UNIVERZA V MARIBORU
PEDAGOŠKA FAKULTETA MARIBOR
ODDELEK ZA MATEMATIKO

Matej Mlakar

DIRICHLETOV IZREK O PRAŠTEVILIH V ARITMETIČNIH ZAPOREDJIH

Maribor, 2000

Neki starejši francoski matematik je dejal: "Matematično teorijo imaš lahko popolno šele tedaj, ko jo napraviš tako razumljivo, da si upaš njeno vsebino pojasniti prvemu mimoidočemu". Zahtevo po jasnosti in veliki dostopnosti, ki je v navedeni misli tako ostra glede matematične teorije, bi še ostreje postavil glede matematičnega problema, ki se poteguje za popolnost; jasnost in vsestranska dostopnost nas namreč privlačita, medtem ko nas pretirana zahtevnost in zapletenost prestrašita. Matematični problem mora biti dovolj težak, da nas privlači, in ne čisto nedostopen, da niso naši napori brezupni. Služiti mora kot smerokaz na za zapletenih poteh, ki vodijo k skritim resnicam, in nas nato nagraditi z veseljem ob najdeni rešitvi.

D. Hilbert ([5], stran 121)

Kazalo

1 Uvod. Osnovni pojmi **5**

2 O kongruencah **8**

3 Značaji **17**

4 Dirichletove L-vrste **26**

5 Dirichletov izrek o praštevilih v aritmetičnem zaporedju **52**

Kratek povzetek vsebine

V diplomskem delu je podan dokaz Dirichletovega izreka o praštevilih v aritmetičnem zaporedju, ki pravi:

V aritmetičnem zaporedju

$$\{l, l+k, l+2k, l+3k, ...\}, \text{ kjer velja } D(k,l) = 1,$$

obstaja neskončno praštevil.

Math.Subj.Class.(2000): 11N13,11B25

Ključni pojmi: *praštevilo, kongruenca, Dirichletov značaj, Dirichletove L-vrste, enakomerna konvergenca vrste, absolutna konvergenca vrste.*

1 Uvod. Osnovni pojmi

V naslednjih nekaj vrsticah definirajmo nekaj osnovnih pojmov, s katerimi se bomo večkrat srečevali v poglavjih, ki sledijo.

Definicija 1.1 (Eulerjeva funkcija φ) *Naj bo $\varphi : \mathbb{N} \to \mathbb{N}$ funkcija, za katero velja*

$$\varphi(n) = |M|\,, \quad \textit{kjer je } M = \{x \in \mathbb{N}; x \leq n, D(x,n) = 1\}.$$

Funkciji φ pravimo Eulerjeva funkcija φ.

Definicija 1.2 (*Möbiusova funkcija* μ :) *Funkciji $\mu : \mathbb{N} \to \mathbb{Z}$, določena s predpisom*

$$\mu(n) = \begin{cases} 1, & \textit{če } \; n = 1 \\ (-1)^r, & \textit{če } n = p_1 \cdot p_2 \cdot ... \cdot p_r, \textit{ kjer so } p_1, p_2, ...p_r \textit{ različna praštevila} \\ 0, & \textit{sicer (če obstaja vsaj eno praštevilo } p, \\ & \textit{katerega kvadrat deli } n), \end{cases}$$

pravimo Möbiusova funkcija μ.

Definicija 1.3 (Von Mongoldtova funkcija Λ) *Funkciji $\Lambda : \mathbb{N} \to \mathbb{R}$, določeni s predpisom*

$$\Lambda(n) = \begin{cases} \ln p, & \textit{če } \; n = p^k, \textit{kjer je } p \textit{ praštevilo, } k \in \mathbb{N} \\ 0, & \textit{sicer} \end{cases},$$

pravimo Von Mongoldtova funkcija Λ.

Izrek 1.1

$$\ln a = \sum_{d|a} \Lambda(d).$$

Dokaz: Naj bo

$$a = \prod_{i=1}^{r} p_i^{l_i}$$

kanonični razcep naravnega števila a. Potem velja

$$\begin{aligned} \ln a &= \ln\left(\prod_{i=1}^{r} p_i^{l_i}\right) = \sum_{i=1}^{r}\left(l_i \cdot (\ln p_i)\right) = \\ &= \sum_{i=1}^{r}\left(\Lambda(p_i) + \Lambda(p_i^2) + ... + \Lambda(p_i^{l_i})\right) = \sum_{d|a}\Lambda(d) \end{aligned}$$ $\square$

Izrek 1.2 (Dirichletov princip) *Naj bo $k \in N$, moč množice A, $m(A) > k$, in moč množice B, $m(B) = k$. Nobena funkcija $f : A \to B$ ni injektivna.*

Dokaz: Izberimo si k elementov v množici A in jih označimo z A_k. Če ni $f : A_k \to B$ injektivna, ni kaj dokazovati. Če je $f : A_k \to B$ injektivna, ima vsak element množice A_k drugo sliko. Če preslikamo poljubni element iz $A - A_k$ v množico B, je slika tega elementa že vsebovana v sliki množice A_k, zato f ne more biti injektivna. $\square$

Definicija 1.4 *Naj bo podano zaporedje funkcij (f_n),kjer so vse funkcije f_n definirane na istem definicijskem območju $A \subseteq \mathbb{R}$ in slikajo v $\mathbb{R}$. Zaporedje (f_n) konvergira po točkah k funkciji f, če za vsak $x \in A$ velja*

$$f(x) = \lim_{n\to\infty} f_n(x).$$

Definicija 1.5 *Vrsta $\sum f_n$, definirana na množici A,* konvergira po točkah *na A, če obstaja funkcija f z isto domeno in zaporedje delnih vsot $\{S_n\} = \{\sum_{i=1}^{n} f_i(x)\}$ konvergira po točkah k funkciji f na A.*

Definicija 1.6 *Naj bo zaporedje funkcij $\{f_n\}$ definirano na $A \subseteq \mathbb{R}$. Pravimo, da vrsta $\sum f_n$* enakomerno konvergira *na A k funkciji F, če za vsak $\varepsilon > 0$, $\exists N \in \mathbb{N}$, da za vsak $n \in \mathbb{N}$, $n > N$*

$$\left|\sum_{i=1}^{n} f_i(x) - F(x)\right| = |S_n(x) - F(x)| < \varepsilon \text{ za vsak } x \in A.$$

Izrek 1.3 (Cauchyev kriterij) *Potreben in zadostni pogoj za enakomerno konvergenco* $\sum f_n$ *na* A *je, da za vsak* $\varepsilon > 0$ *obstaja* $n \in \mathbb{N}$*, da za vsak* $m, n \in \mathbb{N}$*, za katere velja* $m > n > N$*, in za vsak* $x \in A$*, velja* $|S_m(x) - S_n(x)| < \varepsilon$.

Dokaz: glej [3], stran 430.

Izrek 1.4 (Weierstrassov M-test) *Če je* $\sum f_n$ *zaporedje funkcij, definiranih na* A*, in* $\{M_n\}$ *zaporedje pozitivnih realnih števil, da je* $\sum M_n$ *konvergentna in velja* $|f_n(x)| < M_n$ *za vsak* $x \in A$ *in vsak* $n \in N$*, potem* $\sum f_n$ *konvergira enakomerno in absolutno na* A.

Dokaz: glej [3], stran 432.

Tudi naslednji test se včasih imenuje *Weierstrassov M-test* ([2],389).

Izrek 1.5 *Naj bo* $a \in \mathbb{R}$*. Za vsako naravno število* n *naj velja, da je funkcija* $f_n(x)$ *definirana na intervalu* $[a, \infty)$*. Naj bodo* $M_1, M_2, ...$ *nenegativna realna števila. Če*

1. $|f_n(x)| \leq M_n$ *za vsak* $x \geq a, x \in R$*, in za vsak* $n \in \mathbb{N}$*,*
2. $\lim_{x\to\infty} f_n(x)$ *obstaja za vsak* $n \in \mathbb{N}$*,*
3. $\sum_{n=1}^{\infty} M_n$ *konvergira,*

potem velja

$$\lim_{x\to\infty} \sum_{n=1}^{\infty} f_n(x) = \sum_{n=1}^{\infty} \lim_{x\to\infty} f_n(x).$$

Izrek 1.6 *Naj bo* $m, k \in \mathbb{N}$*,* $D(k, m) = 1$*. Če je* $a_1, a_2, ..., a_m$ *popolna množica ostankov po modulu* m*., tedaj je tudi* $a_1k, a_2k, ..., a_mk$ *popolna množica ostankov po modulu* m*.*

Dokaz: glej [1], stran 43.

2 O kongruencah

Definicija 2.1 *Naj bo $m \in \mathbb{N}$ in naj velja $D(a,m) = 1$. Pravimo, da a pripada eksponentu f po modulu m, če je a^f prva izmed potenc $a^1, a^2, a^3, \ldots$ z naravnimi eksponenti, ki zadošča pogoju*

$$a^f \equiv 1 (\text{mod } m).$$

Opomba: *Tak f zmeraj obstaja, saj po Eulerjevem izreku velja*

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

Izrek 2.1 *Naj a pripada eksponentu f po modulu m in naj bosta b_1 in $b_2 \geq 0$. Tedaj velja*

$$a^{b_1} \equiv a^{b_2} (\text{mod } m) \text{ natanko tedaj, ko } b_1 \equiv b_2 (\text{mod } f).$$

Dokaz: Brez škode za splošnost lahko predpostavimo, da je $b_2 \geq b_1 \geq 0$.

($\Rightarrow$) Po predpostavki je $a^{b_1} \equiv a^{b_2} (\text{mod } m)$ oziroma

$$a^{b_2 - b_1} \equiv 1 (\text{mod } m).$$

Eksponent $b_2 - b_1$ lahko po izreku o deljenju z ostankom zapišemo kot

$$b_2 - b_1 = q \cdot f + r, \qquad \text{kjer je } q \geq 0, \qquad r \in \{0, 1, \ldots f-1\}.$$

Odtod sledi

$$1 \equiv a^{b_2 - b_1} \equiv a^{qf+r} \equiv (a^f)^q \cdot a^r (\text{mod } m).$$

Ker je $a^f \equiv 1 (\text{mod } m)$, je $a^r \equiv 1 (\text{mod } m)$. Torej je r lahko enak le 0, saj $a^1, \ldots, a^{f-1}$ niso kongruentna 1 po modulu m. Odtod sledi, da je f delitelj $b_2 - b_1$.

($\Leftarrow$) Iz predpostavke, da je $b_1 \equiv b_2 (\text{mod } f)$, sledi $b_2 - b_1 = q \cdot f$, kjer je $q \geq 0$.

$$\begin{aligned} b_2 &= b_1 + q \cdot f. \\ \text{Z uporabo } a^f &\equiv 1 (\text{mod } m) \text{ sledi trivialni razmislek} \\ a^{b_2} &\equiv a^{q \cdot f + b_1} \equiv a^{b_1} \cdot (a^f)^q \equiv a^{b_1}. \end{aligned}$$

$\square$

Posledica 2.1 $a^1, a^2, a^3, ..., a^{f-1}$ *so paroma nekongruentna števila* $(\mathrm{mod}\ m)$.

Če bi veljalo $a^x \equiv a^y (\mathrm{mod}\ m)$, kjer je $x, y < f$ in $x, y \in \mathbb{N}$, bi veljalo $a^{x-y} \equiv 1(\mathrm{mod}\ m)$, kar pa ne more biti res, saj je f najmanjši tak, za katerega velja $a^f \equiv 1(\mathrm{mod}\ m)$ in $x - y < f$, kar pa je res le, če je $x = y$, .saj je f najmanjše naravno število, za katero velja $a^f \equiv 1(\mathrm{mod}\ m)$ in $0 \leq x - y < f$.

Primer: $m = 13$, $a = 2$, iščemo vrednost α v kongruenci

$$2^{\widetilde{f}} \equiv \alpha(\mathrm{mod}\ 13).$$

$\widetilde{f}$	1	2	3	4	5	6	7	8	9	10	11	12
α	2	4	8	3	6	12	11	9	5	10	7	1

Vidimo lahko, da so vse α (mod 13) različne.

Posledica 2.2 *Naj bo* $b \geq 0$. *Potem je* $a^b \equiv 1(\mathrm{mod}\ m)$ *natanko tedaj, ko* $f \mid b$.

Uporabimo izrek 2.1 za $b_2 = 0$.

Posledica 2.3 *Če* a *pripada eksponentu* f $(\mathrm{mod}\ m)$, *velja* $f \mid \varphi(m)$.

Očitno, saj $a^{\varphi(m)} \equiv 1(\mathrm{mod}\ m)$, zato trditev sledi iz 2.3.

Primer: $m = 7$. Velja

$$\begin{aligned} 1^1 &\equiv 1(\mathrm{mod}\ 7) \\ 2^3 &\equiv 1(\mathrm{mod}\ 7) \\ 3^6 &\equiv 1(\mathrm{mod}\ 7) \\ 4^3 &\equiv 1(\mathrm{mod}\ 7) \\ 5^6 &\equiv 1(\mathrm{mod}\ 7) \\ 6^2 &\equiv 1(\mathrm{mod}\ 7). \end{aligned}$$

Vidimo, da je vsak eksponent delitelj $\varphi(7) = 6$.

Izrek 2.2 *Naj bosta g in p poljubni praštevili. Naj bo $l > 0$ in naj velja*

$$g^l \mid p - 1.$$

Potem obstaja takšen a, ki pripada eksponentu g^l po modulu p.

Dokaz: Vzemimo kongruenco

$$x^{\frac{p-1}{g}} \equiv 1(\mathrm{mod}\, p).$$

Zgornjo kongruenco zapišemo lahko kot $x^{\frac{p-1}{g}} - 1 \equiv 0(\mathrm{mod}\ p)$. Ta ima kvečjemu $\frac{p-1}{g}$ rešitev ([3],str.93). Ker je $\frac{p-1}{g} \leq \frac{p-1}{2} \leq p-2$, je rešitev kongruence prav gotovo manj kot $p-1$(za $p \geq 3$). Torej obstaja vsaj eno število c, kjer je $c \in \{0, 1, ...p-1\}$, da *ne velja* $c^{\frac{p-1}{g}} \equiv 1(\mathrm{mod}\, p)$.

Izberimo kandidata

$$a = c^{\frac{p-1}{g^l}}, \qquad (\clubsuit)$$

in pokažimo, da je ta izbor dober.

$$a^{g^l} \equiv c^{p-1} \equiv 1(\mathrm{mod}\, p).$$

Če a pripada eksponentu f, potem po izreku 2.1 $f \mid g^l$. Torej je q^l večkratnik f. Recimo, da $f \neq g^l$. Če bi veljalo

$$f = g^j, \text{ kjer je } j \leq l - 1,$$

bi iz $a^f \equiv 1(\mathrm{mod}\, p)$ sledilo

$$a^{g^{l-1}} \equiv 1(\mathrm{mod}\, p).$$

Odtod sledi sklep

$$a^{q^{l-1}} \equiv c^{\frac{p-1}{q}} \equiv 1(\mathrm{mod}\, p),$$

kar je protislovno. $\square$

Izrek 2.3 *Naj bo p neko praštevilo. Potem obstaja število g, ki pripada eksponentu $p-1$ po modulu p.*

Dokaz: Naj bo $p = 2$. Potem $g = 1$ zadošča pogojem izreka:

$$g \equiv 1(\text{mod } 2)$$

Če je $p > 2$, potem obstaja kanonični razcep števila $p-1 = \prod_{n=1}^{r} p_n^{l_n}$. Naj bo $r = 1$. Po izreku 2.2 obstaja število g, ki pripada $p-1$ po modulu p, ker je

$$p - 1 = p_1^{l_1}.$$

Naj bo $r > 1$. Za vsak $n \in \{1, 2, ..., r\}$, obstaja tak $a_n \in \{1, 2, ...p-1\}$, ki pripada eksponentu $p_n^{l_n}$ po modulu p. Velja

$$a_n^{p_n^{l_n}} \equiv 1(\text{mod } p).$$

Oblikujmo produkt

$$g = \prod_{n=1}^{r} a_n = a_1 \cdot a_2 \cdot ... \cdot a_n,$$

Naj g pripada f po modulu p. Tedaj $g^f \equiv 1(\text{mod } p)$. Po izreku 2.1 $f \mid p-1$.

Če $f = p - 1$, smo tak g našli.

Če $f \neq p-1$, lahko brez izgube za splošnost predpostavimo, da $f \mid \frac{p-1}{p_1}$. Ker $p_n^{l_n} \mid \frac{p-1}{p_1}$ za $n \in \{2, 3, ...r\}$, velja naslednje

$$1 \equiv g^{\frac{p-1}{p_1}} \equiv \left(\prod_{n=1}^{r} a_n\right)^{\frac{p-1}{p_1}} \equiv a_1^{\frac{p-1}{p_1}} \cdot \left(\prod_{n=2}^{r} a_n^{\frac{p-1}{p_1}}\right) \equiv a_1^{\frac{p-1}{p_1}} (\text{mod } p-1)$$

Po izreku 2.1, posledica 2.3, $p_1^{l_1} \mid \frac{p-1}{p_1}$, kar pa ni res. □

Definicija 2.2 *Vsako število g, ki pripada ekponentu* $p-1$ (mod p), *imenujemo primitivni koren po modulu* p.

Primer: 2 je primitivni koren (mod 13),(glej tabelo v izreku 2.1).

Izrek 2.4 *Naj bo* p *poljubno liho praštevilo in* l *poljubno naravno število. Tedaj obstaja število* g*, ki pripada eksponentu* $\varphi(p^l)$ *po modulu* p^l.

Dokaz: (i) Dokazujemo eksistenco g, da velja

$$g^{\varphi(p^l)} \equiv 1(\bmod p^l)$$

za poljubni p in l.

Naj bo $l = 1$. V tem primeru imamo pogoje, ekvivalentne izreku 2.3 in ni več kaj dokazovati.

Naj bo potemtakem $l > 1$. Dokažimo, da lahko izberemo g, ki je primitivni koren (mod p), za katerega ne velja

$$g^{p-1} \equiv 1(\bmod p^2). \tag{1}$$

Če $g^{p-1} \equiv 1(\bmod p)$, je tudi vsak predstavnik iz iste množice ostankov po modulu p takšen, zato velja

$$(g + p)^{p-1} \equiv 1(\bmod p).$$

Če bi veljalo $g^{p-1} \equiv 1(\bmod p^2)$, bi potem sledilo

$$\begin{aligned}
(g+p)^{p-1} &\equiv g^{p-1} + (p-1)g^{p-2} \cdot p + \frac{(p-1)(p-2)}{2} g^{p-3}p^2 + \\
&\quad + \frac{(p-1)(p-2)(p-3)}{6} g^{p-4}p^3 + ... \\
&\equiv 1 + (p-1)g^{p-2} \cdot p \ (\bmod p^2),
\end{aligned}$$

odkod sledi, da ne more veljati $(g + p)^{p-1} \equiv 1(\bmod p^2)$, ker bi iz tega sledilo

$$g^{p-2} \equiv 1(\bmod p).$$

Dokažimo, da g, izbran kot primitivni koren (mod p), ki ne zadošča (1), zadošča pogojem izreka.

Z matematično indukcijo po l pokažimo, da za vsak $l > 1$ velja

$$g^{p^{l-2}(p-1)} = 1 + h_l \cdot p^{l-1}, \text{kjer } \ p \nmid h_l. \tag{2}$$

Če je $l = 2$ dobimo mali Fermatov izrek

$$g^{p-1} \equiv 1(\bmod p).$$

Če je (2) res za l, potem sledi za $l+1$

$$g^{p^{l-1}(p-1)} = (1 + h_l \cdot p^{l-1})^p = 1 + h_l \cdot p^l + h_l^2 \cdot p \cdot \frac{p-1}{2} \cdot p^{2(l-1)} + n \cdot p^{3(l-1)},$$

kjer je n vsota vseh členov, razen prvih treh, v razvoju potence $(1+h_l \cdot p^{l-1})^p$ z binomsko formulo, pri katerih smo v vsakem izpostavili $p^{3(l-1)}$. Tretji in četrti člen na desni sta deljiva s p^{l+1}, saj je za $l > 2$

$$2(l-1) + 1 \geq l+1, \qquad 3l - 3 \geq l + 1.$$

Torej je desna stran $= 1 + h_{l+1} \cdot p^l$, kjer $p \nmid h_{l+1}$.

(ii) Naj g pripada f po modulu p^l.

Po izreku 2.1, posledica 2.3 $f \mid p^{l-1}(p-1)$.

Ker g pripada eksponentu $p-1 (\mathrm{mod}\ p)$, sledi po izreku 2.1, da je f oblike $p^m(p-1)$, kjer $m \in \{0, 1, ...l-1\}$. Če predpostavimo, da $f \mid p^{l-2}(p-1)$, sledi

$$g^{p^{l-2}(p-1)} \equiv 1 (\mathrm{mod}\ p^l),$$

kar je v nasprotju z (2). Torej je $f = p^{l-1}(p-1) = \varphi(p^l)$. $\square$

Ob določenih pogojih g, ki pripada eksponentu $\varphi(p^l)$ po modulu p^l, zmeraj obstaja.

Lema 2.5 *Naj bo* $l > 2, l \in \mathbb{N}$. *Za vsako liho število* n *velja*

$$n^{\frac{\varphi(2^l)}{2}} = n^{2^{l-2}} \equiv 1 (\mathrm{mod}\ 2^l).$$

Dokaz: Naj bo $l = 3$. Kongruenca $n^2 \equiv 1 (\mathrm{mod}\ 8)$ velja, saj je kvadrat lihega števila $l > 2$ zmeraj $\equiv 1 (\mathrm{mod}\ 8)$ oziroma to sledi po naslednjem razmisleku:

$$(2n+1)^2 = 4(k+1)k + 1,$$

ta kvadrat pa ima pri deljenju z 8 ostanek 1, saj je produkt dveh zaporednih števil sod, torej deljiv z 2.

Indukcijski korak $l \to l+1$: Naj za $l > 2$ velja $n^{2^{l-2}} \equiv 1 (\mathrm{mod}\ 2^l)$. Potem je

$$n^{2^{l-2}} = 1 + h \cdot 2^l, \qquad \text{kjer je } h \in \mathbb{N}.$$

Kvadrirajmo to enakost

$$n^{2^{l-1}} = 1 + h \cdot 2^{l+1} + h^2 \cdot 2^{2l} \equiv 1 (\mathrm{mod}\ 2^{l+1}).$$

Lema torej velja za eksponent $l+1$. Ker velja tudi za $l = 3$, velja splošno. $\square$

Izrek 2.6 *Naj bo* $l \in \mathbb{N}, l > 2$. *Potem* 5 *pripada eksponentu* 2^{l-2} *po modulu* 2^l.

Dokaz: Po lemi 2.5 velja $5^{2^{l-2}} \equiv 1 (\mathrm{mod}\ 2^l)$. Pokažimo, da je 2^{l-2} najmanjši tak eksponent, da velja $5^{2^{l-2}} \equiv 1 (\mathrm{mod}\ 2^l)$.

$$\begin{aligned} 5 &\equiv 1 + 4 (\mathrm{mod}\ 8) \\ 5^2 &\equiv 1 + 8 (\mathrm{mod}\ 16) \\ 5^4 &\equiv 1 + 16 (\mathrm{mod}\ 32) \\ 5^8 &\equiv 1 + 32 (\mathrm{mod}\ 64). \end{aligned}$$

Z indukcijo pokažimo, da velja splošno

$$5^{2^{l-3}} \equiv 1 + 2^{l-1} (\mathrm{mod}\ 2^l).$$

Za $l = 3$ in $l = 4$ velja, saj je $5 \equiv 1 + 4 (\mathrm{mod}\ 8)$ in $5^2 \equiv 1 + 8 (\mathrm{mod}\ 16)$. Predpostavimo, da trditev velja za nek naravni $l > 3$. Pokažimo, da velja tudi za njegovega naslednika $l + 1$ in dokažimo

$$5^{2^{l-2}} \equiv 1 + 2^l (\mathrm{mod}\ 2^{l+1}).$$

Po indukcijski predpostavki velja

$$5^{2^{l-3}} = h \cdot 2^l + \left(1 + 2^{l-1}\right), \text{kjer je } h \text{ naravno število.}$$

S kvadriranjem enakosti dobimo

$$\begin{aligned} 5^{2^{l-2}} &= \left(h \cdot 2^l + \left(1 + 2^{l-1}\right)\right)^2 = \\ &= h^2 2^{2l} + 1 + 2^{2l-2} + 2h2^l + 2h2^{2l-1} + 2^l \equiv \\ &\equiv 1 + 2^l\ (\mathrm{mod}\ 2^{l+1}). \end{aligned}$$

Kongruenco dobimo, če upoštevamo, da za $l > 3$ veljajo naslednji neenakosti

$$2l > l + 1, \quad 2l - 2 > l + 1.$$

Torej ne velja, da $5^{2^{l-3}} \equiv 1 (\mathrm{mod}\ 2^l)$. Odtod sledi, da eksponent števila 5 ne more biti delitelj 2^{l-3}. Ker je delitelj 2^{l-2}, je eksponent enak 2^{l-2}, kar pomeni, da 5 pripada eksponentu 2^{l-2} po modulu 2^l. □

Izrek 2.7 *Naj bo $l \in \mathbb{N}, l > 2$. Za vsako liho število a obstaja enolično določen $b \in \mathbb{Z}$ iz reduciranega sistema ostankv po modulu 2^{l-2}, tako da velja*

$$a \equiv (-1)^{\frac{a-1}{2}} \cdot 5^b \pmod{2^l}$$

Bolj natančno: s tem sta opisani bijekciji množice števil $\equiv 1 \pmod 4$ oziroma množice $\equiv -1 \pmod 4$ iz množice $\{0, 1, ..., 2^l - 1\}$ na množico $\{0, 1, ..., 2^{l-2}\}$.

Dokaz: Vsako liho število je bodisi $\equiv 1 \pmod 4$, bodisi $\equiv 3 \pmod 4$.

(i) Naj bo $a \equiv 1 \pmod 4$ in $b \in \{0, 1, ...2^{l-2} - 1\}$, kjer je $l > 2$.

Vrednosti 5^b predstavljajo natanko 2^{l-2} paroma nekongruentnih števil $\pmod{2^l}$, po izreku **??**. Vse od teh so $\equiv 1 \pmod 4$. Množica $\{0, 1, ..., 2^l - 1\}$ vsebuje natanko 2^{l-2} števil $\equiv 1 \pmod 4$. Imamo torej bijekcijo med vrednostmi iz te množice in vrednostmi b, kjer je $b = b(a)$; odvisna od izbire a. Vrednost b teče po množici $\{0, 1, ..., 2^{l-2} - 1\}$. Odtod sledi, da je

$$a \equiv 5^{b(a)} \pmod{2^l}$$

po *Dirichletovem principu* enolično rešljiva za b.

(ii) Naj bo $a \equiv 3 \pmod 4$ in $b \in \{0, 1, ...2^{l-2} - 1\}$, $l > 2$. Uporabimo (i) in a nadomestimo z $-a$ in dobimo

$$-a \equiv 5^b \pmod{2^l}.$$

Če združimo obe kongruenci v skupen zapis, dobimo

$$a \equiv (-1)^{\frac{a-1}{2}} 5^b \pmod{2^l}$$

□

3 Značaji

Naj velja v tem in v ostalih poglevjih, ki še sledijo, naslednje:

$$\varphi(k) = h,$$

kjer je k neko fiksno naravno število. Če ne bo drugače navedeno, imamo kongruence po modulu k.

Definicija 3.1 *Naj bo funkcija* $\chi : \mathbb{Z} \to \mathbb{C}$. χ *je značaj po modulu* k, *če velja*

(*i*)	$\chi(a) = 0,$ *če* $D(a, k) > 1,$
(*ii*)	$\chi(1) \neq 0,$
(*iii*)	$\chi(a_1) \cdot \chi(a_2) = \chi(a_1 . a_2),$ *če* $D(a_1, k) = 1$ *in* $D(a_2, k) = 1,$
(*iv*)	$\chi(a) = \chi(b),$ *če* $a \equiv b (\text{mod } k)$ *in* $D(a, k) = 1.$

V naslednjih nekaj trditvah si oglejmo nakaj osnovnih lastnosti tako definiranih funkcij χ.

Izrek 3.1 : *Za vsako funkcijo* χ, *ki ustreza definiciji 3, velja*

$$\chi(1) = 1.$$

Dokaz: $\chi(1) \cdot \chi(1)$ je po *definiciji 3* enako $\chi(1 \cdot 1) = \chi(1)$. Od tod sledi zaradi (*ii*), da je $\chi(1) = 1$. □

Izrek 3.2 *Naj bo* $D(a, k) = 1$. *Tedaj je* $(\chi(a))^h = 1$ (*oziroma* $\chi(a)$ *je* $\varphi(k)-$*ti koren enote).*

Dokaz: Po Eulerjevem izreku je

$$a^h \equiv 1 (\text{mod } k).$$

Torej je

$$(\chi(a))^h = \chi(a) \cdot \chi(a) \cdot \chi(a) \cdot ... \cdot \chi(a) = \chi(a^h) = 1$$

(uporabimo definicijo 3.1; (*iii*) na drugem enačaju, (*iv*) na tretjem enačaju). □

Izrek 3.3 *Za vsako naravno število k obstaja končno število značajev* $\chi (\bmod\ k)$, *vedno obstaja vsaj en značaj* $(\bmod\ k)$.

Dokaz:

(1) Znotraj vsakega razreda ostankov $(\bmod\ k)$ so vse vrednosti funkcije χ enake.

Naj a teče po poljubni popolni množici ostankov $(\bmod\ k)$ oziroma $a \in \{1, 2, ..., k\}$. Potem je $\chi(a)$ bodisi h-ti koren enote (za $D(a, k) = 1$), bodisi enak 0 (za $D(a, k) > 1$). $\chi(a)$ izberemo iz končne množice vrednosti (0 ali h-ti koren enote).

Različnih vrednosti $\chi(a)$ za $a \in \{1, 2, ..., k\}$ ne more biti več kot h, torej jih je končno mnogo.

(2) Vedno obstaja vsaj en χ, saj je funkcija

$$\chi_0(a) = \begin{cases} 1, & \text{če } D(a, k) = 1 \\ 0, & \text{sicer.} \end{cases}$$

očitno značaj, ker zadošča definiciji 3.1. □

Definicija 3.2 χ_0 *imenujemo osnovni Dirichletov značaj.*

Izrek 3.4 *Če je* χ *značaj* $(\bmod\ k)$, *je tudi njegova konjugirana vrednost* $\overline{\chi}$ *prav tako značaj*$(\bmod\ k)$.

Dokaz: Pogojem (i)-(iv) iz definicije 3.1 je očitno zadoščeno. □

Izrek 3.5 *Naj a teče po popolni množici ostankov* $(\bmod\ k), a \in \{1, 2, ..., k\}$. *Potem je za konkretni značaj* χ *vrednost vsote po popolni množici ostankov enaka*

$$\sum_{a=1}^{k} \chi(a) = \begin{cases} h, & \text{če } \chi = \chi_0 \\ 0, & \text{sicer.} \end{cases}$$

Dokaz: Takoj opazimo, da je vrednost vsote zaradi lastnosti *(iv)* in definicije 3.1 neodvisna od izbire množice ostankov.

(1) Naj bo $\chi = \chi_0$.

Za vsak a za katerega velja $D(a,k)=1$, je $\chi_0(a)=1$.

Takih vrednosti je v popolni množici ostankov (mod k) enako h. Torej je h členov vsote enakih 1, ostali so 0.

(2) Naj bo $\chi \neq \chi_0$.

Izberimo tako naravno število b, da bo $D(b,k)=1$ in $\chi(b)\neq 1$ (`opomba`: $\chi(b)\neq 1$ vedno obstaja, saj je $\chi\neq\chi_0$). Potem velja po izreku 1.6, da v primeru, ko a preteče vse vrednosti popolne množice ostankov (mod k), tudi $a\cdot b$ preteče vse vrednosti popolne množice ostankov (mod k). Sledi

$$\xi=\sum_{a=1}^{k}\chi(a)=\sum_{a=1}^{k}\chi(b\cdot a)=\sum_{a=1}^{k}\chi(b)\cdot\chi(a)=\chi(b)\cdot\sum_{a=1}^{k}\chi(a)=\chi(b)\cdot\xi;$$

(drugi enačaj velja zaradi zgornje trditve, tretji zaradi (iii) in (i) iz definicije 3.1.

$$(\chi(b)-1)\cdot\xi=0$$

Ker je po predpostavki $\chi(b)\neq 1$, je $\xi=\sum_{a=1}^{k}\chi(a)=0$. □

Izrek 3.6 *Če sta χ_1 in χ_2 značaja, je tudi produkt $\chi_1(a)\cdot\chi_2(a)$ značaj.*

Dokaz: Pogojem (i)-(iv) je očitno zadoščeno. □

V izreku 3.2 smo pokazali, da za vsako naravno število k obstaja končno število značajev (mod k).Označimo to število s c.

Izrek 3.7 *Naj bo χ_1 poljuben značaj. Ko χ preteče po vseh c možnih značajih, tudi $\chi_1\cdot\chi$ preteče po vseh c možnih značajih.*

Dokaz: Naj velja $\chi_1\chi_2=\chi_1\chi_3$.

(1) Če je $D(a,k)=1$, potem $\chi_1(a)\neq 0$. Odtod sledi $\chi_2(a)=\chi_3(a)$.

(2) Če je $D(a,k)>1$, potem $\chi_2(a)=\chi_3(a)=0$.

Torej je $\chi_2(a)=\chi_3(a)$ za vsak $a\in\{1,2,...,k\}$, oziroma $\chi_2=\chi_3$.

Funkcija

$$\chi\longmapsto\chi_1\cdot\chi$$

je injektivna. Po *izreku 2.6* so vse te funkcije značaji.

Vseh značajev za fiksno naravno število k je c, imamo tudi c funkcij oblike $\chi_1\chi$. Po *Dirichletovem principu* so te funkcije tudi vsi značaji (mod k). □

Lema 3.8 *Naj bosta a_1 in a_2 lihi števili. Potem velja*

$$\frac{a_1-1}{2}+\frac{a_2-1}{2}\equiv\frac{a_1a_2-1}{2}(\text{mod } 2).$$

Dokaz:

$$\begin{aligned}(a_1-1)(a_2-1) &\equiv 0(\text{mod } 4)\Longleftrightarrow\\ \Longleftrightarrow (a_1-1)+(a_2-1) &\equiv a_1a_2-1(\text{mod } 4)\Longleftrightarrow\\ \Longleftrightarrow \frac{(a_1-1)}{2}+\frac{(a_2-1)}{2} &\equiv \frac{a_1a_2-1}{2}(\text{mod } 2).\end{aligned}$$

□

Izrek 3.9 *Naj bo $d\in\mathbb{N}$. Naj velja $D(d,k)=1$ in naj ne velja $d\equiv 1(\text{mod } k)$. Tedaj obstaja značaj χ po modulu k, za katerega velja $\chi(d)\neq 1$.*

(`Opomba`: v nadaljevanju bo potrebno imeti tako funkcijo χ, katere eksistenco dokazujemo. Ta izrek konstruktivno pokaže, da tak χ ob zelo šibkih pogojih vedno obstaja)

Dokaz: Definiramo $\chi(a)=0$, če je $D(a,k)\neq 1$.

Potrebno je definirati še tiste vrednosti a, kjer je $D(a,k)=1$. Naj bo $a\in\mathbb{Z}$ poljubno celo število, tuje z k.

Po predpostavki d ni kongruenten 1 (mod k), zato mora veljati natanko ena izmed naslednjih trditev:

(1) obstaja liho praštevilo p in $l\in\mathbb{N}$, da velja

$$p^l \mid k \quad\wedge\quad d \text{ ni kongrunten 1 (mod } p^l),$$

(2) obstaja število oblike 2^l, $l\in\mathbb{N}$, da velja

$$2^l \mid k \quad\wedge\quad d \text{ ni kongruenten 1 (mod } 2^l).$$

V nadaljevanju dokaza ločimo oba primera:

(1) Naj velja, da d ni kongruenten 1 (mod p^l), kjer je p liho praštevilo, $l \in \mathbb{N}$ ter $p^l \mid k$. Takoj opazimo, da $p \nmid d$, saj $D(d,k) = 1$. Izberimo si tako število g, da pripada eksponentu $\varphi(p^l)$ po modulu p^l (izrek 2.4). $D(a,k) = 1$ po predpostavki. Ker $p \mid k$, seveda $p \nmid a$. Obstaja enolično določen $b \in \{1, ..., \varphi(p^l)\}$, tako da velja

$$g^b \in \{g^1, ..., g^{\varphi(p^l)}\}.$$

Množica $\{g^1, ..., g^{\varphi(p^l)}\}$ je reduciran razred ostankov po modulu p^l, saj $p \nmid g$. To pomeni, da je funkcija, definirana s

$$b \longmapsto g^b$$

bijekcija.

Skonstruirajmo takšno funkcijo χ, da bo zadoščala potrebam izreka. Izberimo si kompleksno število

$$\rho = e^{\frac{2\pi i}{\varphi(p^l)}}$$

in

$$\chi(a) = \rho^b.$$

Opazimo lahko, da ima ρ^b periodo $\varphi(p^l)$ in da je b je enolično določen (mod $\varphi(p^l)$), zato je vrednost $\chi(a)$ popolnoma določena z vrednostjo a, saj velja implikacija

$$a \equiv g^{b_1} (\text{mod } p^l) \wedge a \equiv g^{b_2} (\text{mod } p^l) \Longrightarrow b_1 \equiv b_2 (\text{mod } \varphi(p^l)) \Longrightarrow \rho^{b_1} = \rho^{b_2}.$$

Preverimo, če je tako definiran χ res značaj:

(i) $\chi(a) = 0$, če $D(a,k) > 1$ (po definiciji)

(ii) $\chi(1) = \rho^0 = 1$, saj $b = 0$

(iii) Naj bo $D(a_1,k) = 1$ in $D(a_2,k) = 1$, $a_1 \equiv g^{b_1}(\text{ mod } p^l)$ in $a_2 \equiv g^{b_2} (\text{mod } p^l)$

$$\chi(a_1 \cdot a_2) = \rho^{b_1+b_2} = \rho^{b_1}\rho^{b_2} = \chi(a_1) \cdot \chi(a_2)$$

(iv) očitno; za $a_1 \equiv a_2 (\text{mod } k)$ sledi $a_1 \equiv a_2 (\text{mod } p^l)$, saj $p^l \mid k$. Od tod $\chi(a_1) = \chi(a_2)$.

χ je torej značaj. Pokažimo še, da je

$$\chi(d) \neq 1.$$

Naj bo $d \equiv g^r (\text{mod } p^l)$; tak r obstaja, saj je $D(d,k) = 1$. Tedaj je $\chi(d) = \rho^r \neq 1$, saj če bi veljalo

$$\rho^r = 1,$$

bi sledilo

$$\varphi(p^l) \mid r \Rightarrow d \equiv 1 (\text{mod } p^l), \text{kar je v nasprotju s predpostavko izreka.}$$

(2) Naj bo d nekongreuenten $1(\text{mod } 2^l)$, l naravno število in $2^l \mid k$. Potem je k sod in velja $d \equiv 1(\text{mod } 2)$, saj je $D(d,k) = 1$. Potemtakem mora biti $l > 1$.

(2.1) Naj bo $d \equiv 1(\text{mod } 4)$. Za $D(a,k) = 1$ po *izreku 2.6* zaradi $D(d,2) = 1$ lahko izberemo b iz množice $\{0, 1, ...2^{l-2}\}, l > 0$, na en sam način, da bo

$$a \equiv (-1)^{\frac{a-1}{2}} \cdot 5^b (\text{mod } 2^l).$$

Izberimo

$$\rho = e^{\frac{2\pi i}{2^{l-2}}} \text{ in definirajmo } \chi(a) = \rho^b.$$

ρ^b ima periodo 2^{l-2}, b je določen po $(\text{mod } 2^{l-2})$. Pokažimo, da je χ značaj.

(ii) $\chi(1) = \rho^0 = 1$,ker $b = 0$,

(iii) Naj bo $D(a_1,k) = 1$ in $D(a_2,k) = 1$ ter $a_1 \equiv (-1)^{\frac{a_1-1}{2}} \cdot 5^{b_1} (\text{mod } 2^l)$ in $a_2 \equiv (-1)^{\frac{a_2-1}{2}} \cdot 5^{b_2} (\text{mod } 2^l)$. Po *izreku 1.6* in *lemi 3.8* je

$$\begin{aligned} a_1 a_2 &\equiv (-1)^{\frac{a_1-1}{2}+\frac{a_2-1}{2}} \cdot 5^{b_1+b_2} \equiv (-1)^{\frac{a_1 \cdot a_2 - 1}{2}} \cdot 5^{b_1+b_2} (\text{mod } 2^l), \\ \chi(a_1 a_2) &= \rho^{b_1+b_2} = \rho^{b_1}\rho^{b_2} = \chi(a_2).\chi(a_1). \end{aligned}$$

(iv) očitno; $a_1 \equiv a_2 (\text{mod } k)$. Ker $2^l \mid k$.Iz $a_1 \equiv a_2 (\text{mod } 2^l)$ sledi $\chi(a_1) = \chi(a_2) (\text{mod } 2^l)$.

Ker d ni kongruenten $1 (\text{mod } 2^l)$ in $d \equiv 1 (\text{mod } 4)$, lahko izberemo r, da velja $d \equiv 5^r (\text{mod } 2^l)$,

$$2^{l-2} \nmid r, \ \chi(d) = \rho^r \neq 1.$$

(*2.2*) Naj bo $d \equiv -1 (\text{mod } 4.)$. Če je $D(a,k) = 1$ je tak a liho število. Izberimo

$$\chi(a) = (-1)^{\frac{a-1}{2}}$$

Pokažimo, da je tako izbrani χ značaj:

(ii) $\chi(1) = (-1)^{\frac{1-1}{2}} = 1,$

(iii) Naj bo $D(a_1, k) = 1$ in $D(a_2, k) = 1$. Z uporabo *leme 3.8* imamo

$$\begin{aligned} \chi(a_1 \cdot a_2) &= (-1)^{\frac{a_1 \cdot a_2 - 1}{2}} = (-1)^{\frac{a_1-1}{2}} \cdot (-1)^{\frac{a_2-1}{2}} = \\ &= \chi(a_1) \cdot \chi(a_2) \end{aligned}$$

(iv) Očitno, saj $4 \mid k$.

Razen tega je

$\chi(d) = -1 \neq 1.$ □

Izrek 3.10 *Naj bo a neko fiksno naravno število. Vsota po vseh značajih je*

$$\sum_\chi \chi(a) = \begin{cases} c & \textit{če} \quad a \equiv 1 (\text{mod } k) \\ 0, & \textit{sicer} \end{cases} .$$

Dokaz: Naj bo $a \equiv 1 (\text{mod } k)$. Po *izreku 3.1* je v vsoti natanko c vrednosti $\chi(a)$, ki so enake 1 (če je $a \equiv 1$, je $\chi(a) = 1$). Enakost je trivialno dosežena.

Naj bo zdaj $D(a,k) > 1$.Potem je vsak člen $\chi(a) = 0$.

Če pa je $D(a,k)=1$ in ne velja $a\equiv 1(\text{mod } k)$, pa izberimo tak značaj $\chi_1(a)$, da bo veljalo $\chi_1(a)\neq 1$ (to po *izreku 3.7* vedno lahko storimo). Sledi

$$\begin{aligned}\eta &= \sum\nolimits_\chi \chi(a) = \sum\nolimits_\chi \chi(a)\cdot\chi_1(a) = \\ &= \chi_1(a)\cdot\sum\nolimits_\chi \chi(a) = \chi_1(a)\cdot\eta; \\ &\Longrightarrow (\chi_1(a)-1)\cdot\eta = 0; \text{torej je } \eta = 0.\end{aligned}$$

(Na drugem enačaju smo uporabili lastnost značajev iz *izreka 3.7*). □

Izrek 3.11 *Vseh značajev* $(\text{mod } k)$ *je natanko* $\varphi(k)$, (*oziroma:* $c=h$).

Dokaz: Ideja dokaza je tem, da primerjemo vsoto vrednosti enaga značaja po popolni množici ostankov po modulu k in vsoto vrednosti vseh možnih značajev za konkreten razred ostankov po modulu k.

Oblikujmo dvojno vsoto

$$\sum\nolimits_{a,\chi}\chi(a), \text{ kjer je } a\in\{1,...k\} \text{ in } \chi \text{ teče po vseh značajih.}$$

Lahko jo zapišemo na dva načina

$$\begin{aligned}\sum\nolimits_{a=1}^{k}\left(\sum\nolimits_\chi \chi(a)\right) &= c+0+0+...+0=c, \\ \sum\nolimits_\chi\left(\sum\nolimits_{a=1}^{k}\chi(a)\right) &= \varphi(k)+0+...=\varphi(k)=h.\end{aligned}$$

V prvo vsoto prispeva le člen indeks $a=0$, vsi ostali prispevajo 0, v drugo pa le indeks χ_0, ostali dajo 0.

Vseh značajev $(\text{mod } k)$ je natanko $\varphi(k)$. □

Izrek 3.12 *Naj velja* $D(a,l)=1$. *Potem je*

$$\sum\nolimits_\chi \chi(a)\cdot\frac{1}{\chi(l)} = \begin{cases}\varphi(k), & \text{če} \quad a\equiv l(\text{mod } k) \\ 0, & \textit{sicer}\end{cases}.$$

Dokaz: Izberimo si tako naravno število j, da velja

$$j\cdot l\equiv 1(\text{mod } k).$$

Velja

$$\chi(j) \cdot \chi(l) = \chi(j \cdot l) = 1$$

(prva enakost drži zaradi lastnosti(iii), drugi zaradi lastnosti (iv) iz *definicije 3.1*),

$$\chi(j) = \frac{1}{\chi(l)}.$$

Vsoto $\sum_\chi \chi(a) \cdot \frac{1}{\chi(l)}$ lahko sedaj zapišemo kot

$$\sum\nolimits_\chi \chi(a)\chi(j),$$

kar je enako

$$\sum\nolimits_\chi \chi(a \cdot j).$$

Uporabimo zadnji dokazani *izrek 3.11* in pridemo do željenega rezultata:

$$\begin{aligned}\sum\nolimits_\chi \chi(a) \cdot \frac{1}{\chi(l)} &= \begin{cases} \varphi(k), & \text{če} \quad a \cdot j = 1(\text{mod } k) \\ 0, & \text{sicer} \end{cases} \\ &= \begin{cases} \varphi(k), & \text{če} \quad a \equiv l(\text{mod } k) \\ 0, & \text{sicer} \end{cases}\end{aligned}$$

□

V nadaljevanju bomo zelo pozorni na to, kakšne vrednosti zavzamejo značaji. V ta namen definirajmo:

Definicija 3.3 *Velja:*

(i) χ *je značaj prve vrste, če je* $\chi = \chi_0$.

(ii) χ *je značaj druge vrste, če je* χ *realna in* $\chi \neq \chi_0$, $(0, 1, -1$ *so edine funkcijske vrednosti in* -1 *se dejansko pojavi).*

(iii) χ *je značaj tretje vrste, če obstaja vsaj ena funkcijska vrednost* χ, *ki ni realna.*

4 Dirichletove L-vrste

Definicija 4.1 *Vrsto*

$$\sum_{a=1}^{\infty} \frac{\chi(a)}{a^s}$$

kjer je $s \in \mathbb{R}$, in funkcija χ Dirichletov značaj, imenujemo Dirichletova L-vrsta.

Definicija 4.2 Dirichletova L-funkcija *je definirana s formulo*

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

kjer je χ Dirichletov značaj, s pa teče po množici vseh realnih števil, za katere je Dirichletova L-vrsta *konvergentna.*

Izrek 4.1 *Za vsakega od $\varphi(k)$ značajev* $(\mathrm{mod}\ k)$ *je vrsta*

$$\sum_{a=1}^{\infty} \frac{\chi(a)}{a^s}$$

absolutno konvergentna za $s > 1$.

Dokaz: Po definiciji značaja je $|\chi(a)| \leq 1$. Potem je

$$\left| \frac{\chi(a)}{a^s} \right| \leq \frac{1}{a^s}.$$

Ker $\sum_{a=1}^{\infty} \frac{1}{a^s}$ konvergira ([3],str.348), konvergira tudi $\sum_{a=1}^{\infty} \frac{|\chi(a)|}{a^s}$, odkod sledi, da je $L(s, \chi)$ absolutno konvergentna. □

Izrek 4.2 *Naj bo χ značaj, $\chi \neq \chi_0$. Potem velja*

$$\left| \sum_{a=u}^{v} \chi(a) \right| \leq \frac{h}{2},$$

kjer sta $u, v \geq 1$ in $\varphi(k) = h$.

Dokaz: Vseh členov vsote $\sum_{a=u}^{v}\chi(a)$ je $v-u+1$. To lahko zapišemo v obliki

$$v-u+1=t\cdot k+l,\qquad \text{kjer je } t\geq 0 \text{ in } l\in\{0,1,...k-1\}.$$

Če je $t>0$, imamo v vsoti $t\cdot k$ členov, ki predstavljajo t krat popolno množico ostankov $(\mathrm{mod}\ k)$.

Po *izreku 3.5* je $\sum\chi(a)$ po popolni množici ostankov enaka 0. Brez škode za splošnost lahko predpostavimo, da je $t=0$. Ostane nam največ l neničelnih členov vsote $\sum_{a=u}^{v}\chi(a)$.

V nadaljevanju upoštevajmo, da je v popolni množici ostankov natanko h vrednosti $|\chi(a)|$ enako 1, ostale vrednosti pa so enake 0. Predpostavimo, da se zdaj v naši 'delni' množici ostankov pojavlja največ $\frac{h}{2}$ členov, za katere velja $\chi(a)=1$. Potem lahko uporabimo predpostavko in s trikotniško neenakostjo ocenimo

$$\left|\sum_{a=u}^{v}\chi(a)\right|\leq\sum_{a=u}^{v}|\chi(a)|\leq\frac{h}{2}.$$

Če bi se v 'delni' množici ostankov pojavilo več kot $\frac{h}{2}$ členov, za katere je $|\chi(a)|=1$, bi bila ocena naslednja:

$$\left|\sum_{a=u}^{v}\chi(a)\right|=\left|\sum_{a=u}^{u+k-1}\chi(a)-\sum_{a=v+1}^{u+k-1}\chi(a)\right|=\left|\sum_{a=v+1}^{u+k-1}\chi(a)\right|\leq\sum_{a=v+1}^{u+k-1}|\chi(a)|<\frac{h}{2}$$

($k-1$ zaporednih ostankov tvori namreč popolno množico ostankov $(\mathrm{mod}\ k)$, vsota ustreznih členov je 0, ostane nam le odštevanec, ki ga ustrezno ocenimo).

V naslednjem izreku pripravimo vse potrebno za dokaz enakomerne konvergence $L(s,\chi)$, kjer je $\chi\neq\chi_0$ in $s\geq 1$. □

Izrek 4.3 *Naj bo* $a\in\{u,u+1,...,v\}$, *in definirajmo preslikavo*

$\Gamma:\{u,u+1,...,v\}\to\mathbb{C}$,

$$\Gamma: a\longmapsto\gamma_a.$$

Naj bo

$$\begin{aligned}R(w)&=\sum_{a=u}^{w}\gamma_a\quad \textit{za } u\leq w\leq v,\\ \max_{u\leq w\leq v}|R(w)|&=\nu\quad\textit{in}\quad \varepsilon_u\geq\varepsilon_{u-1}\geq...\geq\varepsilon_v\geq 0.\end{aligned}$$

Potem velja

$$\left|\sum_{a=u}^{v} \varepsilon_a \cdot \gamma_a\right| \leq \varepsilon_u \cdot \nu.$$

Dokaz: Brez škode za splošnost lahko predpostavimo, da je $R(u-1)=0$. Ocenimo vrednost $\sum_{a=u}^{v} \varepsilon_a \cdot \gamma_a$.

$$\sum_{a=u}^{v} \varepsilon_a \cdot \gamma_a = \sum_{a=u}^{v} \varepsilon_a \cdot (R(a) - R(a-1)) = \sum_{a=u}^{v-1} R(a) \cdot (\varepsilon_a - \varepsilon_{a+1}) + R(v) \cdot \varepsilon_v,$$

Ker je $R(a) \leq \nu$ za vsak $u \leq a \leq v-1$, je $\sum_{a=u}^{v-1} R(a) \cdot (\varepsilon_a - \varepsilon_{a+1}) \leq \nu \cdot \left(\sum_{a=u}^{v-1} (\varepsilon_a + \varepsilon_{a+1})\right)$. Torej velja

$$\left|\sum_{a=u}^{v} \varepsilon_a \cdot \gamma_a\right| \leq \nu \cdot \left(\sum_{a=u}^{v} (\varepsilon_a - \varepsilon_{a+1}) + \varepsilon_v\right) = \nu \cdot \varepsilon_u.$$ □

Izrek 4.4 *Če χ ni osnovni značaj, potem vrsta $\sum_{a=1}^{\infty} \frac{\chi(a)}{a^s}$ konvergira enakomerno za $s \geq 1$.*

Dokaz: Naj bo $v \geq u \geq 1$. Uporabimo prejšnji *izrek 4.3* in izberimo

$$\varepsilon_a = \frac{1}{a^s},\ \gamma_a = \chi(a), \nu = \max_{u \leq w \leq v} \left|\sum_{a=u}^{v} \chi(a)\right|.$$

Po *izreku 4.2* velja $|\sum_{a=u}^{v} \chi(a)| \leq \frac{h}{2}$, kar zadostuje za oceno

$$\left|\sum_{a=u}^{v} \frac{\chi(a)}{a^s}\right| \leq \max_{u \leq w \leq v} \left|\sum_{a=u}^{v} \chi(a)\right| \cdot \varepsilon_a \leq \frac{h}{2} \cdot \frac{1}{a^s} \leq \frac{h}{2} \cdot \frac{1}{u^s} \leq \frac{h}{2u}, \quad \text{kjer je } s \geq 1.$$

Izberimo poljuben $\delta > 0$.

$$\left|\sum_{a=u}^{v} \frac{\chi(a)}{a^s}\right| < \delta, \quad \text{če je } \frac{h}{2u} \leq \delta.$$

Očitno lahko vedno izberemo u, da bo veljala zgornja neenakost. Naj bo med vsemi možnimi izbirami u število u_0 najmanjše. Ker je u_0 popolnoma neodvisen od vrednosti s, smo pokazali željeno enakomerno konvergenco. □

Lema 4.5 *Naj bo $s > 1$. Vrsta*

$$\sum_{a=1}^{\infty} \frac{\ln a}{a^s}$$

je konvergentna.

Dokaz: Funkcija $f(a) = \frac{\ln a}{a^s}$ je monotono padajoča funkcija za $a > 1$. Velja, da je $\sum_{a=1}^{\infty} \frac{\ln a}{a^s} < \int_1^{\infty} \frac{\ln a}{a^s} da$. Posplošeni integral integriramo 'per partes' in dobimo

$$\lim_{b\to\infty} \int_1^b \frac{\ln a}{a^s} da = \lim_{b\to\infty} \left(\frac{a^{1-s}}{1-s} \cdot \ln a - \frac{a^{1-s}}{(1-s)^2} \right) |_1^b \, .$$

Posplošeni integral obstaja, saj $\lim_{b\to\infty} \left(\frac{b^{1-s}}{1-s} \cdot \ln b \right)$ obstaja po L'Hospitalovem pravilu in je enaka 0, sledi $\lim_{b\to\infty} \int_1^b \frac{\ln a}{a^s} da = \frac{1}{(1-s)^2}$. Po integralskem kriteriju ([6], stran296) je vrsta $\sum_{a=1}^{\infty} \frac{\ln a}{a^s}$, kjer je $s > 1$, konvergentna. □

Izrek 4.6 *Vrsta*

$$\sum_{a=1}^{\infty} \frac{\chi(a) \cdot \ln a}{a^s}$$

je absolutno konvergentna za vsak $s > 1$ in je enakomerno konvergentna na intervalu $(1+\varepsilon, \infty)$, kjer je $\varepsilon > 0$ poljuben.

Dokaz: Izberimo poljubno število $s > 1$. Zaradi gostosti množice realnih števil obstaja $\varepsilon > 0$, da velja $s > 1 + \varepsilon$. Izberimo tak ε.

Oglejmo si vrsto

$$M_a = \sum_{a=1}^{\infty} \frac{\ln a}{a^{1+\varepsilon}}.$$

Ta vrsta je konvergentna. Po *Weierstrassovem M-testu* za $f_n(a) = \sum_{a=1}^{\infty} \frac{\chi(a) \cdot \ln a}{a^s}$ dobimo enakomerno konvergenco $\sum_{a=1}^{\infty} \frac{\chi(a) \cdot \ln a}{a^s}$ za $s \in (1+\varepsilon, \infty)$.

Absolutna konvergenca sledi iz tega, ker je

$$\left| \frac{\chi(a) \cdot \ln a}{a^s} \right| \leq \frac{\ln a}{a^s}.$$

Ker $\sum_{a=1}^{\infty} \frac{\ln a}{a^s}$ konvergira *(lema 4.5)*, sledi da $\sum_{a=1}^{\infty} \frac{\chi(a) \cdot \ln a}{a^s}$ absolutno konvergira za vsak $s \geq 1$. □

Izrek 4.7 *Naj bo* $s > 1$. *Potem je odvod funkcije* L *enak*

$$L'(s,\chi) = -\sum_{a=1}^{\infty} \frac{\chi(a)\cdot \ln a}{a^s}.$$

Dokaz: $L(s,\chi) = \sum_{a=1}^{\infty} \frac{\chi(a)}{a^s}$. Če vsak člen te vrste parcialno odvajamo po s, dobimo splošni člen

$$\frac{\partial}{\partial s}\left(\frac{\chi(a)}{a^s}\right) = -\frac{\chi(a)\cdot \ln a}{a^s}.$$

Po prejšnjem izreku $\sum_{a=1}^{\infty} \frac{\chi(a)\cdot \ln a}{a^s}$ enakomerno konvergira za $s \in (1+\varepsilon, \infty)$. Vsota odvodov členov $\sum_{a=1}^{\infty} \frac{\chi(a)}{a^s}$ je po ([3],str.437) enaka odvodu vrste, odkod sledi

$$L'(s,\chi) = -\sum_{a=1}^{\infty} \frac{\chi(a)\cdot \ln a}{a^s}.$$

$\square$

Naslednja trditev pove še več: konvergenca $\sum_{a=1}^{\infty} \frac{\chi(a)\cdot \ln a}{a^s}$ je enakomerna za $s \geq 1$, če je vrsta $L(s,\chi)$ določena z značajem $\chi \neq \chi_0$ (torej druge ali tretje vrste). Hkrati pokažemo še omejenost L'.

Izrek 4.8 *Naj bo* χ *značaj druge ali tretje vrste. Potem vrsta*

$$\sum_{a=1}^{\infty} \frac{\chi(a)\cdot \ln a}{a^s}$$

enakomerno konvergira za vse $s \geq 1$, *in velja:*

$$\left|\sum_{a=1}^{\infty} \frac{\chi(a)\cdot \ln a}{a^s}\right| < h.$$

Dokaz: Dokažimo najprej enakomerno konvergenco. Naj bo $s \geq 1$ in

$\chi \neq \chi_0$. Oglejmo si funkcijo $\frac{\ln \xi}{\xi}$ oziroma njen odvod po spremenljivki ξ :

$$\frac{\partial}{\partial \xi}\left(\frac{\ln \xi}{\xi^s}\right) = \frac{1}{\xi}\cdot\frac{1}{\xi^s} - \frac{s\ln\xi}{\xi^{s+1}} = \frac{1-s\ln\xi}{\xi^{s+1}}.$$

Z odvodom pokažemo, da je $\frac{\ln \xi}{\xi}$ padajoča natanko tedaj, ko je

$$1 - s\ln\xi < 0,$$

oziroma ko je $\xi > e^{\frac{1}{s}}$.

Velja tudi ocena $e^{\frac{1}{s}} \le e \le 3$. Potem je za $\xi \ge 3$ funkcija zagotovo padajoča. Izberimo $\xi \ge 3$ in naj bosta u in v takšni naravni števili, da velja $3 \le u \le v$. Po *izreku 4.3* in *izreku 3.3* je

$$\left|\sum_{a=u}^{v} \frac{\chi(a) \cdot \ln a}{a^s}\right| \le \frac{h}{2} \cdot \frac{\ln u}{u^s} \le \frac{h}{2} \cdot \frac{\ln u}{u}.$$

Ker $\frac{\ln u}{u} \to 0$, ko $u \to \infty$, sledi

$$\left|\sum_{a=u}^{v} \frac{\chi(a) \cdot \ln a}{a^s}\right| \to 0 \quad \text{za dovolj velike } u \text{ in } v.$$

Po *Cauchyevem kriteriju (izrek 1.3)* sledi enakomerna konvergenca.

Omejenost $\left|\sum_{a=1}^{\infty} \frac{\chi(a)\cdot\ln a}{a^s}\right|$ pokažemo s pomočjo *izreka 4.4* in *izreka 4.3*

$$\left|\sum_{a=3}^{v} \frac{\chi(a) \cdot \ln a}{a^s}\right| \le \frac{h}{2} \cdot \frac{\ln 3}{3}, \text{kar da } \left|\sum_{a=3}^{\infty} \frac{\chi(a) \cdot \ln a}{a^s}\right| \le \frac{h}{2} \cdot \frac{\ln 3}{3},$$

$$\left|\sum_{a=1}^{2} \frac{\chi(a) \cdot \ln a}{a^s}\right| = \left|\frac{\chi(1) \cdot \ln 1}{1^s} + \frac{\chi(2) \cdot \ln 2}{2^s}\right| = \left|\frac{\chi(2) \cdot \ln 2}{2^s}\right| \le \frac{\ln 2}{2}.$$

Upoštevajoč obe oceni pridemo do željenega rezultata.

$$\begin{aligned}\left|\sum_{a=1}^{\infty} \frac{\chi(a) \cdot \ln a}{a^s}\right| &= \left|\sum_{a=1}^{2} \frac{\chi(a) \cdot \ln a}{a^s} + \sum_{a=3}^{\infty} \frac{\chi(a) \cdot \ln a}{a^s}\right| \le \\ &\le \frac{\ln 2}{2} + \frac{h}{2} \cdot \frac{\ln 3}{3} < \frac{1}{2} + \frac{h}{2} \le h.\end{aligned}$$

□

V nadaljevanju bomo potrebovali poleg $L'(s, \chi)$ še funkcijsko vrsto

$$\sum_{a=1}^{\infty} \frac{\chi(a) \cdot \mu(a)}{a^s},$$

kjer je μ *Möbiusova funkcija*, definirana v uvodu.

Izrek 4.9 *Naj bo $s > 1$ in $s \in R$. Potem je vrsta*

$$\sum_{a=1}^{\infty} \frac{\chi(a) \cdot \mu(a)}{a^s}$$

absolutno konvergentna.

Dokaz: Trivialno; ker je $|\mu(a)| \leq 1$, je

$$\left|\frac{\chi(a)\cdot\mu(a)}{a^s}\right| \leq \frac{1}{a^s}.$$

Vrsta $\sum_{a=1}^{\infty}\frac{1}{a^s}$ konvergira za $s>1$, od kod sledi konvergenca vrste

$$\sum_{a=1}^{\infty}\left|\frac{\chi(a)\cdot\mu(a)}{a^s}\right|.$$

□

Lema 4.10 *Naj bo $s>1$. Potem je*

$$\sum_{b=1}^{\infty}\frac{\chi(b)}{b^s}\cdot\sum_{a=1}^{\infty}\frac{\chi(a)\cdot\mu(a)}{a^s}=\sum_{l=1}^{\infty}\sum_{a\cdot b=l}\frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s}$$

absolutno konvergentna vrsta.

Dokaz:

(1) Dokažimo, da je $\sum_{l=1}^{\infty}\sum_{a\cdot b=l}\frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s}$ absolutno konvergentna vrsta.

Zaradi trikotniške neenakosti zadostuje za konvergenco vrste $\sum_{l=1}^{\infty}\left|\sum_{a\cdot b=l}\frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s}\right|$ pokazati konvergenco $\sum_{l=1}^{\infty}\sum_{a\cdot b=l}\left|\frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s}\right|$.

Definirajmo

$$\widetilde{C}_l=\sum_{a\cdot b=l}|\chi(b)|\cdot|\chi(a)\cdot\mu(a)|$$

in pokažimo, da je $\sum_{l=1}^{\infty}\frac{\widetilde{C}_l}{l^s}$ konvergentna vrsta.

Naj bo $L\in\mathbb{N}$ in naj velja

$$\begin{aligned}
\widetilde{S}_c(L) &= \sum_{l=1}^{L}\frac{\widetilde{C}_l}{l^s},\\
\widetilde{S}_a(L) &= \sum_{a=1}^{L}\frac{|\chi(a)\cdot\mu(a)|}{a^s},\\
\widetilde{S}_b(L) &= \sum_{a=1}^{L}\frac{|\chi(b)|}{b^s}.
\end{aligned}$$

Pokažimo, da je $\lim_{L\to\infty}\widetilde{S}_c(L)=\lim_{L\to\infty}\widetilde{S}_a(L)\cdot\lim_{L\to\infty}\widetilde{S}_b(L)$.

Limiti na desni obstajata, saj sta to dve konvergentni vrsti *(izrek 4.1* in *izrek 4.9*).

Vsaka vrednost $l, l \in \mathbb{N}$ razpade na produkte ab,kjer sta $a, b \in \mathbb{N}$. Preoblikujmo $\widetilde{S}_c(L) = T_1(L) + T_2(L) + T_3(L)$, kjer je

$$
\begin{aligned}
T_1(L) &= \sum_{l=1}^{L} \sum_{\substack{a\cdot b=l \\ a,b<\sqrt{L}}} \left| \frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s} \right| \\
T_2(L) &= \sum_{l=1}^{L} \sum_{\substack{a\cdot b=l \\ 1\le a\le\sqrt{L} \\ b>\sqrt{L}}} \left| \frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s} \right| \\
T_3(L) &= \sum_{l=1}^{L} \sum_{\substack{a\cdot b=l \\ 1\le b\le\sqrt{L} \\ a>\sqrt{L}}} \left| \frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s} \right|
\end{aligned}
$$

Očitno je $T_1 = \widetilde{S_a}(\sqrt{L}) \cdot \widetilde{S}_b(\sqrt{L})$.

Ko $L \to \infty$, gre T_1 k vrednostim produkta

$$
\sum_{b=1}^{\infty} \frac{|\chi(b)|}{b^s} \cdot \sum_{a=1}^{\infty} \frac{|\chi(a)\cdot\mu(a)|}{a^s}.
$$

Ocenimo še vsoti T_2 in T_3.

$$
T_2 \le \sum_{1\le a\le\sqrt{L}} \frac{|\chi(a)\cdot\mu(a)|}{a^s} \cdot \sum_{\sqrt{L}<b} \frac{|\chi(b)|}{b^s} \le \left(\sum_{a=1}^{\infty} \frac{|\chi(a)\cdot\mu(a)|}{a^s} \right) \cdot \left(\sum_{\sqrt{L}<b} \frac{|\chi(b)|}{b^s} \right)
$$

Ker je $\sum_{b=1}^{\infty} \frac{|\chi(b)|}{b^s}$ konvergentna vrsta (*izrek 4.1*), je ostanek

$$
\lim_{L\to\infty} \sum_{\sqrt{L}<b} \frac{|\chi(b)|}{b^s} = 0.
$$

Prvi faktor $\sum_{a=1}^{\infty} \frac{|\chi(a)\cdot\mu(a)|}{a^s}$ je konvergentna vrsta (*izrek 4.9*)

Torej je $\lim_{L\to\infty} T_2(L) = 0$.

Podobno velja tudi za T_3.

$$
T_3 \le \sum_{a=1}^{\infty} \frac{|\chi(a)|}{a^s} \cdot \sum_{a>\sqrt{L}} \frac{|\chi(a)\cdot\mu(a)|}{a^s} \quad \text{in}
$$

Ker je $\sum_{a=1}^{\infty} \frac{|\chi(a)\cdot\mu(a)|}{a^s}$ konvergentna, je limita ostanka

$$\lim_{L\to\infty} \sum_{a>\sqrt{L}} \frac{|\chi(a)\cdot\mu(a)|}{a^s} = 0,$$

$\sum_{a=1}^{\infty} \frac{|\chi(a)|}{a^s}$ pa konvergira. Zato sledi $\lim_{L\to\infty} T_3(L) = 0$.

Pokazali smo $\lim_{L\to\infty} \widetilde{S}_c(L) = \lim_{L\to\infty} \widetilde{S}_a(L) \cdot \lim_{L\to\infty} \widetilde{S}_b(L)$. Produkt dveh absolutno konvergentnih vrst je absolutno konvergentna vrsta, kar pomeni, da je $\sum_{l=1}^{\infty} \sum_{a\cdot b=l} \frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s}$ absolutno konvergentna vrsta.

(2) Podobno pokažimo, da je vrednost vsote $\sum_{l=1}^{\infty} \sum_{a\cdot b=l} \frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s}$ enaka produktu konvergentnih vrst $\sum_{b=1}^{\infty} \frac{\chi(b)}{b^s} \cdot \sum_{a=1}^{\infty} \frac{\chi(a)\cdot\mu(a)}{a^s}$.

Vsi členi, pri katerih je produkt $a \cdot b$ iste vrednosti, gredo skupaj; npr.: $a \cdot b = l$. Ker sta $a, b \in \{1, 2, ...\infty\}$, je tudi njun produkt $l \in \{1, 2, ...\infty\}$.

Podobno kot v (1) zapišemo vsoto na desni kot

$$\sum_{c=1}^{\infty} \frac{c_l}{l^s}, \qquad \text{kjer je } \ l = a \cdot b,$$

$$c_l = \sum_{a\cdot b=l} \chi(b)\cdot\chi(a)\cdot\mu(a) = \sum_{b|l} \chi(b)\cdot\chi(\frac{l}{b})\cdot\mu(\frac{l}{b}).$$

Naj bo $L \in \mathbb{N}$ in definirajmo končne delne vsote

$$\begin{aligned} S_c(L) &= \sum_{l=1}^{L} \frac{c_l}{l^s}, \\ S_a(L) &= \sum_{a=1}^{L} \frac{\chi(a)\cdot\mu(a)}{a^s}, \\ S_b(L) &= \sum_{a=1}^{L} \frac{\chi(b)}{b^s}. \end{aligned}$$

Pokažimo, da $S_c(L) \to S_a(L) \cdot S_b(L)$, ko $L \to \infty$.

Problikujmo $S_c(L) = T_1(L) + T_2(L) + T_3(L)$, kjer je

$$\begin{aligned}
T_1(L) &= \sum_{l=1}^{L} \sum_{\substack{a\cdot b=l \\ a,b<\sqrt{L}}} \frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s} \\
T_2(L) &= \sum_{l=1}^{L} \sum_{\substack{a\cdot b=l \\ 1\le a\le\sqrt{L} \\ b>\sqrt{L}}} \frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s} \\
T_3(L) &= \sum_{l=1}^{L} \sum_{\substack{a\cdot b=l \\ 1\le b\le\sqrt{L} \\ a>\sqrt{L}}} \frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s}
\end{aligned}$$

Opazimo,da je

$$T_1 = S_a(\sqrt{L})\cdot S_b(\sqrt{L}).$$

Ko $L\to\infty$, gre T_1 k vrednostim produkta

$$\sum_{b=1}^{\infty}\frac{\chi(b)}{b^s}\cdot\sum_{a=1}^{\infty}\frac{\chi(a)\cdot\mu(a)}{a^s}.$$

Ker je $\sum_{b=1}^{\infty}\frac{\chi(b)}{b^s}$ (absolutno) konvergentna vrsta (*izrek 4.1*), je ostanek

$$\lim_{L\to\infty}\sum_{\sqrt{L}<b}\frac{\chi(b)}{b^s} = 0.$$

Prvi faktor $\sum_{a=1}^{\infty}\frac{\chi(a)\cdot\mu(a)}{a^s}$ je (absolutno) konvergentna vrsta (*izrek 4.9*)

Torej je $\lim_{L\to\infty} T_2(L) = 0$.

Podobno velja tudi za T_3.

$$T_3 \le \sum_{a=1}^{\infty}\frac{\chi(a)}{a^s}\cdot\sum_{a>\sqrt{L}}\frac{\chi(a)\cdot\mu(a)}{a^s} \qquad \text{in}$$

ker je $\sum_{a=1}^{\infty}\frac{\chi(a)\cdot\mu(a)}{a^s}$ konvergentna, je limita ostanka

$$\lim_{L\to\infty}\sum_{a>\sqrt{L}}\frac{\chi(a)\cdot\mu(a)}{a^s} = 0,$$

$\sum_{a=1}^{\infty}\frac{|\chi(a)|}{a^s}$ pa konvergira. Zato sledi $\lim_{L\to\infty} T_3(L) = 0$.

Pokazali smo $\lim_{L\to\infty} S_c(L) = \lim_{L\to\infty} S_a(L) \cdot \lim_{L\to\infty} S_b(L)$, kar pomeni, da je (2) dokazano. $\square$

Izrek 4.11 *Naj bo* $s > 1, s \in \mathbb{R}$. *Potem je*

$$L(s,\chi) \cdot \sum_{a=1}^{\infty} \frac{\chi(a)\cdot\mu(a)}{a^s} = 1.$$

(`Opomba` : *to med drugim pomeni, da je* $L(s,\chi) \neq 0$.)

Dokaz: Pokazali smo že, da je $L(s,\chi)$ absolutno konvergentna za $s > 1$, in da je $\sum_{a=1}^{\infty} \frac{\chi(a)\cdot\mu(a)}{a^s}$ absolutno konvergentna za $s > 1$.

Uporabimo *lemo 4.10*

$$\sum_{b=1}^{\infty} \frac{\chi(b)}{b^s} \cdot \sum_{a=1}^{\infty} \frac{\chi(a)\cdot\mu(a)}{a^s} = \sum_{l=1}^{\infty} \sum_{a\cdot b=l}^{\infty} \frac{\chi(b)\cdot\chi(a)\cdot\mu(a)}{b^s\cdot a^s} = \sum_{l=1}^{\infty}\left(\frac{\chi(l)}{l^s}\sum_{a|l}\mu(a)\right) = 1.$$

$\square$ Dirichletove L-vrste lahko zapišemo tudi v obliki neskončnih produktov. Še prej pa bomo potrebovali naslednjo lemo.

Lema 4.12 ***(Eulerjeva produktna formula)****: Naj bo* $f : \mathbb{N} \to \mathbb{C}$ *multiplikativna funkcija(velja* $f(a\cdot b) = f(a)f(b)$,*za* $D(a,b) = 1, a, b \in \mathbb{N}$), *in* $F(s) = \sum_{a=1}^{\infty} \frac{f(a)}{a^s}$. *Če je* $s \in \mathbb{R}$, *da* $F(s)$ *absolutno konvergira, velja*

$$F(s) = \prod_{p\in\mathbb{P}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + ... + \frac{f(p^a)}{p^{as}} + ...\right).$$

`Opomba`: *Naj bo* $f(a) = 1$ *za vsak* a. *Če je* $s > 1$, *imenujemo funkcijo*

$$\zeta(s) = \sum_{a=1}^{\infty} \frac{1}{a^s} = \prod_{p\in\mathbf{P}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + ... + \frac{1}{p^{as}} + ...\right)$$

Riemannova Zeta-funkcija.

Dokaz: Za vsako praštevilo p velja ocena

$$1 + \frac{|f(p)|}{p^s} + \frac{|f(p^2)|}{p^{2s}} + ... + \frac{|f(p^a)|}{p^{as}} + ... \leq \sum_{a=1}^{\infty} \frac{|f(a)|}{a^s} < \infty.$$

Zaradi lastnosti Cauchyevega produkta ([3],str.362) lahko opazimo, da za $s > 1$

$$\left(1 + \frac{f(2)}{2^s} + \frac{f(2^2)}{2^{2s}} + ...\right) \cdot \left(1 + \frac{f(3)}{3^s} + \frac{f(3^2)}{3^{2s}} + ...\right) = \sum_{a \in A}^{\infty} \frac{f(a)}{a^s},$$

kjer je množico $A = \{2^\alpha 3^\beta; \alpha, \beta \in \mathbb{N}_0\} = \{1, 2, 3, 4, 6, 8, 9, 12, ...\}$. Uporabili smo multiplikativnost funkcije f; $f(2^\alpha 3^\beta) = f(2^\alpha) \cdot f(3^\beta)$.

Naj bo ξ poljubno realno število. Definirajmo

$$f_\xi(a) = \begin{cases} a & \text{če} \quad \text{je } a \text{število, ki ima v kanoničnem razcepu le praštevila } p \leq \xi \\ 0, & \text{sicer} \end{cases} .$$

Potem z večkratno uporabo izreka o lastnostih *Cauchyevega produkta* ([3],str.362) sledi

$$\prod_{p \leq \xi} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \frac{f(p^3)}{p^{3s}} + ...\right) = \sum_{a=1}^{\infty} \frac{f_\xi(a)}{a^s}.$$

Pokažimo, da

$$\lim_{\xi \to \infty} \sum_{a=1}^{\infty} \frac{f_\xi(a)}{a^s} = \sum_{a=1}^{\infty} \lim_{\xi \to \infty} \frac{f_\xi(a)}{a^s} = F(s).$$

Uporabimo *Weierstrassov M-test (2.oblika)* za vrednosti $M_a = \frac{f(a)}{a^s}$ in zaporedje funkcij $\frac{f_\xi(a)}{a^s}$. Upoštevajmo, da je

$$\lim_{\xi \to \infty} f_\xi(a) = f(a)$$

za vsak fiksni a. Odtod pa sledi

$$\prod_{p \in \mathbb{P}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + ... + \frac{f(p^a)}{p^{as}} + ...\right) = \lim_{\xi \to \infty} \sum_{a=1}^{\infty} \frac{f_\xi(a)}{a^s} = F(s).$$

$\square$

Izrek 4.13 *Naj bo $s > 1$. Potem velja*

$$\prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^s}\right) = \frac{1}{L(s, \chi)}.$$

Dokaz: Uporabimo *lemo 4.12* za vrednosti $f = \chi$ in $F(s) = L(s, \chi)$;

Vemo že, da je $L(s, \chi)$ je absolutno konvergentna za $s > 1$.

$$\prod_{p \in \mathbb{P}} \left(1 - \frac{f(p)}{p^s}\right) = \frac{1}{F(s)},$$

odkod sledi

$$\prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^s}\right) = \frac{1}{L(s, \chi)}. \qquad \square$$

Izrek 4.14 *Naj bo $s \in R, s > 1$ in naj bo $\Lambda : \mathbb{N} \to \mathbb{R}$ von Mongoldtova funkcija. Potem velja*

(i)

$$\sum_{a=1}^{\infty} \frac{\chi(a) \cdot \Lambda(a)}{a^s} = -\frac{L'(s, \chi)}{L(s, \chi)} \quad \textit{in}$$

(ii)

$$\sum_{a=1}^{\infty} \frac{\chi(a) \cdot \Lambda(a)}{a^s} \quad \textit{je absolutno konvergentna.}$$

Dokaz:

(i) Ker je $|\chi(a) \cdot \Lambda(a)| \leq \ln a$, sledi očitna absolutna konvergenca

$$\sum_{a=1}^{\infty} \frac{\chi(a) \cdot \Lambda(a)}{a^s}\ , \ \text{ saj je}$$

$$\sum_{a=1}^{\infty} \frac{|\chi(a) \cdot \Lambda(a)|}{a^s} \leq \sum_{a=1}^{\infty} \frac{\ln a}{a^s},$$

za slednjo pa že vemo, da konvergira za $s > 1$ (*izrek* 4.6).

(ii) Po *izreku 1* v uvodu je $\ln l = \sum_{a|l} \Lambda(a)$.

Naj bo $s > 1$.

$$L(s, \chi) \cdot \sum_{a=1}^{\infty} \frac{\chi(a) \cdot \Lambda(a)}{a^s} = \sum_{b=1}^{\infty} \frac{\chi(b)}{b^s} \cdot \sum_{a=1}^{\infty} \frac{\chi(a) \cdot \Lambda(a)}{a^s}.$$

Pomagajmo si z *lemo 4.10.* Vlogo Mobiusove funkcije μ prevzame zdaj von Mongoldtova funkcija Λ.

(komentar: to lahko storimo, saj je Λ prav tako multiplikativna. Na mestu, kjer ugotavljamo konvergenco T_2 in T_3 potrebujemo konvergenco vrste $\sum_{a=1}^{\infty}\frac{\Lambda(a)}{a^s}$, kjer je $s>1$.

Velja $\sum_{a=1}^{\infty}\frac{\Lambda(a)}{a^s} < \sum_{a=1}^{\infty}\frac{\ln a}{a^s}$. Po *lemi 4.5* je vrsta na desni konvergentna, zato je po primerjalnem kriteriju ([6], stran 295) konvergentna tudi $\sum_{a=1}^{\infty}\frac{\Lambda(a)}{a^s}$).

Zaradi tega velja

$$\begin{aligned}\sum_{b=1}^{\infty}\frac{\chi(b)}{b^s}\cdot\sum_{a=1}^{\infty}\frac{\chi(a)\cdot\Lambda(a)}{a^s} &= \sum_{l=1}^{\infty}\sum_{a\cdot b=l}\frac{\chi(b)\cdot\chi(a)\cdot\Lambda(a)}{b^s\cdot a^s} = \\ &= \sum_{l=1}^{\infty}\frac{\chi(l)}{l^s}\sum_{a|l}\Lambda(a) = \sum_{l=1}^{\infty}\frac{\chi(l)}{l^s}\ln l.\end{aligned}$$

Po *izreku 4.6* je

$$\sum_{l=1}^{\infty}\frac{\chi(l)}{l^s}\ln l = -L'(s,\chi),$$

oziroma

$$L(s,\chi)\cdot\sum_{a=1}^{\infty}\frac{\chi(a)\cdot\Lambda(a)}{a^s} = -L'(s,\chi).$$

□

Izrek 4.15 *Naj pada $s\downarrow 1$. Potem je*

$$\lim_{s\downarrow 1}\frac{L'(s,\chi_0)}{L(s,\chi_0)} \to -\infty.$$

Dokaz: Uporabimo *definicijo 3.2* osnovnega značaja χ_0,

$$-\frac{L'(s,\chi_0)}{L(s,\chi_0)} = \sum_{\substack{a=1\\ D(a,k)=1}}^{\infty}\frac{\chi_0(a)\cdot\Lambda(a)}{a^s} + \sum_{\substack{a=1\\ D(a,k)>1}}^{\infty}\frac{\chi_0(a)\cdot\Lambda(a)}{a^s}.$$

Druga vrsta je enaka 0 ($\chi_0(a)=0$, če $D(a,k)>1$), prvo pa zapišimo malce drugače.

$$\sum_{\substack{a=1\\ D(a,k)=1}}^{\infty}\frac{\chi_0(a)\cdot\Lambda(a)}{a^s} = \sum_{\substack{a=1\\ D(a,k)=1}}^{\infty}\frac{\Lambda(a)}{a^s} = \sum_{a=1}^{\infty}\frac{\Lambda(a)}{a^s} - \sum_{\substack{a=1\\ D(a,k)>1}}^{\infty}\frac{\Lambda(a)}{a^s}.$$

(i) Kaj predstavlja $\sum_{\substack{a=1 \\ D(a,k)>1}}^{\infty} \frac{\Lambda(a)}{a^s}$?

Za vsa števila a, oblike $a = \prod_{i=1}^{r} p_i^{m_i}$, kjer je $r > 1$,velja $\Lambda(a) = 0$.

Če je $D(a,k) > 1$, obstaja praštevilo p, da velja $p \mid k, \quad p \mid a$.

Potem je

$$\frac{\Lambda(a)}{a^s} = \frac{\ln p}{p^{ms}},$$

če je $a = p^{ms}$, kjer je $m \in \mathbb{N}_0$.

Upoštevajmo, da lahko a izberemo iz množice naravnih števil. Vse neničelne člene v vrsti $\sum_{\substack{a=1 \\ D(a,k)>1}}^{\infty} \frac{\Lambda(a)}{a^s}$ zapišemo potem kot $\sum_{p \in P} \frac{\Lambda(p^m)}{p^{ms}}$, kjer je $m \in \mathbb{N}$, vrsta pa teče le po tistih praštevilih p, ki delijo k. Velja

$$\sum_{\substack{a=1 \\ D(a,k)>1}}^{\infty} \frac{\Lambda(a)}{a^s} = \sum_{\substack{p \in P \\ p \mid k \\ m \in \mathbb{N}}} \frac{\Lambda(p^m)}{p^{ms}} = \sum_{p \mid k} \left(\sum_{m=1}^{\infty} \frac{\ln p}{p^{ms}} \right).$$

Ker je

$$\begin{aligned} \sum_{m=1}^{\infty} \frac{1}{(p^m)^s} &= \frac{1}{p^s} + \left(\frac{1}{p^s}\right)^2 + \left(\frac{1}{p^s}\right)^3 + \ldots = \\ &= \frac{1}{p^s} \left(\frac{1}{1 - \frac{1}{p^s}} \right) = \frac{1}{p^s} \cdot \frac{p^s}{p^s - 1} = \frac{1}{p^s - 1}, \end{aligned}$$

sledi

$$\sum_{\substack{a=1 \\ D(a,k)>1}}^{\infty} \frac{\Lambda(a)}{a^s} = \sum_{p \mid k} \left(\ln p \sum_{m=1}^{\infty} \frac{1}{(p^m)^s} \right) = \sum_{p \mid k} \frac{\ln p}{p^s - 1}.$$

$\lim_{s \downarrow 1} \sum_{p \mid k} \frac{\ln p}{p^s - 1} = \sum_{p \mid k} \frac{\ln p}{p - 1} < \infty$, saj obstaja končno mnogo praštevil, ki delijo k.

(ii) Pokažimo še: $\lim_{s \downarrow 1} \sum_{a=1}^{\infty} \frac{\Lambda(a)}{a^s} = \infty$.

Vrsta

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

je divergentna ([1],str.92). Potem je tudi vrsta $\sum_{p\in P} \frac{\ln p}{p}$ divergentna (po primerjalnem kriteriju ([6], stran 295) in potem je divergentna tudi $\sum_{a=1} \frac{\Lambda(a)}{a}$.

Torej za vsak $\omega > 0$ obstaja $b = b(\omega)$, da velja

$$\sum_{a=1}^{b} \frac{\Lambda(a)}{a} > \omega.$$

Za $1 < s < 1 + \varepsilon(\omega)$ velja $\sum_{a=1}^{b} \frac{\Lambda(a)}{a^s} > \omega$.

Odtod sledi

$$\sum_{a=1}^{\infty} \frac{\Lambda(a)}{a^s} > \omega.$$

$\square$

Izrek 4.16 *Naj bo $r \in (0,1)$ in $\varphi \in \mathbb{R}$. Tedaj velja*

$$(1-r)^3 \cdot \left|1 - re^{i\varphi}\right|^4 \cdot \left|1 - re^{2i\varphi}\right|^2 < 1.$$

Dokaz: Velja ocena

$$2\cos\varphi + \cos 2\varphi = 2\cos\varphi + 2\cos^2\varphi - 1 = -\frac{3}{2} + 2\left(\cos\varphi + \frac{1}{2}\right)^2 \geq -\frac{3}{2}$$

in

$$\left|1 - re^{i\varphi}\right|^2 > 0, \qquad \left|1 - re^{2i\varphi}\right|^2 > 0.$$

Upoštevajmo, da je geometrijska sredina treh pozitivnih števil manjša ali enaka od aritmetične sredine teh treh števil.($\diamondsuit$)

Z elementarnim računom

$$\begin{aligned}
&\left|1 - re^{i\varphi}\right|^4 \cdot \left|1 - re^{2i\varphi}\right|^2 = \left|1 - re^{i\varphi}\right|^2 \cdot \left|1 - re^{i\varphi}\right|^2 \cdot \left|1 - re^{2i\varphi}\right|^2 = \\
&= (1 - 2r\cos\varphi + r^2) \cdot (1 - 2r\cos\varphi + r^2) \cdot (1 - 2r\cos 2\varphi + r^2) \leq \\
&\leq \left(1 - \frac{2}{3}r(2\cos\varphi + \cos 2\varphi) + r^2\right)^3 \leq \left(1 + r + r^2\right)^3 < \left(\frac{1}{1-r}\right)^3
\end{aligned}$$

pokažemo željeno. Prva neenakost velja zaradi ($\diamondsuit$), zadnja neenakost pa velja, ker so prvi trije členi geometrijske vrste manjši od vsote te geometrijske vrste. $\square$

Izrek 4.17 *Naj bo $s > 1$. Za poljubni značaj χ tedaj velja*

$$(L(s,\chi_0))^3 \cdot |L(s,\chi)|^4 \cdot \left|L(s,\chi^2)\right|^2 \geq 1.$$

Dokaz: Po *izreku 3.6* je χ^2 značaj. Splošno velja, da je χ kompleksna funkcija. Vstavimo

$$\begin{aligned} \chi(p) &= e^{i\varphi}, \\ r &= \frac{1}{p^s} \end{aligned}$$

v prejšnji *izrek 4.16.*

Po *izreku 4.13* velja

$$\frac{1}{(L(s,\chi_0))^3} \cdot \frac{1}{|L(s,\chi)|^4} \cdot \frac{1}{|L(s,\chi^2)|^2} = \prod_{p\in\mathbb{P}} \left(1 - \frac{\chi_0(p)}{p^s}\right)^3 \cdot \left|1 - \frac{\chi(p)}{p^s}\right|^4 \cdot \left|1 - \frac{\chi^2(p)}{p^s}\right|^2.$$

1. Naj velja $p \nmid k$.

   Produkt je sestavljen iz faktorjev $\left(1 - \frac{\chi_0(p)}{p^s}\right)^3 \cdot \left|1 - \frac{\chi(p)}{p^s}\right|^4 \cdot \left|1 - \frac{\chi^2(p)}{p^s}\right|^2$, ki ustrezajo pogojem *izreka 3.12.* Za neko praštevilo p je faktor $\left(1 - \frac{\chi_0(p)}{p^s}\right)^3$ potenca nekega realnega števila iz intervala $(0,1)$. Označimo jo z $(1-r)^3$, kjer je $r \in (0,1)$. V faktorju $\left|1 - \frac{\chi(p)}{p^s}\right|^4$ je število $\frac{\chi(p)}{p^s}$ v splošnem iz množice $\mathbb{C}$, zato ga lahko označimo z $|1 - re^{i\varphi}|^4$. Podobno velja tudi za $\left|1 - \frac{\chi^2(p)}{p^s}\right|^2$, ki ga označimo z $|1 - re^{2i\varphi}|^2$. *Izrek 4.16* pravi, da je

   $$\prod_{p\in\mathbb{P}} \left(1 - \frac{\chi_0(p)}{p^s}\right)^3 \cdot \left|1 - \frac{\chi(p)}{p^s}\right|^4 \cdot \left|1 - \frac{\chi^2(p)}{p^s}\right|^2 < 1.$$

2. Če $p \mid k$, je vsak faktor enak 1 (definicija značaja, lastnost *(i)*) in velja $1 = 1$.

   Torej velja $(L(s,\chi_0))^3 \cdot |L(s,\chi)|^4 \cdot |L(s,\chi^2)|^2 \geq 1$. □

Izrek 4.18 *Za vsak značaj χ tretje vrste je $L(s,\chi) \neq 0$.*

Dokaz: Spomnimo se, da je χ je značaj tretje vrste, če je v zalogi vrednosti funkcije χ vsaj eno število $\chi(n) \in \mathbb{C} - \mathbb{R}$. Zato χ^2 ni osnovni značaj. Če bi bil $\chi^2 = \chi_0$, bi morala biti χ realna funkcija, kar pa ni, saj je tretje vrste.

Po *izreku 4.4* χ^2 kot tak enakomerno konvergira za $s \geq 1$ in po oceni v istem izreku velja

$$\left|\sum_{a=u}^{v} \frac{\chi^2(a)}{a^s}\right| \leq \frac{h}{2u} \qquad \text{za } v \geq u \geq 0.$$

Pošljimo $v \to \infty$ in vstavimo $u = 1$.

$$\left|\sum_{a=1}^{\infty} \frac{\chi^2(a)}{a^s}\right| \leq \frac{\varphi(k)}{2u} < \varphi(k).$$

Ugotovili smo, da je

$$L(s, \chi^2) < \varphi(k) \text{ za vse } s > 1.$$

Po *izreku 4.17* je za $s > 1$

$$(L(s,\chi_0))^3 \cdot |L(s,\chi)|^4 \cdot \left|L(s,\chi^2)\right|^2 \geq 1,$$

$$|L(s,\chi)| \geq \sqrt[4]{\frac{1}{(L(s,\chi_0))^3} \cdot \frac{1}{|L(s,\chi^2)|^2}}.$$

Velja $\sum_{a=1}^{\infty} \frac{1}{a^s} \leq \int\limits_1^{\infty} \frac{da}{a^s}$.

Če prištejemo 1 na desni, dobimo $\sum_{a=1}^{\infty} \frac{1}{a^s} < 1 + \int\limits_1^{\infty} \frac{da}{a^s}$, kar uporabimo v naslednji oceni. Ker je

$$\begin{aligned} L(s,\chi_0) &= \sum_{a=1}^{\infty} \frac{\chi_0(a)}{a^s} = \sum_{\substack{a=1 \\ D(a,k)=1}}^{\infty} \frac{1}{a^s} \leq \sum_{a=1}^{\infty} \frac{1}{a^s} < 1 + \int\limits_1^{\infty} \frac{da}{a^s} = \\ &= 1 + \frac{1}{s-1} = \frac{s}{s-1} < \frac{2}{s-1}, \end{aligned}$$

sledi za $s \in (1,2)$

$$L(s,\chi) \geq \frac{1}{(L(s,\chi_0))^{\frac{3}{4}}} \cdot \frac{1}{|L(s,\chi^2)|^{\frac{2}{4}}} > \left(\frac{s-1}{2}\right)^{\frac{3}{4}} \cdot \frac{1}{\sqrt{\varphi(k)}} > \frac{(s-1)^{\frac{3}{4}}}{2\sqrt{\varphi(k)}} \geq 0.$$

Pokazali smo, da je $L(s,\chi) > 0$ za $s > 1$. Pokažimo še, da je

$$L(1,\chi) = 0$$

za neki značaj(mod k) tretjega reda. Potem je za $\eta \geq 1$ po *izreku 4.7* in *izreku 4.8*

$$L'(\eta,\chi) \text{ zvezna funkcija.}$$

Naj bo $s > 1$.

$$|L(s,\chi)| = |L(s,\chi) - L(1,\chi)| = \left| \int_1^s L'(\eta,\chi) d\eta \right| < \varphi(k) \cdot (s-1)\,.$$

Za oceno smo uporabili neenakost iz *izreka 3.6.* Odtod sledi, da za vsak s, $1 < s < 2$, velja $(s-1)^{\frac{1}{4}} > \frac{1}{2 \cdot h^{\frac{3}{2}}}$. Ta izraz ne drži za $s = 1 + \frac{1}{16h^6}$, kar pomeni, da je predpostaka $L(s,\chi) = 0$ napačna. □

Izrek 4.19 *Za vsak značaj χ druge vrste je*

$$L(s,\chi) \neq 0.$$

Komentar: to je hkrati tudi najzahtevnejše mesto dokaza. Dirichlet dokaže izrek v izvirni obliki s pomočjo teorije razrednih števil kvadratičnih form (glej [4],str. 237). Kar sledi v nadaljevanju so njegove ideje, le sam dokaz je zapisan bolj eksplicitno in je bolj direkten.

Dokaz: Najprej pokažimo nenegativnost $L(1,\chi)$.

$L(1,\chi) \geq 0$, saj je po *izreku 4.13* $L(s,\chi) \geq 0$ za vsak $s > 1$. Po *izreku 4.4* je $L(s,\chi)$ zvezna za $s \geq 1$. Vsaka funkcija, ki je nenegativna na $(1,\infty)$ in zvezna na $[1,\infty)$, je tudi nenegativna na $[1,\infty)$, zato velja

$$L(1,\chi) \geq 0.$$

Pokazati strogo neenakost pa je dosti težje. V ta namen vpeljimo funkcijo f kot

$$f(a) = \sum_{d|a} \chi(d);$$

oziroma kot vsoto vrednosti χ, kjer χ deluje na vse delitelje a.

Primera:

$$\begin{aligned} f(7) &= \chi(1) + \chi(7), \\ f(10) &= \chi(1) + \chi(2) + \chi(5) + \chi(10). \end{aligned}$$

Za vsak $l \geq 0$ je

$$f(p^l) = \chi(1) + \chi(p) + \chi(p^2) + ... + \chi(p^l).$$

Ker je χ druge vrste, zavzame $\chi(p)$ eno izmed vrednosti $1, -1, 0$.

Vrednosti $f(p^l)$ so odisne od $\chi(p)$, pa tudi od eksponenta l. Upoštevajmo še $\chi(p^2) = \chi(p) \cdot \chi(p)$ in z induktivnim sklepanjem pridemo do

$$\chi(p^l) = (\chi(p))^l.$$

Potem velja

$$\begin{aligned} f(p^l) &= \begin{cases} 1 + 0 + 0 + ... + 0 & \text{če } \chi(p) = 0 \\ 1 + 1 + 1 + ... \geq 1 & \text{če } \chi(p) = 1 \\ 1 - 1 - 1 - 1 + ... & \text{če } \chi(p) = -1 \end{cases} = \\ &= \begin{cases} 1 & \text{če } \chi(p) = 0 \\ \geq 1 & \text{če } \chi(p) = 1 \\ 0 & \text{če } \chi(p) = -1 \text{ in } l \equiv 1 (\text{mod } 2) \\ 1 & \text{če } \chi(p) = -1 \text{ in } l \equiv 0 (\text{mod } 2) \end{cases}. \end{aligned}$$

Odtod sledi ocena

$$f(p^l) \geq \begin{cases} 0, & \text{vedno} \\ 1, & \text{če } l \equiv 0 (\text{mod } 2) \end{cases}.$$

Izberimo si zdaj tuji naravni števili a_1 in a_2, $D(a_1, a_2) = 1$.

Definirajmo preslikavo $\Psi : (d_1, d_2) \longmapsto d_1 d_2$, kjer so $d_1$delitelji števila $a_1$in d_2 delitelji števila a_2. Ta preslikava je injektivna, saj iz $d_1 d_2 = d_1' d_2'$ sledi $d_1 = d_1'$ in $d_2 = d_2'$.

Vseh deliteljev števila $a_1 = \prod_{i=1}^{r_1} p_i^{\alpha_i}$ je končno mnogo, natančneje $\prod_{i=1}^{r_1}(\alpha_i+1)$. Ker velja $D(a_1, a_2) = 1$,nastopajo v kanoničnem razcepu a_2 druga praštevila. Vseh deliteljev števila $a_2 = \prod_{i=1}^{r_2} q_i^{\beta_i}$ je končno mnogo, natančneje $\prod_{i=1}^{r_2}(\beta_i + 1)$.

Vseh deliteljv produkta a_1a_2 je potem $\prod_{i=1}^{r_1}(\alpha_i + 1) \cdot \prod_{i=1}^{r_2}(\beta_i + 1)$. Število urejenih parov (d_1, d_2) je enako $\prod_{i=1}^{r_1}(\alpha_i + 1) \cdot \prod_{i=1}^{r_2}(\beta_i + 1)$, tudi število različnih produktov d_1d_2 je enako $\prod_{i=1}^{r_1}(\alpha_i+1)\cdot\prod_{i=1}^{r_2}(\beta_i+1)$. Ker imata obe končni množici enako moč, sledi, da je Ψ bijekcija.

Dokažimo

$$f(a_1) \cdot f(a_2) = f(a_1 \cdot a_2)$$

$$f(a_1 \cdot a_2) = \sum_{d|a_1 \cdot a_2} \chi(d)$$

$$\begin{aligned}
\sum_{d|a_1\cdot a_2} \chi(d) &= \sum_{\substack{d_1|a_1 \\ d_2|a_2}} \chi(d_1d_2), \quad \text{saj je vsak } d \text{ oblike } d_1d_2. \\
\sum_{\substack{d|a_1 \\ d|a_2}} \chi(d_1d_2) &= \sum_{d_1|a_1} \chi(d_1) \cdot \sum_{d_2|a_2} \chi(d_2) = f(a_1) \cdot f(a_2)
\end{aligned}$$

Naj bo a poljubno sestavljeno število.

$$\begin{aligned}
a &= \prod_{t=1}^{r} p_t^{l_t} = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_r^{l_r}, \\
f(a) &= f(p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_r^{l_r}) = f(p_1^{l_1}) \cdot f(p_2^{l_2}) \cdot \ldots \cdot f(p_r^{l_r}).
\end{aligned}$$

Če je a popolni kvadrat, potem mora biti eksponent l_t sod za vsak $t \in \{1, 2, ...r\}$. Torej je $f(p_t^{l_t}) \geq 1$ za vsak $t \in \{1, 2, ...r\}$, odkod sledi

$$f(a) = f\left(\prod_{t=1}^{r} p_t^{l_t}\right) \geq 1.$$

Prišli smo do rezultata, ki nam poda vrednost $f(a)$ za poljubno število a :

$$f(a) \geq \begin{cases} 0, & \text{vedno} \\ 1, & \text{če je } a \text{ popolni kvadrat} \end{cases}.$$

V nadaljevanju bo v dokazu nekaj analitičnih trikov. Tu velja pripomniti, da gre zgodovinsko izviren Dirichletov dokaz v drugo smer; v *teorijo kvadratičnih form (* glej [4],str.91).

Označimo

$$m = (4h)^6,$$

kjer ima h že znano vrednost $\varphi(k)$. Definirajmo vrednost

$$z = \sum_{n=1}^{m} 2(m-n) \cdot f(n).$$

Vrednost z lahko zapišemo kot

$$\begin{aligned} z &= \sum_{n=1}^{m} \left(2(m-n) \sum_{b|n} \chi(b) \right) = \sum_{n=1}^{m} \left(\sum_{b|n} 2(m-n) \cdot \chi(b) \right) = \\ &= \sum_{\substack{a \cdot b \leq m \\ a \in \mathbb{N} \\ b \in \mathbb{N}}} 2(m-ab) \cdot \chi(b) = \sum_{\substack{a=1 \\ a|m}}^{m} \left(\sum_{b=1}^{\frac{m}{a}} 2(m-ab) \cdot \chi(b) \right). \end{aligned}$$

Ker je $m = (4h)^6$, je $\sqrt{m} \in \mathbb{N}$ in $\frac{\sqrt{m}}{2} \in \mathbb{N}$.

Ocenimo

$$z \geq \sum_{b=1}^{\sqrt{m}} 2(m-b^2) \geq \sum_{b=1}^{\frac{1}{2}\sqrt{m}} 2(m-b^2) \geq \sum_{b=1}^{\frac{1}{2}\sqrt{m}} 2(m-\frac{m}{4}) = \frac{3}{4} m^{\frac{3}{4}} = \frac{3}{4}(4h)^9.$$

Po drugi strani pa množica M, ki vsebuje vse ustrezne urejene pare $(a,b) \in \mathbb{N} \times \mathbb{N}$ razpade na dve podmnožici:

$$M = \{(a,b); ab \leq m, \quad a,b \in \mathbb{N}\} = M_1 \cup M_2, \text{ kjer je}$$

$$M_1 = \{(a,b) \in M;\ a \leq \sqrt[3]{m}, b > m^{\frac{2}{3}}\} \quad \text{in}$$

$$M_2 = \{(a,b) \in M;\ b \leq m^{\frac{2}{3}}\}.$$

Geometrijsko sta območji predstavljeni s sliko v **prilogi 1** zadaj.

V ravnini označimo področje M kot množico parov $(a,b) \in \mathbb{N} \times \mathbb{N}$, ki ležijo pod ali na pozitivnem kraku hiperbole $ab = m$ in ki jo še omejujejo premici

$a = 1, b = 1.$ Premica $b = m^{\frac{2}{3}}$razdeli M na M_1 in M_2, vse točke, ki ležijo na premici $b = m^{\frac{2}{3}}$, pa pripadajo M_2.

Zato lahko z zapišemo kot

$$z = z_1 + z_2,$$

kjer je

$$z_1 = \sum_{a=1}^{\sqrt[3]{m}} \sum_{m^{\frac{2}{3}} < b \le \frac{m}{a}} 2(m - ab) \cdot \chi(b) \quad \text{in}$$

$$z_2 = \sum_{b=1}^{m^{\frac{2}{3}}} \sum_{0 < a \le \frac{m}{b}} 2(m - ab) \cdot \chi(b).$$

Ocenimo z_1 navzgor.

Po *izreku 4.3*, kjer vstavimo namesto a vrednost b, namesto

$$\begin{aligned} \gamma_b &= \chi(b) \\ \varepsilon_b &= 2(m - ab), \end{aligned}$$

upoštevajoč *izrek 4.2*, kjer je

$$\nu \le \frac{h}{2}, \qquad \varepsilon_u < 2m,$$

sledi ocena

$$\begin{aligned} z_1 &= \sum_{a=1}^{\sqrt[3]{m}} \sum_{m^{\frac{2}{3}} < b \le \frac{m}{a}} 2(m - ab) \cdot \chi(b) \le \sum_{a=1}^{\sqrt[3]{m}} \left| \sum_{m^{\frac{2}{3}} < b \le \frac{m}{a}} 2(m - ab) \cdot \chi(b) \right| \le \\ &\le \sum_{a=1}^{\sqrt[3]{m}} 2m \cdot \frac{h}{2} = m \cdot h \sum_{a=1}^{\sqrt[3]{m}} 1 = m^{\frac{4}{3}} \cdot h. \end{aligned}$$

Prva neenakost preprosto velja zaradi lastnosti absolutne vrednosti, druga pa je posledica *izreka 4.3.* Podobno premislimo še za z_2.

$$z_2 = \sum_{b=1}^{m^{\frac{2}{3}}} \left(\chi(b) \cdot \sum_{0 < a \le \frac{m}{b}} 2(m - ab) \right).$$

Oglejmo si najprej

$$\sum_{a=1}^{\frac{m}{b}} 2(m-ab) = 2m\sum_{a=1}^{\frac{m}{b}} 1 - b\sum_{a=1}^{\frac{m}{b}} 2a$$

Poglejmo vsako vsoto posebej.

$$\sum_{a=1}^{\frac{m}{b}} 1 = \left[\frac{m}{b}\right], \qquad \text{kjer je } a\in\mathbb{N}, [\cdot] \text{ pa funkcija 'celi del'},$$

$$\sum_{a=1}^{\frac{m}{b}} 2a = 2\sum_{a=1}^{\frac{m}{b}} a = 2\cdot\frac{\left[\frac{m}{b}\right]\cdot\left(\left[\frac{m}{b}\right]+1\right)}{2} = \left[\frac{m}{b}\right]\cdot\left(\left[\frac{m}{b}\right]+1\right).$$

Označimo $\left[\frac{m}{b}\right] = \frac{m}{b} - \theta(m,b)$, kjer je $\theta(m,b)\in[0,1)$. Ostanek θ je torej odvisen od parametrov m in b,

$$\theta(m,b) = \left[\frac{m}{b}\right] - \frac{m}{b}.$$

Izračunamo

$$\begin{aligned}
\sum_{a=1}^{\frac{m}{b}} 2m-2ab &= 2m\left[\frac{m}{b}\right] - b\left[\frac{m}{b}\right].\left(\left[\frac{m}{b}\right]+1\right) = \\
&= 2m\left(\frac{m}{b}-\theta\right) - b\left(\left(\frac{m}{b}-\theta\right)^2 + \frac{m}{b}-\theta\right) = \\
&= \frac{2m^2}{b} - 2m\theta - b\left(\frac{m^2}{b^2} - 2\theta\frac{m}{b} + \theta^2 + \frac{m}{b} - \theta\right) = \\
&= \frac{m^2}{b} - m + b\left(\theta-\theta^2\right).
\end{aligned}$$

Ker je $\theta(m,b)\in[0,1)$, je $|\theta(m,b)-\theta(m,b)^2|\leq 1$.

$$\begin{aligned}
z_2 &= \sum_{b=1}^{m^{\frac{2}{3}}} \chi(b)\left(\frac{m^2}{b} - m + b\left(\theta-\theta^2\right)\right) = \\
&= m^2\sum_{b=1}^{m^{\frac{2}{3}}}\frac{\chi(b)}{b} - m\sum_{b=1}^{m^{\frac{2}{3}}}\chi(b) + \sum_{b=1}^{m^{\frac{2}{3}}}\chi(b)\cdot b\cdot\left(\theta(m,b)-\theta(m,b)^2\right).
\end{aligned}$$

Ocenimo:

(1)
$$\sum_{b=1}^{m^{\frac{2}{3}}} \frac{\chi(b)}{b} = L(1,\chi) - \sum_{b=1+m^{\frac{2}{3}}}^{\infty} \frac{\chi(b)}{b}.$$

Po *izreku 4.4* je $\left|\sum_u^v \frac{\chi(b)}{b}\right| \leq \frac{h}{2u}$.Vzemimo za $u = 1 + m^{\frac{2}{3}}$in pošljimo $v \to \infty$. Potem je
$$\left|\sum_{b=1+m^{\frac{2}{3}}}^{\infty} \frac{\chi(b)}{b}\right| \leq \frac{h}{2}\frac{1}{m^{\frac{2}{3}}},$$
odkod sledi
$$\sum_{b=1}^{m^{\frac{2}{3}}} \frac{\chi(b)}{b} \leq L(1,\chi) - \frac{h}{2} \cdot \frac{1}{m^{\frac{2}{3}}}.$$

(2) Zaradi *izreka 4.3* velja
$$\sum_{b=1}^{m^{\frac{2}{3}}} \chi(b) \leq \frac{h}{2}.$$

(3)
$$\sum_{b=1}^{m^{\frac{2}{3}}} \chi(b) \cdot b \cdot \left(\theta - \theta^2\right) \leq m^{\frac{2}{3}} \sum_{b=1}^{m^{\frac{2}{3}}} 1 \leq m^{\frac{4}{3}} h.$$

To velja, ker je $\chi(b) \cdot b \cdot (\theta - \theta^2) \leq b$, sledi
$$\sum_{b=1}^{m^{\frac{2}{3}}} \chi(b) \cdot b \cdot \left(\theta - \theta^2\right) \leq \sum_{b=1}^{m^{\frac{2}{3}}} b = \frac{m^{\frac{2}{3}}(m^{\frac{2}{3}}+1)}{2} \leq m^{\frac{2}{3}} \cdot m^{\frac{2}{3}} = m^{\frac{2}{3}} \sum_{b=1}^{m^{\frac{2}{3}}} 1$$

Z ocenami (1), (2) in (3) je vse pripravljeno za zaključno oceno vrednosti z_2.

$$\begin{aligned} z_2 &\leq m^2 \left(L(1,\chi) - \frac{h}{2}\frac{1}{m^{\frac{2}{3}}} \right) + m^{\frac{4}{3}}\frac{h}{2} + m^{\frac{4}{3}} h = \\ &= m^2 \cdot L(1,\chi) + m^{\frac{4}{3}} h \left(\frac{1}{2} + \frac{1}{2} + 1 \right) = \\ &= m^2 \cdot L(1,\chi) + 2m^{\frac{4}{3}} h \end{aligned}$$

Uporabimo zdaj prvo oceno za z in oceni za z_1 in z_2:

$$\begin{aligned}
\frac{3}{4}(4h)^9 &\leq z < m^2 \cdot L(1,\chi) + 3m^{\frac{4}{3}}h = \\
&= m^2 \cdot L(1,\chi) + 3(4m)^8 h = \\
&= m^2 \cdot L(1,\chi) + \frac{3}{4}(4h)^9
\end{aligned}$$

Sledi

$$0 < m^2 \cdot L(1,\chi),$$

$$0 < L(1,\chi).$$

Dokazano je, da je $L(1,\chi) \neq 0$ za χ druge vrste. $\square$

Izrek 4.20 *Če je χ značaj druge ali tretje vrste, je kvocient*

$$\frac{L'(s,\chi)}{L(s,\chi)}$$

omejen za $s > 1$.

Dokaz: Po *izreku 4.4* je $L(s,\chi)$ zvezna za vsak $s \geq 1$. Po *izreku 4.11* je $L(s,\chi)$ različna od 0 za vsak $s > 1$, torej je $L(s,\chi)$ različna od 0 za vsak $s \in (1,2]$. *Izrek 4.18* in *izrek 4.19* pravita, da je $L(s,\chi) \neq 0$ za $s = 1$. Torej je $\frac{1}{L(s,\chi)}$ omejena za $s \in [1,2]$. Isto velja tudi za $s > 2$ (zaradi *izreka 4.9* in *izreka 4.11)*. Po *izreku 3.6* je $L'(s,\chi)$ omejena na množici $S = \{s \in \mathbb{R};\ s \geq 1\}$.

Odtod sledi, da je $\frac{L'(s,\chi)}{L(s,\chi)}$ omejena na $S = \{s \in \mathbb{R};\ s \geq 1\}$. $\square$

5 Dirichletov izrek o praštevilih v aritmetičnem zaporedju

Izrek 5.1 *Naj bosta k in l tuji si naravni števili. Potem za vsako realno število $s > 1$ velja:*

$$-\frac{1}{h}\sum_{\chi}\frac{1}{\chi(l)}\cdot\frac{L'(s,\chi)}{L(s,\chi)}=\sum_{a\equiv l}\frac{\Lambda(a)}{a^s},$$

kjer je $h = \varphi(k), \chi$ Dirichletovi značaji po modulu k, vsota na desni pa seštevek po vseh naravnih številih $a \equiv l(\mathrm{mod}\ k)$ v naraščajočem vrstnem redu.

Dokaz: Oglejmo si levo stran enakosti, pomnoženo s h. Po *izreku 4.14* velja

$$-\sum_{\chi}\frac{1}{\chi(l)}\cdot\frac{L'(s,\chi)}{L(s,\chi)}=\sum_{\chi}\left(\frac{1}{\chi(l)}\cdot\sum_{a=1}^{\infty}\frac{\chi(a)\cdot\Lambda(a)}{a^s}\right)$$

Ker je vseh $\chi(\mathrm{mod}\ k)$ končno mnogo, h, si privoščimo

$$\sum_{\chi}\left(\frac{1}{\chi(l)}\cdot\sum_{a=1}^{\infty}\frac{\chi(a)\cdot\Lambda(a)}{a^s}\right)=\sum_{a=1}^{\infty}\frac{\Lambda(a)}{a^s}\cdot\sum_{\chi}\frac{\chi(a)}{\chi(l)}$$

Po *izreku 3.11* velja

$$\sum_{\chi}\frac{\chi(a)}{\chi(l)}=\begin{cases}\varphi(k), & \textit{če} \quad a\equiv l(\mathrm{mod}\ k)\\ 0, & \textit{sicer}\end{cases},$$

zato je

$$-\sum_{\chi}\left(\frac{1}{\chi(l)}\cdot\sum_{a=1}^{\infty}\frac{\chi(a)\cdot\Lambda(a)}{a^s}\right)=\left(\sum_{a\equiv l}\frac{\Lambda(a)}{a^s}\right)\cdot h$$

Dokazali smo

$$-\frac{1}{h}\sum_{\chi}\frac{1}{\chi(l)}\cdot\frac{L'(s,\chi)}{L(s,\chi)}=\sum_{a\equiv l}\frac{\Lambda(a)}{a^s}.$$

□

Izrek (Dirichlet, 1839) *Naj bosta si števili k in l tuji. Potem obstaja neskončno mnogo praštevil p, za katere velja*

$$p \equiv l (\text{mod } k).$$

`Opomba`: izrek lahko podamo v ekvivalentni obliki, ki pravi: *v aritmetičnem zaporedju*

$$\{l, l+k, l+2k, l+3k, ...\},$$

kjer velja $D(k,l) = 1$, obstaja neskončno praštevil.

Dokaz:

Brez škode za splošnost lahko predpostavimo, da je $l \in \mathbb{N}$.

Po *izreku 5.1* je

$$\frac{1}{\varphi(k)} \sum_{\chi} \frac{1}{\chi(l)} \cdot \frac{L'(s,\chi)}{L(s,\chi)} = -\sum_{a \equiv l} \frac{\Lambda(a)}{a^s}.$$

Levo stran enakosti lahko zapišemo kot vsoto

$$\frac{1}{\varphi(k)} \sum_{\chi} \frac{1}{\chi(l)} \cdot \frac{L'(s,\chi)}{L(s,\chi)} = \frac{1}{\varphi(k)} \sum_{\chi_0} \frac{1}{\chi_0(l)} \cdot \frac{L'(s,\chi_0)}{L(s,\chi_0)} + \frac{1}{\varphi(k)} \sum_{\chi \neq \chi_0} \frac{1}{\chi(l)} \cdot \frac{L'(s,\chi)}{L(s,\chi)}$$

Naj bo $s \in \mathbb{R}$. Izračunajmo $\lim\limits_{s \downarrow 1} \left(\frac{1}{\varphi(k)} \sum_{\chi_0} \frac{1}{\chi_0(l)} \cdot \frac{L'(s,\chi_0)}{L(s,\chi_0)} \right)$.

Po *izreku 4.15* je $\lim\limits_{s \downarrow 1} \frac{L'(s,\chi_0)}{L(s,\chi_0)} = -\infty$, zato je

$$\lim_{s \downarrow 1} \left(\frac{1}{\varphi(k)} \sum_{\chi_0} \frac{1}{\chi_0(l)} \cdot \frac{L'(s,\chi_0)}{L(s,\chi_0)} \right) = -\infty.$$

Limita ostalih $h-1$ členov oblike $\frac{1}{\varphi(k)} \sum_{\chi \neq \chi_0} \frac{1}{\chi(l)} \cdot \frac{L'(s,\chi)}{L(s,\chi)}$ pa obstaja, saj je količnik $\frac{L'(s,\chi)}{L(s,\chi)}$, kjer je $\chi \neq \chi_0$, omejen na $S = \{s \in \mathbb{R};\ \ s \geq 1\}$. (*izrek 4.20*).

Sklepamo lahko, da je potemtakem

$$\lim_{s \downarrow 1} \frac{1}{\varphi(k)} \sum_{\chi} \frac{1}{\chi(l)} \cdot \frac{L'(s,\chi)}{L(s,\chi)} = -\infty,$$

oziroma da velja

$$\lim_{s\downarrow 1}\sum_{a\equiv l}\frac{\Lambda(a)}{a^s}=\infty.$$

Uporabimo definicijo funkcije Λ in $\sum_{a\equiv l}\frac{\Lambda(a)}{a^s}$ zapišimo malce drugače.

$$\sum_{a\equiv l}\frac{\Lambda(a)}{a^s}=\sum_{p\equiv l}\frac{\Lambda(p)}{p^s}+\sum_{\substack{p^m\equiv l\\ m>1}}\frac{\Lambda(p^m)}{p^{ms}}+\sum_{a'\equiv l}\frac{\Lambda(a')}{a'^s},$$

kjer p pomeni praštevila, a' pa števila oblike $a'=\prod_{i=1}^{r}p_i^{t_i}$, kjer je $r>1$.

Ker je

$$\begin{aligned}\sum_{p\equiv l}\frac{\Lambda(p)}{p^s}&=\sum_{p\equiv l}\frac{\ln p}{p^s},\\ \sum_{\substack{p^m\equiv l\\ m>1}}\frac{\Lambda(p^m)}{p^{ms}}&=\sum_{\substack{p^m\equiv l\\ m>1}}\frac{\ln p}{p^{ms}},\\ \sum_{a'\equiv l}\frac{\Lambda(a')}{a'^s}&=0,\end{aligned}$$

velja

$$\sum_{a\equiv l}\frac{\Lambda(a)}{a^s}=\sum_{p\equiv l}\frac{\ln p}{p^s}+\sum_{\substack{p,m\\ p^m\equiv l\\ m>1}}\frac{\ln p}{p^{ms}}.$$

Oglejmo si še $\sum_{\substack{p,m\\ p^m\equiv l\\ m>1}}\frac{\ln p}{p^{ms}}$ in ocenimo vrednost te končne vsote. Upoštevajmo, da je

$$\sum_{m=1}^{\infty}\frac{1}{(p^m)^s}=\frac{1}{p^s-1}$$

in

$$p^s-1>(p-1)p.$$

Sledi

$$\sum_{\substack{p,m\\ p^m\equiv l\\ m>1}}\frac{\ln p}{p^{ms}}\le\sum_{\substack{p,m\\ m>1}}\frac{\ln p}{p^{ms}}<\sum_{p\in\mathbb{P}}\frac{\ln p}{p(p-1)}\le\sum_{a=1}^{\infty}\frac{\ln a}{a(a-1)}<\sum_{a=2}^{\infty}\frac{2\ln a}{a^2}.$$

Ker vrsta $\sum_{a=2}^{\infty} \frac{\ln a}{a^2}$ konvergira, saj konvergira $\sum_{a=2}^{\infty} \frac{\ln a}{a^s}, s > 1$ (po *lemi 4.5)*, konvergira tudi

$$\sum_{\substack{p,m \\ p^m \equiv l \\ m>1}} \frac{\ln p}{p^{ms}}.$$

Zdaj do končnega rezultata ni več daleč.

$\sum_{a\equiv l} \frac{\Lambda(a)}{a^s}$ divergira. Ker $\sum_{\substack{p,m \\ p^m \equiv l \\ m>1}} \frac{\ln p}{p^{ms}}$ konvergira, mora biti vrsta

$$\sum_{p\equiv l} \frac{\ln p}{p^s} = \sum_{a\equiv l} \frac{\Lambda(a)}{a^s} - \sum_{\substack{p,m \\ p^m \equiv l \\ m>1}} \frac{\ln p}{p^{ms}}$$

divergentna.

To pa se lahko zgodi le v primeru, če imamo v vrsti $\sum_{p\equiv l} \frac{\ln p}{p^s}$ neskončno členov, oziroma če je neskončno praštevil p, za katere velja

$$p \equiv l (\mathrm{mod}\ k).$$

$\square$

Literatura

[1] E. Landau: *Elementary number theory*, American Mathematical Society, 1999

[2] I. Niven, H. S. Zuckerman, H. L. Montgomery: *An introduction to the theory of numbers*, Fifth edition,Wiley&Sons, 1991

[3] H. S. Gaskill, P. P. Narayanaswami: *Foundations of analysis. The theory of limits*, Harper&Row, 1989.

[4] P. G. L. Dirichlet: *Lectures on number theory. Supplements by R. Dedekind*, American Mathematical Society, London Mathematical Society, 1999

[5] N. A. Virčenko: *Matematika v aforizmih, citatih in izrekih*, DMFA, Ljubljana 1990

[6] I. N. Bronštejn, K. A. Semendjajev, G. Musiol, H. Mühlig: *Matematični priročnik*, Tehnična založba Slovenije, Ljubljana 1997