dosti obtížné a vypadají zcela jinak než ve speciálním případě součtu $S_{a,q}$.

Jiný takový pomocný problém je odhad součtu (kap. II)

$$\sum_{\substack{x_1, \ldots, x_m = 1 \\ F(x_1, \ldots, x_m) \neq 0}}^{P} d^k(|F(x_1, \ldots, x_m)|),$$

kde F je polynom v m proměnných s celistvými koeficienty, $d(a)$ pak značí počet dělitelů čísla a.

---

37) Toto odpovídá *Huově* formuli (81a).

38) S použitím novější *Vinogradovovy* methody by se vystačilo s nerovností $r \geqq 10n^2 \log n$.

39) $S_{a,q}$ ze vzorce (51) dostaneme pro $f(x) = ax^n$.

Ale formulí (138) není ještě vše hotovo. Dá se snadno dokázat, že $\mathbf{S}(N) < b_1$, kde b_1 je číslo nezávislé na N. Ale kdyby pro některá N bylo $\mathbf{S}(N)$ buďto rovno nule nebo velmi blízké nule, potom by vzorec (138) říkal jenom, že $W(N)$ je „nižšího řádu" než $N^{\frac{r}{n}-1} \log^{-r} N$, ale první člen v (138) by ztrácel význam hlavního členu, ba ani by nebylo patrno, zda je $W(N) > 0$ pro všechna velká N. Je tedy záhodno, dokázati nerovnost tvaru

$$\mathbf{S}(N) > b_2, \tag{139}$$

kde b_2 je kladné číslo, nezávislé na N. To provádí *Hua* v kap. VIII, ale jen pro speciální polynom $f(x) = x^n$, t. j. pro vyjádření

$$N = p_1^n + \ldots + p_r^n \tag{140}$$

a dostává vskutku nerovnost (139), ale pouze pro taková N, která vyhovují kongruenci

$$N \equiv r \pmod{K}, \tag{141}$$

kde K je jisté číslo závislé jen na n. (Podrobně: Vezměme všechna prvočísla p, pro něž n je dělitelno číslem $p - 1$. U každého z těchto p stanovme nejvyšší mocninu p^γ, která je dělitelem čísla n — může býti ovšem též $\gamma = 0$. Potom položím $\Theta = \gamma + 1$, s jedinou výjimkou: je-li $p = 2$, n sudé, kladu $\Theta = \gamma + 2$. Potom K je součinem všech těchto čísel p^Θ. Užitím *Fermatovy* věty se snadno ukáže: Je-li p_i prvočíslo, a není-li p_i dělitelem čísla K, potom je $p_i^n \equiv 1 \pmod{K}$. Jestliže tedy žádné p_i v rovnici (140) není dělitelem čísla K, potom nutně platí (141). Tedy: Chci-li nějaké číslo N, *nevyhovující* kongruenci (141), vyjádřiti ve tvaru (140), musím aspoň jedno p_i voliti *zcela speciálně*, totiž mezi prvočiniteli čísla K. Lze proto očekávati, a dalo by se asi snadno dokázat, že pro čísla N, *nevyhovující* kongruenci (141), je počet řešení $W(N)$ nižšího řádu než $N^{\frac{r}{n}-1} \log^{-r} N$, a že pro takováto N asi $\mathbf{S}(N)$ konverguje k nule pro $N \to +\infty$.)

Tím je tedy řešen *Waring-Goldbachův* problém pro $f(x) = x^n$ a pro r, vyhovující buďto nerovnosti (136) nebo (137). Z (138), (139) plyne speciálně $W(N) > 0$ pro všechna dostatečně velká N, vyhovující kongruenci (141). Jestliže se však snažíme, dokázati pouze řešitelnost rovnice (140) a nestaráme se o počet řešení (jde tedy o něco podobného jako o poměr problému III a II ve *Waringově* problému), můžeme opět zlepšiti nerovnosti (136), (137) pro r. V kap. IX dokazuje *Hua* v tomto směru, že každé dostatečně velké N, vyhovující kongruenci (141), lze vyjádřiti jako součet r sčítanců tvaru p_i^n, jestliže $r \geqq r_0(n)$, kde $r_0(n)$ pro velká n je asymptoticky rovno $6n \log n$. Vidíte, že v problému *Waring-Goldbachově* dospíváme kvalitativně i kvantitativně k výsledkům téhož rázu jako v problému *Waringově*, až na podmínku (141). Podotkněme ještě, že pro malá n udal *Hua* zvláště nízké hodnoty pro číslo $r_0(n)$ uvedené před chvílí: $r_0(4) = 15$, $r_0(5) = 25$, $r_0(6) = 39$, $r_0(7) = 55$.

Poznamenejme ještě toto: Ve *Waringově* problému jsme zjistili, že asymptotická formule pro $W_{n,r}(N)$ (a podobně je tomu u *Waring-Goldbachova* problému, formule (138)) platí pro

$$r \geqq 2^n + 1 \tag{142}$$

a rovněž pro

$$r \geqq [10n^2 \log n] \quad (n \geqq 12). \tag{143}$$

K odvození vzorce (143) je nutno užíti obtížné *Vinogradovovy* methody odhadu trigonometrických součtů, kdežto k odvození vzorce (142) se hodí methoda *Weylova* (ovšem s užitím *Vinogradovem* inspirované *Huovy* formule (81)). Pro velká n je ovšem (143) nesrovnatelně lepší než (142); pro malé hodnoty n dává však (142) lepší výsledky než (143).

Zbytek *Huovy* knihy obsahuje vedle několika „růzností" ještě problém řešení *soustavy* rovnic

$$\begin{aligned} p_1 + \ldots + p_r &= N_1 \\ p_1^2 + \ldots + p_r^2 &= N_2 \\ &\ldots\ldots\ldots\ldots \\ p_1^n + \ldots + p_r^n &= N_n. \end{aligned} \tag{144}$$

Tedy: při pevně daných n, r si klademe úkol: zvolíme-li přirozená čísla $N_1, \ldots, N_n$ jaký je počet řešení $W(N_1, \ldots, N_n)$ systému (144) (při čemž p_i mají býti prvočísla)? Řešení je ovšem dosti komplikované, ale probíhá podobně jako u *Waring-Goldbachova* problému: Pro dostatečně velké r se vyjádří $W(N_1, \ldots, N_n)$ asymptoticky opět vhodnou singulární řadou, a dokáže se, že součet singulární řady je větší než jistá kladná konstanta, vyhovují-li $N_1, \ldots, N_n$ jistým podmínkám. Tyto podmínky jsou zčásti opět číselně theoretického rázu (ovšem složitější než (141)), ale přistupují k nim ještě další podmínky kvantitativního rázu. Je na př. zřejmo, že má-li (144) míti řešení, musí jistě být $N_2 > N_1$ (neboť $p_i^2 > p_i$), ale současně musí $N_2 \leqq N_1^2$, jak ihned dostanete z (144). Toto je ovšem jen hrubá informace, podrobné vylíčení těchto podmínek najde čtenář v *Huově* knize. Jest poznamenati, že systémem (144) se s velkým úspěchem zabýval též sovětský matematik *Mardžanišvili*.

Na znalosti čtenáře klade *Huova* kniha asi stejné požadavky jako kniha *Vinogradovova*. Studium knihy je velmi zajímavé pro toho, kdo má o věc speciální zájem; ale je značně obtížné, neboť jde vlastně jen o jeden problém, technicky velmi složitý. K tomu přistupuje ještě tato obtíž: K řešení problémů této knihy je nutno kombinovati několik method (hlavně *Vinogradovových*), po případě je doplniti a připojiti k nim další pomocné úvahy na pohled dosti jiného rázu (na př. kap. I, II). Jde tedy vlastně o řešení řady dílčích úkolů a jejich koordinaci s hlediska společného cíle. Tato koordinace není na některých místech zcela jasně provedena. To vede někdy k značným obtížím pro čtenáře, někde i k menším nesprávnostem, které však na štěstí nemají vlivu na hlavní výsledky knihy. Zdá se, že rukopis této velmi pěkné a záslužné knihy by byl po této stránce potřeboval revise; nezapomínejme ovšem, že publikace této knihy byla na pět let přerušena válečnými událostmi.[40]) S tím souvisí asi také značný počet drobných nedopatření v tisku — není vždy jasno, jde-li o přepsání autora či překladatelů či o tiskové chyby.

[40]) A že, jak se zdá, byla aspoň částečně sázena za nepřítomnosti autorovy.