Dowód, że każda funkcya liniowa o spółczynnikach całkowitych zespolonych i niespółdzielnych przedstawia nieskończenie wiele liczb pierwszych.

PODAŁ

F. MERTENS. [1])

1. Dirichlet [2]) udowodnił, że twierdzenie, iż każda funkcya liniowa $L+Mz$ o spółczynnikach L, M całkowitych i niespółdzielnych przedstawia nieskończenie wiele liczb pierwszych, ma miejsce i dla liczb $a+bi$, gdzie a, b są liczby rzeczywiste całkowite. Lecz dowód jego wymaga nie tylko stosowania prawa wzajemności reszt kwadratowych w teoryi tych liczb zespolonych, ale i rozległej teoryi form kwadratowych dwójkowych ze spółczynnikami całkowitemi zespolonemi.

Mniemamy, że nie będzie pozbawiony interesu dowód poniższy, przy pomocy środków bardzo prostych przeprowadzony.

2. Niechaj będzie funkcya liniowa $L+Mz$ o spółczynnikach L, M niespółdzielnych; mamy dowieść, że istnieje nieskończenie wiele liczb pierwszych z, dla których $L+Mz$ jest liczbą pierwszą zespoloną dwuwyrazową.

Liczbę zespoloną ζ nieparzystą, t. j. niepodzielną przez $1+i$, nazwijmy pierwotną, gdy:

$$\zeta \equiv 1 \pmod{(1+i)^3}.$$

Można wtedy, bez szkody dla ogólności, ograniczyć się na przypadku, w którym L jest liczbą nieparzystą i pierwotną, M liczbą podzielną przynajmniej przez $(1+i)^3$ i nadto $N(M)>8$.

[1]) Z „Sitzungeberichte“ Akademii Wiedeńskiej, Maj 1899.

[2]) „Abhandlungen der Berliner Akademie“ 1841, Dirichlet's, Werke, t. I, s. 511.

W samej rzeczy, gdy L jest liczbą parzystą, a więc M nieparzystą, to funkcyę $L+Mz$ można zastąpić przez $(L+M)+Mz$. Ta ostatnia zaś może przedstawiać liczby nieparzyste tylko, gdy z jest liczbą parzystą, a wtedy liczby pierwsze nieparzyste, które przedstawia funkcya $L+Mz$ schodzą się z liczbami pierwszemi nieparzystemi, które przedstawia funkcya $(L+M)+(1+i)Mz$. Można tedy przyjąć, że L jest nieparzyste, M zaś parzyste.

Gdy M jest podzielne przez $1+i$, a nie jest podzielne przez $(1+i)^3$, wtedy liczby pierwsze, które przedstawia funkcya $L+Mz$, schodzą się z liczbami pierwszemi, które przedstawiają funkcye:

$$L+(1+i)^2Mz, \qquad L+M+(1+i)^2Mz, \qquad L+M+(1+i)^2Mz,$$
$$L+(1+i)M+(1+i)^2Mz,$$

i dość przeprowadzić dowodzenie dla każdej z tych funkcyj. Gdy M jest podzielne przez $(1+i)^2$, a nie jest podzielne przez $(1+i)^3$, wtedy liczby pierwsze, które przedstawia funkcya $L+Mz$, schodzą się z liczbami pierwszemi, które przedstawiają funkcye:

$$L+(1+i)Mz, \qquad L+M+(1+i)Mz,$$

Gdy zaś M jest podzielne przez $(1+i)^3$, $L\equiv i^\varrho \pmod{(1+i)^3}$, ϱ zaś różne od zera, wtedy—przy przyjęciu, że liczby pierwsze stowarzyszone nie są zasadniczo różne—funkcya $Li^{-\varrho}+Mz$ przedstawia te same liczby pierwsze, co funkcya $L+Mz$, tylko w postaci liczb pierwotnych.

Można wreszcie przyjąć, że norma liczby M, t. j. $N(M)$ jest >8, gdyż dla funkcyi $1+(1+i)^3z$, przedstawiającej wszystkie możliwe liczby pierwsze nieparzyste pierwotne, dowodu nie potrzeba.

3. Niechaj będzie $M=a+ib$, $N(M)=a^2+b^2=P$, d zaś największym spólnym dzielnikiem liczb a i b.

Otrzymujemy układ zupełny $\mathfrak{R}$ reszt dla modułu M, biorąc wszystkie liczby $x+iy$, w których x należy do szeregu $0, 1, 2, \ldots \frac{P}{d}-1$, y zaś do szeregu $0, 1, 2, \ldots d-1$.

Ogół wszystkich liczb układu $\mathfrak{R}$, niespółdzielnych z liczbą M i pierwotnych, oznaczmy przez Ω, a liczbę tych liczb przez r.

Według Kroneckera [1]) istnieje w Ω układ liczb:

$$g_1, g_2, \ldots\ldots, g_r,$$

[1]) „Monatsberichte der Berliner Akademie“ 1870.

czyniących zadość następującemu warunkowi: Jeżeli liczby $g_1, g_2, \ldots, g_\nu$ należą według modułu M odpowiednio do wykładników $\tau_1, \tau_2, \ldots, \tau_\nu$, to wtedy każda liczba, wzięta z Ω, przystaje, według modułu M, do jednego i tylko do jednego iloczynu potęg:

$$g_1^{\alpha_1} g_2^{\alpha_2} \ldots\ldots g_\nu^{\alpha_\nu},$$

gdzie α_1 jest jedną z liczb szeregu $0, 1, 2, \ldots, \tau_1-1$; α_2 jedną z liczb szeregu $0, 1, 2, \ldots, \tau_2-1$; $\ldots\ldots$; α_ν jedną z liczb szeregu $0, 1, 2, \ldots, \tau_\nu-1$, tak że

$$\tau_1 \tau_2 \ldots \tau_\nu = \gamma.$$

Jeżeli więc ζ jest liczbą pierwotną niespółdzielną z M, to istnieją wykładniki $\alpha_1, \alpha_2, \ldots, \alpha_\nu$, zupełnie oznaczone i mniejsze od $\tau_1, \tau_2, \ldots \tau_n$, takie, że:

$$\zeta \equiv g_1^{\alpha_1} g_2^{\alpha_2} \ldots\ldots g_\nu^{\alpha_\nu} \pmod M.$$

Wykładniki te nazwijmy skaźnikami liczby ζ i oznaczmy je w ten sposób:

$$\alpha_1 = \operatorname{ind}_1 \zeta, \quad \alpha_2 = \operatorname{ind}_2 \zeta, \ldots\ldots \alpha_\nu = \operatorname{ind}_\nu \zeta.$$

Jeżeli ζ_1, ζ_2 są dwie liczby pierwotne niespółdzielne z M, będzie:

$$\begin{aligned}
\operatorname{ind}_1 (\zeta_1\zeta_2) &\equiv \operatorname{ind}_1 \zeta_1 + \operatorname{ind}_1 \zeta_2 \pmod{\tau_1},\\
\operatorname{ind}_2 (\zeta_1\zeta_2) &\equiv \operatorname{ind}_2 \zeta_1 + \operatorname{ind}_2 \zeta_2 \pmod{\tau_2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
\operatorname{ind}_\nu (\zeta_1\zeta_2) &\equiv \operatorname{ind}_\nu \zeta_1 + \operatorname{ind}_\nu \zeta_2 \pmod{\tau_\nu}.
\end{aligned}$$

Jest:

$$\operatorname{ind}_1 \zeta = \operatorname{ind}_2 \zeta = \ldots\ldots = \operatorname{ind}_\nu \zeta = 0,$$

jeżeli $\zeta \equiv 1 \pmod M$ i tylko w tym przypadku.

4. Dla otrzymania układu $g_1, g_2, \ldots, g_\nu$ postępujemy w ten sposób:

Niechaj $\mathfrak{A}, \mathfrak{B}, \ldots, \mathfrak{E}$ będą liczby z Ω, J zaś niech oznacza zbiór wszystkich tych liczb w Ω, które przystają do iloczynu potęg $\mathfrak{A}^\alpha \mathfrak{B}^\beta \ldots \mathfrak{E}^\varepsilon$ według modułu M. Liczby zbioru J mają następujące własności:

Iloczyn dwóch jakichkolwiek liczb z J przystaje do jednej z liczb tegoż zbioru według modułu M. Toż samo stosuje się do pierwiastku kongruencyi $mz \equiv n \pmod M$.

Dla każdej liczby pierwotnej ζ niespółdzielnej z M istnieje wykładnik dodatni najmniejszy ε taki, że ζ^ε przystaje do jednej z liczb zbioru J według modułu M. Wykładnik ten nazwijmy wykładnikiem liczby ζ w odniesieniu do zbioru J.

Iloczyny wszystkich liczb zbioru J przez potęgi $1, \zeta, \zeta^2, \ldots, \zeta^{\varepsilon-1}$ są nieprzystającemi według modułu M. Albowiem przypuszczenie:

$$\zeta^\alpha m \equiv \zeta^\beta m' \pmod M$$

w przypadku, gdy $\alpha > \beta$, prowadzi do sprzeczności:

$$\zeta^{\alpha-\beta} \equiv m'' \pmod M;$$

m, m', m'' oznaczają tu liczby ze zbioru J. Wynika stąd, że liczby układu Ω, przystające według modułu M do uważanych tu iloczynów, dają nam wszystkie liczby układu Ω, które przystają według modułu M do iloczynu potęg liczb $\mathfrak{A}, \mathfrak{B}, \ldots, \mathfrak{E}, \zeta$.

Każdy wykładnik, dla którego liczba ζ przystaje do jednej z liczb J według modułu M, jest wielokrotnością liczby ε. Jeżeli m i n są liczbami pierwotnemi niespółdzielnemi z M, α i β ich wykładnikami odnośnie do J, to można znaleść liczbę pierwszą, której wykładnik w odniesieniu do J jest najmniejszą wielokrotną μ liczb α i β. Aby tego dowieść przyjmijmy, że δ jest największym spólnym dzielnikiem liczb α, β i że $\alpha = \delta\alpha'$, $\beta = \delta\beta'$. Rozłóżmy δ na czynnik ϱ niespółdzialny z α' i na czynnik σ, dzielący potęgę liczby α'. Liczba $m^\varrho n^\sigma$ ma wtedy wykładnik μ w odniesieniu do zbioru J.

Niechaj π będzie tym wykładnikiem, wtedy liczba $m^{\varrho\pi} n^{\sigma\pi}$ przystaje do jednej z liczb w J według modułu M, a więc przystają i liczby:

$$(m^{\varrho\pi} n^{\sigma\pi})^{\frac{\beta}{\sigma}} = (n^\beta)^\pi m^{\beta'\pi\varrho\varrho},$$

$$(m^{\varrho\pi} n^{\sigma\pi})^{\frac{\alpha}{\varrho}} = (m^\alpha)^\pi n^{\alpha'\pi\sigma\sigma}.$$

Wtedy zaś liczby $m^{\beta'\pi\varrho\varrho}$, $n^{\alpha'\pi\varrho\varrho}$ przystają do liczb ze zbioru J, a stąd wynika, że $\beta'\pi\varrho^2$ musi być podzielne przez α, $\alpha'\pi\sigma^2$ przez β, lub $\beta'\pi\varrho$ przez $\alpha'\sigma$, $\alpha'\pi\sigma$ przez $\beta'\varrho$. Ponieważ wszakże liczby $\alpha'\sigma$ i $\beta'\varrho$ są niespółdzielne, przeto π musi być podzielne przez każdą z nich, a więc także przez ich iloczyn $\alpha'\sigma \cdot \beta'\varrho = \alpha'\beta'\delta = \mu$. Z drugiej strony $(m^\sigma n^\sigma)^\mu = (m^\alpha)^{\varrho\beta'} \cdot (n^\beta)^{\sigma\alpha'}$ przystaje do jednej z liczb zbioru J, a zatem μ musi być podzielne przez μ. Jest przeto $\pi = \mu$.

Z tego twierdzenia wynika odrazu, że wykładniki wszystkich liczb układu Ω w odniesieniu do zbioru J muszą dzielić największy z tych wykładników γ, a więc potęga γ-ta każdej liczby pierwotnej, niespółdzielnej z M, musi przystawać do jednej z liczb w J według modułu M.

Niechaj teraz będzie g_1 jedną z liczb układu Ω, należącą do jednego z możliwie największych wykładników τ_1 według modułu M, albo—co wychodzi na jedno — liczbą, która w odniesieniu do zbioru J_0, zawierającego

tylko jedność 1, posiada możliwie największy wykładnik τ_1, J_1 zaś zbiorem wszystkich liczb układu Ω, które przystają według modułu M do jednej z potęg $1, g_1, g_1^2, \ldots, g_1^{\tau-1}$.

Jeżeli $\tau_1 = r$, to J_1 zlewa się z Ω, g_1 zaś tworzy układ żądany.

Jeżeli przeciwnie $\tau_1 < r$, to szukamy w Ω takiej liczby g_2, której wykładnik, w odniesieniu do J_1 jest możliwie największy, i która, według modułu M, należy do możliwie najmniejszego wykładnika t_2; niechaj J_2 będzie zbiorem wszystkich liczb z Ω, które przystają do iloczynu potęg liczb g_1, g_2 według modułu M. Wtedy $\tau_2 > 1$, a zbiór J_2 zawiera $\tau_1\,\tau_2$ liczb, zatem więcej liczb niż J_1.

Jeżeli $\tau_1\tau_2 = r$, to J_2 zlewa się z Ω.

Jeżeli przeciwnie $\tau_1\tau_2 < r$, to szukamy w Ω liczby g_3, którą w odniesieniu do J_2 ma wykładnik możliwie największy τ_3 i należy, według modułu M, do wykładnika możliwie najmniejszego t_3. Wtedy $\tau_3 > 1$ i J_3 zawiera $\tau_1\tau_2\tau_3$ liczb, a zatem więcej liczb niż J_2.

Jeżeli $\tau_1\tau_2\tau_3 = r$, to J_3 zlewa się z Ω. Jeżeli zaś $\tau_1\tau_2\tau_3 < r$, to postępujemy dalej w sposób wyżej wskazany.

Ponieważ zbiory $J_1, J_2, J_3, \ldots$ zawierają coraz więcej liczb z Ω, jest przeto jasnem, że we wszystkich przypadkach musimy, po pewnej liczbie kroków, dojść do szeregu liczb $g_1, g_2, \ldots, g_\nu$, które wszystkie należą do Ω i mają tę własność, że zbiór J_ν złożony z $\tau_1, \tau_1, \ldots, \tau_\nu$ liczb z Ω, przystających według modułu M do iloczynu potęg liczb $g_1, g_2, \ldots g_\nu$ zlewa się z układem Ω. Wtedy $g_1, g_2, \ldots, g_\nu$ stanowią układ żądany.

Aby to stwierdzić, należy jeszcze okazać, że $t_2 = \tau_2$, $t_3 = \tau_3, \ldots, t_\nu = \tau_\nu$, gdy $\nu > 1$.

Wykładnik τ_k, gdy $k > 1$, dzieli bez reszty każdy poprzedzający np. τ_i, albowiem $g_k^{\tau_i}$ przystaje do jednej z liczb zbioru J_{i-1}, a więc i zbioru J_{k-1} według modułu M, i dla tego τ_i musi być podzielne przez wykładnik τ_k liczby g_k w odniesieniu do J_{k-1}.

Jeżeli iloczyn liczby g_i^λ przez liczbę m ze zbioru J_{i-1} przystaje do potęgi τ_k-ej liczby pierwotnej c według modułu M i $i < k$, to λ jest podzielne przez τ_k. Albowiem mamy:

$$(m g_i^\lambda)^{\frac{\tau_i}{\tau_k}} \equiv c^{\tau_i} \pmod{M}$$

a ponieważ $m^{\frac{\tau_i}{\tau_k}}$, c^{τ_i} przystają do liczb z J_{i-1} według modułu M, przeto i $g_i^{\frac{\lambda\tau_i}{\tau_k}}$ do takiej liczby przystaje, stąd $\frac{\lambda\tau_i}{\tau_k}$ musi być podzielne przez τ_i, a więc λ przez τ_k.

Potęga τ_k-ta każdej liczby pierwotnej c niespółdzielnej z M przystaje do potęgi τ_k-tej liczby ze zbioru J_{k-1} według modułu M. Wymaga to dowodu tylko dla $k > 1$. Liczba c^{τ_k} przystaje do liczby ze zbioru J_{k-1} według modułu M i możemy napisać:

$$c^{\tau_k} \equiv g_1^{\alpha_1} g_2^{\alpha_2} \ldots\ldots g_{k-1}^{\alpha_{k-1}} \pmod{M}.$$

Na zasadzie tej kongruencyi iloczyn liczby $g_{k-1}^{\alpha_{k-1}}$ przez liczbę ze zbioru J_{k-2} przystaje do potęgi τ_k-ej liczby pierwotnej c według modułu M, przeto α_{k-1} jest podzielne przez τ_k i mamy kongruencyę:

$$c_1^{\tau_k} \equiv g_1^{\alpha_1} g_2^{\alpha_2} \ldots\ldots g_{k-2}^{\alpha_{k-2}} \pmod{M},$$

gdy $k > 2$. Z tej kongruencyi przy pomocy podobnego rozumowania wynika podzielność liczby α_{k-2} przez τ_k. W ten sposób dostajemy kolejno:

$$\alpha_{k-1} \equiv \alpha_{k-2} \equiv \ldots\ldots \equiv \alpha_1 \equiv 0 \pmod{\tau_k}.$$

Mamy tedy, gdy m oznacza liczbę ze zbioru J_{k-1}:

$$g_k^{\tau_k} \equiv m^{\tau_k} \pmod{M}.$$

Jeżeli $mm' \equiv 1 \pmod{M}$, n zaś jest liczbą z Ω, przystającą do iloczynu $m' g_k$ według modudułu M, to n w odniesieniu do J_{k-1} posiada wykładnik τ_k, gdyż dla każdego wykładnika dodatniego mniejszego od τ liczba g_k^τ, a więc i liczba $m'^\tau g_k^\tau$ nie przystaje do żadnej liczby ze zbioru J_{k-1} według modułu M. Na zasadzie przyjęcia musi tedy liczba n należeć, według modułu M, do wykładnika, który jest $\geqq t_k$; lecz n należy do wykładnika τ_k, jak to widać z kongruencyi:

$$n^{\tau_k} \equiv (m' g_k)^{\tau_k} \equiv (m' m)^{\tau_k} \equiv 1 \pmod{M},$$

a zatem $\tau_k \geqq t_k$. Ponieważ z drugiej strony t_k musi być podzielne przez τ_k, przeto być musi $t_k = \tau_k$.

5. Niechaj $\omega_1, \omega_2, \ldots, \omega_\nu$ oznaczają odpowiednio pierwiastki z jedności stopnia $\tau_1, \tau_2, \ldots, \tau_\nu$ dowolne. Jeżeli zestawimy każdą wartość pierwiastka ω_1 z każdą wartością pierwiastka ω_2 i t. d., otrzymamy $\tau_1\tau_2 \ldots \tau_\nu = \tau$ połączeń pierwiastków $\omega_1, \omega_2, \ldots, \omega_\nu$. Pomiędzy niemi znajduje się połączenie $1, 1, \ldots 1$, które nazywamy połączeniem zerowem; pozostałe połączenia w dowolnym porządku nazwijmy: pierwszem, drugiem, $\ldots$, $(\tau-1)$-em.

Jeżeli $\omega_1, \omega_2, \ldots, \omega_\nu$ jest połączeniem h-tem, to niechaj dla każdej liczby zespolonej pierwotnej niespółdzielnej z M będzie:

$$c_{h,m} = \omega_1^{\mathrm{ind}_1 m} \omega_2^{\mathrm{ind}_2 m} \ldots\ldots \omega_\nu^{\mathrm{ind}_\nu m},$$

dla liczb zaś, które nie są niespółdzielnemi z M lub nie są pierwotnemi, niechaj będzie $c_{h,m}$ zerem.

Mamy tedy $c_{h,m'} = c_{h,m}$ gdy $m' \equiv m \pmod M$, oraz $c_{h,n} \cdot c_{h,n'} = c_{h,nn'}$ gdy n, n' są liczby pierwotne nieparzyste.

Jeżeli $h > 0$, to biorąc sumę dla wszystkich liczb m, należących do $\mathfrak{N}$, otrzymujemy:

$$\Sigma c_{h,m} = 0,$$

gdyż przy tem sumowaniu można odwrócić uwagę od wszystkich liczb m, nie należących do Ω, a pozostałe przyjąć w postaci $g_1^{\alpha_1} g_2^{\alpha_2} \ldots . g_n^{\alpha_n}$. Będzie tedy:

$$c_{h,m} = \omega_1^{\alpha_1} \omega_2^{\alpha_2} \ldots . \omega_\nu^{\alpha_\nu},$$

a sumowanie dość rozciągnąć na wartości $0, 1, 2, \ldots, \tau_1 - 1$ wykładnika α_1, wartości $0, 1, 2, \ldots, \tau_2 - 1$ wykładnika α_2 i t. d. Jeżeli ω_λ jest różnym od jedności pierwiastkiem w h-tem połączeniu pierwiastków, to należy przyjąć $g_1^{\alpha_1} g_2^{\alpha_2} \ldots . g_\nu^{\alpha_\nu} = n g_\lambda^{\alpha_\lambda}$. Jeżeli wykonamy sumowanie najprzód względem α_λ, to otrzymamy agregat, złożony z samych wyrażeń:

$$c_{h,n} (\omega_\lambda^{\ 0} + \omega_\lambda + \omega_\lambda^{\ 2} + \ldots . , \omega_\lambda^{\tau_\lambda - 1}) = c_{h,n} \frac{\omega_\lambda^{\tau_\lambda} - 1}{\omega_\lambda - 1},$$

które są wszystkie zerami. Jeżeli k jest jakąkolwiek liczbą zespoloną całkowitą, to $k+m$ wraz z m przebiega zupełny układ reszt względem modułu M i dla tego jest także:

$$\Sigma c_{h,k+m} = 0.$$

6. Znikanie sumy $\Sigma c_{h,m}$, rozciągniętej na wszystkie liczby należące do $\mathfrak{N}$, pociąga za sobą to, że suma $\theta(s) = \Sigma c_{h,m}$, rozciągnięta na wszystkie liczby m, których norma nie jest większa od pewnej liczby dodatniej s, jest rzędu wielkości $\sqrt{s}$, jeżeli $h > 0$.

Niechaj będzie:

$$E\sqrt{s} = \eta, \qquad E\frac{d\eta}{P} = A, \qquad E\frac{\eta}{d} = B,$$

gdzie $E\,z$ oznacza największą liczbę całkowitą, zawartą w z; oznaczmy nadto przez $[G]$ liczbę zespoloną, której wartość bezwzględna nie przekracza liczby dodatniej G.

Jeżeli y jest liczbą, która—jeżeli odwrócimy uwagę od jej znaku—nie jest większa od η, i jeżeli położymy:

$$E\sqrt{s-y^2} = \xi, \qquad S_y = c_{h,iy} + c_{h,1+iy} + c_{h,2+iy} + \ldots + c_{h,\xi+iy},$$

to—gdy $k \frac{P}{d}$ jest wielokrotnością liczby $\frac{P}{d}$, nie większą od ξ, będzie:

$$S_y = c_{h,iy} + c_{h,1+iy} + \ldots . + c_{h,\frac{kP}{d}-1+iy} + \left[\xi + 1 - k\frac{P}{d}\right];$$

ponieważ wszakże:

$$\xi + 1 \leqslant \frac{P}{d}\left(1 + E\frac{d\sqrt{s-y^2}}{P}\right),$$

to będzie:

$$S_y = c_{h,iy} + c_{h,1+iy} + \ldots . , c_{h,\frac{kP}{d}-1+iy} + \frac{P}{d}\left[1 + E\frac{d\sqrt{s-y^2}}{P} - k\right].$$

Jeżeli $(l+1)d \leqslant \eta$, $l \geqslant 0$, y zaś jest jedną z liczb ld, $ld+1$, $ld+2, \ldots, ld+d-1$, będzie:

$$E\frac{d\sqrt{s-y^2}}{P} \leqslant E\frac{d\sqrt{s^2-l^2d^2}}{P}; \quad \xi \geqslant \frac{P}{d} E\frac{d}{p}\sqrt{s-(l+1)^2d^2}$$

i można będzie przyjąć:

$$k = E\frac{d}{p}\sqrt{s-(l+1)^2d^2},$$

a wtedy:

$$S_y = c_{h,iy} + c_{h,1+iy} + \ldots . + c_{h,\frac{kP}{d}-1+iy} + \frac{P}{d}\left[1 + E\frac{d\sqrt{s^2-l^2d^2}}{P} - E\frac{d}{P}\sqrt{s-(l+1)^2d^2}\right].$$

Kładąc $y = ld, ld+1, \ldots, ld+d-1$, sumując i uwzględniając równanie:

$$c_{h,ild} + c_{h,1+ild} + \ldots . + c_{h,\frac{kP}{d}-1+ild}$$

$$+ c_{h,ild+i} + c_{h,1+ild+i} + \ldots . + c_{h,\frac{kP}{d}-1+ild+1}$$

$$\ldots \ldots \ldots \ldots \ldots \ldots \ldots$$

$$+ c_{h,ild+id-i} + c_{h,1+ild+id-i} + \ldots . + c_{h,\frac{kP}{d}-1+ild+id-i} = 0,$$

znajdziemy:

$$S_{ld} + S_{ld+1} + \ldots . + S_{ld+d-1} = P\left[1 + E\frac{d}{P}\sqrt{s^2-l^2d^2} - E\frac{d}{P}\sqrt{s-(l+1)^2d^2}\right].$$

Jeżeli zaś $ld \leqslant \eta, (l+1)d > \eta$, y zaś jest jedną z liczb $ld, ld+1, \ldots, \eta$, wtedy można przyjąć $k=0$ i będzie:

$$S_y = \frac{P}{d}\left[1+E\frac{d}{P}\sqrt{s-l^2d^2}\right],$$

a więc:

$$S_{ld} + S_{ld+1} + \ldots\ldots + S_\eta = \frac{P}{d}\left[1+E\frac{d}{P}\sqrt{s-l^2d^2}\right](\eta - ld+1).$$

Ponieważ Bd jest największą wielokrotnością liczby d, zawartą w η, przeto:

$$\begin{aligned} S_0 + S_1 + S_2 + \ldots + S_\eta &= P\left[B+E\frac{d\sqrt{s}}{P} - E\frac{d}{P}\sqrt{s-B^2d^2}\right] \\ &+ \frac{P}{d}(\eta - Bd+1)\left[1+E\frac{d}{P}\sqrt{s-B^2d^2}\right] \\ &= P\left[A+B+1-\left(B+1-\frac{\eta+1}{d}\right)\left(E\frac{d}{P}\sqrt{s-B^2d^2}+1\right)\right] \\ &= P(A+B+1). \end{aligned}$$

W ten sposób widać bezpośrednio, że:

$$S_0 + S_{-1} + S_{-2} + \ldots\ldots + S_{-\eta} = P[A+B+1],$$

a gdy położymy $S'_y = c_{h,iy} + c_{h,iy-1} + \ldots + c_{h,iy-\xi}$, będzie:

$$\begin{aligned} S'_0 + S'_1 + S'_2 + \ldots\ldots + S'_\eta &= P[A+B+1], \\ S'_0 + S'_{-1} + S'_{-2} + \ldots\ldots + S'_{-\eta} &= P[A+B+1]. \end{aligned}$$

Lecz jest:

$$\begin{aligned} \vartheta(s) = {} & S_0 + S_1 + S_2 + \ldots\ldots + S_\eta \\ & + S_0 + S_{-1} + S_{-2} + \ldots\ldots + S_{-\eta} \\ & + S'_0 + S'_1 + S'_2 + \ldots\ldots + S'_\eta \\ & + S'_0 + S'_{-1} + S'_{-2} + + \ldots\ldots + S'_{-\eta} \\ & - S_0 - S'_0 \\ & - c_{h,i} - c_{h,2i} - \ldots\ldots - c_{h,\eta i} \\ & - c_{h,-i} - c_{h,2i} - \ldots\ldots - c_{h,-\eta i}, \end{aligned}$$

a stąd:

$$\begin{aligned} \vartheta(s) &= 4P[A+B+1] + 4[\sqrt{s}] \\ &= 4\left[d\sqrt{s} + \frac{P}{d}\sqrt{s} + P\sqrt{s} + \sqrt{s}\right]. \end{aligned}$$

Jeżeli dla skrócenia napiszemy $4(1+d)\left(1+\frac{P}{ld}\right) = C$, będzie dla każdej dodatniej wartości s:

$$\vartheta(s) = [C\sqrt{s}].$$

7. Niechaj będzie

$$\mathfrak{a}_n = \Sigma c_{h,m}$$

w przypadku, gdy liczba dodatnia całkowita n jest normą liczby całkowitej zespolonej, t.j. daje się przedstawić w postaci sumy dwu kwadratów, przytem suma rozciąga się na wszystkie liczby całkowite zespolone m, czyniące zadość równaniu $N(m) = n$; w przypadku zaś, gdy n nie jest normą liczby całkowitej zespolonej, niechaj będzie:

$$\mathfrak{a}_n = 0.$$

Jeżeli $h > 0$, to szereg

$$L_h(\lambda) = \frac{\mathfrak{a}_1}{1^\lambda} + \frac{\mathfrak{a}_2}{2^\lambda} + \frac{\mathfrak{a}_3}{3^\lambda} + \ldots\ldots$$

jest zbieżny dla każdej wartości rzeczywistej λ większej od $\frac{1}{2}$.

Aby to wykazać, położymy:

$$S = \frac{\mathfrak{a}_{1+n}}{(1+n)^\lambda} + \frac{\mathfrak{a}_{2+n}}{(2+n)^\lambda} + \ldots\ldots + \frac{\mathfrak{a}_{n'+n}}{(n'+n)^\lambda},$$

Mamy:

$$\mathfrak{a}_{n+k} = \vartheta(n+k) - \vartheta(n+k-1),$$

przeto:

$$\begin{aligned} S &= \frac{\vartheta(n+1)-\vartheta(n)}{(n+1)^\lambda} + \frac{\vartheta(n+2)-\vartheta(n+1)}{(n+2)^\lambda} + \ldots + \frac{\vartheta(n+n')-\vartheta(n+n'-1)}{(n+n')^\lambda} \\ &= -\frac{\vartheta(n)}{(n+1)^\lambda} + \vartheta(n+1)\left(\frac{1}{(n+1)^\lambda} - \frac{1}{(n+2)^\lambda}\right) + \vartheta(n+2)\left(\frac{1}{(n+2)^\lambda} - \frac{1}{(n+3)^\lambda}\right) \\ &+ \ldots\ldots + \vartheta(n+n'-1)\left(\frac{1}{(n+n'-1)^\lambda} - \frac{1}{(n+n')^\lambda}\right) + \frac{\vartheta(n+n')}{(n+n')^\lambda}. \end{aligned}$$

Stąd wynika:

$$S=\frac{[C\sqrt{n}]}{(n+1)^\lambda}+[C\sqrt{n+1}]\left(\frac{1}{(n+1)^\lambda}-\frac{1}{(n+2)^\lambda}\right)+[C\sqrt{n+2}]\left(\frac{1}{(n+2)^\lambda}-\frac{1}{(n+3)^\lambda}\right)$$

$$+\ldots+[C\sqrt{n+n'-1}]\left(\frac{1}{(n+n'-1)^\lambda}-\frac{1}{(n+n')^\lambda}\right)+\frac{[C\sqrt{n+n'}]}{(n+n')^\lambda}$$

$$=\left[C\frac{\sqrt{n}+\sqrt{n+1}}{(n+1)^\lambda}\right]+\left[C\frac{\sqrt{n}+2-\sqrt{n+1}}{(n+2)^\lambda}\right]+\ldots+\left[C\frac{\sqrt{n+n'}-\sqrt{n+n'-1}}{(n+n')^\lambda}\right].$$

Lecz:

$$\frac{\sqrt{n+k}-\sqrt{n+k-1}}{(n+k)^\lambda}=\frac{1}{(\sqrt{n+k}+\sqrt{n+k-1})(n+k)^\lambda}<\frac{1}{(n+k)^{\lambda+\frac{1}{2}}}$$

$$<\frac{1}{\lambda-\frac{1}{2}}\left(\frac{1}{(n+k-1)^{\lambda-\frac{1}{2}}}-\frac{1}{(n+k)^{\lambda-\frac{1}{2}}}\right),$$

przeto:

$$S=C\left[\frac{\sqrt{n}+\sqrt{n+1}}{(n+1)^\lambda}+\frac{1}{\lambda-\frac{1}{2}}\left(\frac{1}{(n+1)^{\lambda-\frac{1}{2}}}-\frac{1}{(n+2)^{\lambda-\frac{1}{2}}}\right)\right.$$

$$\left.+\frac{1}{\lambda-\frac{1}{2}}\left(\frac{1}{(n+2)^{\lambda-\frac{1}{2}}}-\frac{1}{(n+3)^{\lambda-\frac{1}{2}}}\right)+\ldots\ldots\right]$$

$$=C\left[\frac{\sqrt{n}}{(n+1)^\lambda}+\frac{2\lambda+1}{2\lambda-1}\cdot\frac{1}{(n+1)^{\lambda-\frac{1}{2}}}\right].$$

A zatem przez wybór odpowiedniej wartości n można uczynić sumę S do wolnie małą. W szczególności jest:

$$L_h(\lambda)=\left[C\frac{2\lambda+1}{2\lambda-1}\right],$$

$$\frac{a_{n+1}}{n+1}+\frac{a_{n+2}}{n+2}+,\ldots\ldots+\frac{a_{n+n'}}{n+n'}=\left[\frac{4C}{\sqrt{n+1}}\right].$$

Podobnie otrzymujemy:

$$\frac{a_2\log 2}{2}+\frac{a_3\log 3}{3}+\ldots\ldots+\frac{a_n\log n}{n}$$

$$=\frac{\theta 3-\theta 2}{3}\log 3+\frac{\theta 4-\theta 3}{4}\log 4+\ldots\ldots+\frac{\theta n-\theta(n-1)}{n}\log n$$

$$=-\frac{\theta 2}{3}\log 3+\theta 3\left(\frac{\log 3}{3}-\frac{\log 4}{4}\right)+\ldots\ldots$$

$$+\theta(n-1)\left(\frac{\log(n-1)}{n-1}-\frac{\log n}{n}\right)+\frac{\theta(n)\log n}{n}$$

$$=C\left[\frac{\sqrt{2}\log 3}{3}+\sqrt{3}\left(\frac{\log 3}{3}-\frac{\log 4}{4}\right)+\ldots\ldots\right.$$

$$\left.+\sqrt{n-1}\left(\frac{\log(n-1)}{n-1}-\frac{\log n}{n}\right)+\frac{\sqrt{n}\log n}{n}\right]$$

$$=C\left[\frac{\sqrt{2}\log 3}{3}+\frac{\log 3}{4\sqrt{3}}+\frac{\log 4}{5\sqrt{4}}+\ldots\ldots+\frac{\log(n-1)}{n\sqrt{n-1}}+\frac{\log n}{\sqrt{n}}\right]$$

Jeżeli więc przez ω oznaczymy sumę:

$$\frac{\log 3}{4\sqrt{3}}+\frac{\log 4}{4\sqrt{4}}+\frac{\log 5}{6\sqrt{5}}+\ldots\ldots$$

będzie:

$$\frac{a_2\log 2}{2}+\frac{a_3\log 3}{3}+\ldots\ldots+\frac{a_n\log n}{n}=C\left[1+\omega+\frac{\sqrt{2}}{3}\log 3\right].$$

Jeżeli ϱ oznacza liczbę dodatnią niewiększą od 1, i wprowadzimy oznaczenia:

$$\vartheta_k=\frac{a_k}{k}+\frac{a_{k+1}}{k+1}+\ldots\ldots+\frac{a_n}{n}$$

$$\Delta=\frac{a_1}{1}+\frac{a_2}{2}+\frac{a_3}{3}+\ldots+\frac{a_n}{n}-\frac{a_1}{1^{1-\varrho}}-\frac{a_2}{2^{1-\varrho}}-\ldots-\frac{a_n}{n^{1+\varrho}},$$

będzie:

$$\Delta=\frac{1}{2}a_2\left(1-\frac{1}{2^\varrho}\right)+\frac{1}{3}a_3\left(1-\frac{1}{3^\varrho}\right)+\ldots+\frac{1}{n}a_n\left(1-\frac{1}{n^\varrho}\right)$$

$$=(\vartheta_2-\vartheta_3)\left(1-\frac{1}{2^\varrho}\right)+(\vartheta_3-\vartheta_4)\left(1-\frac{1}{3^\varrho}\right)+\ldots+\vartheta_n\left(1-\frac{1}{n^\varrho}\right)$$

$$=\vartheta_2\left(1-\frac{1}{2^\varrho}\right)+\vartheta_3\left(\frac{1}{2^\varrho}-\frac{1}{3^\varrho}\right)+\ldots+\vartheta_n\left(\frac{1}{(n-1)^\varrho}-\frac{1}{n^\varrho}\right).$$

Lecz:

$$\frac{1}{(k-1)^\varrho}-\frac{1}{k^\varrho}=\frac{\varrho}{k^{1+\varrho}}+\frac{\varrho(1+\varrho)}{2!\,k^{2+\varrho}}+\ldots<\frac{\varrho}{k^{1+\varrho}}+\frac{\varrho}{k^{2+\varrho}}+\ldots<\frac{\varrho}{k-1},$$

a stąd:

$$\Delta = 4\,C_\varrho\left[\frac{1}{1\sqrt{2}}+\frac{1}{2\sqrt{3}}+\frac{1}{3\sqrt{4}}+\ldots\ldots\right].$$

Ponieważ dalej:

$$\frac{1}{1\sqrt{2}}+\frac{1}{2\sqrt{3}}+\frac{1}{3\sqrt{4}}+\ldots\ldots<3,$$

a więc dla $n=\infty$:

$$L_h(1)-L_h(1+\varrho)=[12\,C_\varrho],$$

i będzie:

$$L_h(1+\varrho)=L_h(1)+[12\,C_\varrho];\qquad |L_h(1+\varrho|<L_h(1)+12\,C_\varrho.$$

8. Suma:

$$c_{0,m}+c_{1m}+c_{2m}+\ldots\ldots+c_{r-1,m},$$

ma wartość r lub zero, stosownie do tego, czy $m\equiv 1(\mathrm{mod}\,M)$ lub nie. Jeżeli m nie jest niespółdzielne z M lub niepierwotne, to każdy wyraz poprzedniej sumy znika. Jeżeli m jest niespółdzielne z M, pierwotne i nieprzystające do 1 modulo M, to przynajmniej jedna z liczb:

$$\mathrm{ind}_1 m,\qquad \mathrm{ind}_2 m,\quad \ldots\ldots,\quad \mathrm{ind}_\nu m,$$

jest różna od zera, dajmy na to $\mathrm{ind}_\mu m$. Jeżeli położymy $c_{h\,m}=c'_m\omega_\mu^{\mathrm{ind}_\mu m}$ to sumując względem wszystkich pierwiastków ω_μ stopnia τ_μ-go z jedności — przyczem inne ewentualne pierwiastki pozostają stałemi — otrzymamy agregat wyrażeń:

$$c'_m(1+\omega^{\mathrm{ind}_\mu m}+\omega^{2\,\mathrm{ind}_m}+\ldots+)=c'_m\,\frac{\omega^{\tau_\mu \mathrm{ind}_\mu m}-1}{\omega^{\mathrm{ind}_\mu n}-1},$$

gdzie ω oznacza pierwiastek stopnia τ_μ z jedności: lecz te wszystkie wyrażenia są zerami. Jeżeli przeciwnie $m\equiv 1(\mathrm{mod}\,M)$, to $\mathrm{ind}_1 m=\mathrm{ind}_2 m=\ldots=\mathrm{ind}_\nu m=0$, $c_{h,m}=1$, a więc $c_{0,m}+c_{1,m}+\ldots+c_{r-1,m}=r$. Jeżeli m jest niespółdzielne z M, pierwotne i należy względem M do wykładnika t, wtedy będzie tożsamościowo dla z:

$$\Pi_h(1-c_{h,m}z)=(1-z^t)^{\frac{r}{t}}.$$

Gdyż, jeżeli $z<1$, to:

$$\log\Pi_h(1-c_{h,m}z)=-z\sum_h c_{h,m}-\tfrac{1}{2}z^2\sum_h c^2_{h,m}-\tfrac{1}{3}z^3\sum_h c^3_{h,m}-\ldots;$$

ponieważ wszakże

$$\sum_h(c_{h,m})^\pi=\sum_h c_{h,m^\pi}$$

według powyższego wzoru ma wartość r lub zero, stosownie do tego, czy π jest lub nie jest podzielne przez t, będzie:

$$\log\Pi_h(1-c_{h,m}z)=-r\left(\frac{z^t}{t}+\frac{z^{2t}}{2t}+\frac{z^{3t}}{3t}+\ldots\ldots\right)=\frac{r}{t}\log(1-z^t)$$

$$\Pi_h(1-c_{h,m}z)=(1-z^t)^{\frac{r}{t}}.$$

9. Jeżeli ϱ oznacza dowolną liczbę dodatnią, to:

$$L_h(1+\varrho)=\Pi\frac{1}{1-\frac{c_{h,\varphi}}{(N\varphi)^{1+\varrho}}},$$

gdzie iloczyn rozciąga się na wszystkie liczby zespolone pierwotne nieparzyste φ, nie dzielące modułu M. Według wzoru w ust. poprzedzającym wynika stąd:

$$\Pi_h L_h(1+\varrho)=\Pi\frac{1}{\left(1-\frac{1}{(N\varphi)^{\varrho(1+t}}\right)^{\frac{r}{t}}},$$

gdzie t oznacza każdorazowy wykładnik, do którego należy φ według modułu M. Mamy przeto:

$$\Pi_h L_h(1+\varrho)>1.$$

Jeżeli połączenie k-te pierwiastków $\omega_1,\omega_2,\ldots,\omega_\nu$ zawiera przynajmniej jeden pierwiastek urojony i jeżeli połączenie, składające się z pierwiastków sprzężonych z pierwiastkami $\omega_1,\omega_2,\ldots,\omega_\nu$ jest połączeniem k'-tem, wtedy $L_k(1+\varrho)$, $L_{k'}(1+\varrho)$ są ilościami sprzężonemi, i będzie:

$$|L_k(1+\varrho)|^2=L_k(1+\varrho)\,L_{k'}(1+\varrho),$$

$$\Pi_h L_h(1+\varrho)=|L_k(1+\varrho)|^2\,\Pi_{h'}L_{h'}(1+\varrho),$$

gdzie h' przebiega przez wartości $0,1,\ldots,r-1$, prócz k i k'. Lecz ponieważ, gdy $h>0$, jest:

$$|L_{h'}(1+\varrho)|\leqslant C\,\frac{2(1+\varrho)+1}{2(1+\varrho)-1}<3\,C,$$

otrzymujemy przeto:

$$\Pi_h L_h(1+\varrho) < (3C)^{r-3} L_0(1+\varrho) |L_k(1+\varrho)|^2.$$

Jest dalej:

$$L_0(1+\varrho) < \frac{1}{1-\frac{1}{2^{1-\varrho}}} \Pi \frac{1}{\left(1-\frac{1}{p^{1+\varrho}}\right)^2} \cdot \Pi \frac{1}{1-\frac{1}{q^{2+2\varrho}}},$$

gdzie p przebiega przez wszystkie liczby pierwsze rzeczywiste nieparzyste, q przez wszystkie liczby pierwsze rzeczywiste nieparzyste $4n+3$. A zatem gdy p przebiega przez wszystkie możliwe liczby pierwsze rzeczywiste, p_2 przez wszystkie takież liczby nieparzyste, będzie:

$$L_0(1+\varrho) < \Pi \frac{1}{1-\frac{1}{p_1^{1+\varrho}}} \cdot \Pi \frac{1}{1-\frac{(-1)^{\frac{p_2-1}{2}}}{p_2^{1+\varrho}}}$$

$$< \left(1+\frac{1}{2^{1+\varrho}}+\frac{1}{3^{1-\varrho}}+\ldots\right)\left(1-\frac{1}{3^{r+\varrho}}+\frac{1}{5^{1+\varrho}}-\ldots\right).$$

Lecz

$$1+\frac{1}{2^{2+\varrho}}+\frac{1}{3^{1+\varrho}}+\ldots < 1+\frac{1}{\varrho}\left(1-\frac{1}{2^\varrho}\right)+\frac{1}{\varrho}\left(\frac{1}{2^\varrho}-\frac{1}{3^\varrho}\right)+\ldots$$

$$< \frac{1+\varrho}{\varrho}$$

$$1-\frac{1}{3^{1+\varrho}}+\frac{1}{5^{1+\varrho}}-\frac{1}{7^{1+\varrho}}+\ldots < 1,$$

przeto;

$$L_0(1+\varrho) < \frac{1+\varrho}{\varrho}.$$

Otrzymujemy więc:

$$|L_k(1+\varrho)|^2 \frac{1+\varrho}{\varrho}(3C)^{r-3} > \Pi_h L_h(1+\varrho) > 1,$$

skąd wynika:

$$|L_h(1+\varrho)| > \sqrt{\frac{\varrho}{1+\varrho}} \cdot \frac{1}{(3C)^{\frac{r-3}{2}}}.$$

Na mocy ustępu **7.** będzie tedy:

$$L_k(1)+12C\varrho > \sqrt{\frac{\varrho}{1+\varrho}} \frac{1}{(3C)^{\frac{r-3}{2}}}.$$

lub

$$|L_k(1)| > \sqrt{\frac{\varrho}{1+\varrho}} \frac{1}{(3C)^{\frac{r-3}{2}}} - 12C\varrho.$$

Jeżeli przyjmiemy:

$$\varrho = \frac{1}{128} \frac{1}{(3C)^{r-1}},$$

będzie:

$$|L_k(1)| > \frac{1}{32} \cdot \frac{1}{(3C)^{r-2}}.$$

10. Liczba r jest zawsze parzysta. Albowiem $4r$ jest liczbą wszystkich liczb zupełnego układu reszt $\mathfrak{R}$, które są niepółdzielnemi z M. Ta liczba jest podzielna przez 8, jeżeli liczba M jest podzielna przez $(1+i)^4$. Gdy zaś liczba M jest tylko podzielna przez $(1+i)^3$, to zawiera przynajmniej jeszcze jeden czynnik pierwszy nieparzysty φ, $4r$ jest podzielne przez $4(N\varphi-1)$, a więc co najmniej przez 16. Równanie $\tau_1\tau_2\ldots\tau_\nu=r$ pokazuje tedy, że jeden lub więcej z wykładników $\tau_1, \tau_2, \ldots, \tau_\nu$ muszą być liczbami parzystemi. Ponieważ zaś w ciągu liczbowym $\tau_1, \tau_2, \ldots, \tau_\nu$ każda liczba dzieli się przez wszystkie po niej następujące, przeto liczby parzyste muszą w nim poprzedzać liczby nieparzyste. Niechaj więc $\tau_1, \tau_2, \ldots, \tau_\lambda$, o ile $\lambda<\nu$, będą liczbami parzystemi, $\tau_{\lambda+1}, \tau_{\lambda+2}, \ldots, \tau_\nu$ liczbami nieparzystemi. Idzie o wyznaczenie liczby λ.

Jeżeli ζ jest resztą kwadratową modułu M, zawartą w Ω, wtedy kongruencya

$$v^2 \equiv \zeta \pmod{M}$$

ma zawsze pierwiastek pierwotny, zawarty w układzie Ω. Jeżeli bowiem v jest jednym z pierwiastków tej kongruencyi, to ponieważ ζ jest liczbą pierwotną, będzie

$$v^2-1 = (v-1)(v+1) \equiv 0 \pmod{(1+i)^3},$$

i jedna z liczb $v+1$, $v-1$ musi być podzielna przez 2. Gdy zaś $\frac{v\mp1}{2}$ jest liczbą całkowitą, to i $\frac{v\mp1}{2}$ jest też liczbą całkowitą, i jedna z tych liczb ze względu na równanie:

$$\frac{v\mp1}{2} - \frac{v\mp1}{2} = \pm 1,$$

musi być podzielna przez $1+i$. Mamy zatem:

$$v \equiv \pm 1 \pmod{(1+i)^3},$$

i jest jasnem, że jeden z pierwiastków $v, -v$ jest pierwotny. Jeżeli więc v jest pierwiastkiem pierwotnym powyższej kongruencyi, to:

$$\mathrm{ind}_1\zeta \equiv 2\,\mathrm{ind}_1 v \pmod{\tau_1}, \quad \mathrm{ind}_2\zeta \equiv 2\mathrm{ind}_2 v \pmod{\tau_2}, \ldots, \mathrm{ind}_\lambda \zeta \equiv 2\mathrm{ind}_\lambda v \pmod{\tau_\lambda};$$

aby więc ζ było resztą kwadratową modułu M, jest koniecznem, by liczby $\mathrm{ind}_1\zeta$, $\mathrm{ind}_2, \ldots, \mathrm{ind}_\nu\zeta$ były parzyste. Warunek ten jest i wystarczający, jeżeli bowiem:

$$\mathrm{ind}_1\zeta = 2\alpha_1, \quad \mathrm{ind}_2\zeta = 2\alpha_2, \ldots\ldots, \mathrm{ind}_\lambda\zeta = 2\alpha_\lambda,$$

i położymy w przypadku $\nu > \lambda$;

$$\tfrac{1}{2}(1+\tau_{\lambda+1})\,\mathrm{ind}_{\lambda+1}\zeta = \alpha_{\lambda+1}, \ldots\ldots, \tfrac{1}{2}(1+\tau_\lambda)\,\mathrm{ind}_\nu\zeta = \alpha_\nu,$$

to będzie:

$$\zeta \equiv (g_1^{\alpha_1} g_2^{\alpha_2} \ldots\ldots g_\nu^{\alpha_\lambda} Q)^2 \pmod{M},$$

gdzie Q w przypadku $\lambda = \nu$ oznacza jedność, w przypadku $\lambda < \nu$ iloczyn $g_{\lambda+1}^{\alpha_{\lambda+1}}, \ldots, g_\nu^{\alpha_\nu}$. Otrzymamy tedy wszystkie reszty kwadratowe modułu M, zawarte w Ω, jeżeli za $\mathrm{ind}_1\zeta$ weźmiemy $\frac{\tau_1}{2}$ liczb $0, 2, 4, \ldots, \tau_1 - 2$; za $\mathrm{ind}_2\zeta$ weźmiemy $\frac{\tau_2}{2}$ liczb $0, 2, 4, \ldots, \tau_2 - 2, \ldots$ i t. d., za $\mathrm{ind}_\nu\zeta$ $\frac{1}{2}\tau_\lambda$ liczb $0, 2, 4, \ldots \tau_\lambda - 2$ w przypadku zaś $\nu > \lambda$ za $\mathrm{ind}_{\lambda+1}\zeta, \ldots, \mathrm{ind}_\nu\zeta$ odpowiednie wszystkie liczby $0, 1, 2, \ldots, \tau_{\lambda+1} - 1,\ 0, 1, 2, \ldots, \tau_\nu - 1$. Liczba wszystkich reszt kwadratowych modułu M, zawartych w Ω, jest przeto:

$$\frac{\tau_1 \tau_2 \ldots\ldots \tau_\nu}{2^\lambda} = \frac{r}{2^\lambda}.$$

Można tę liczbę wyznaczyć jeszcze innym sposobem.

Utwórzmy kwadraty wszystkich liczb, zawartych w układzie Ω, i dobierzmy w Ω liczby, przystające do nich według modułu M, to otrzymamy zbiór J, złożony z r liczb, który zawiera tylko reszty kwadratowe liczby M i każdą resztę kwadratową tej liczby M, zachodzącą w Ω, zawierać musi. Aby otrzymać przeto liczbę wszystkich reszt kwadratowych modułu M, zawartych w układzie Ω, dość wyznaczyć, ile razy jedna i ta sama liczba występuje w zbiorze J.

W tym celu oznaczmy przez v_0 jednę liczbę określoną, przez v każdą

zaś liczbę z układu Ω, takie, że do ich kwadratów przystaje liczba ζ według modułu M. Jeżeli położymy:

$$v \equiv v_0 w \pmod{M},$$

to w będzie liczbą pierwotną i czynić będzie zadość kongruencyi $w^2 \equiv 1 \pmod{M}$. Odwrotnie, niechaj w będzie jakimkolwiek pierwiastkiem pierwotnym tej kongruencyi, v liczbą, przystającą do iloczynu $v_0 w$ w układzie Ω według modułu M, to będzie:

$$v^2 \equiv v_0^2 w^2 \equiv v_0^2 \equiv \zeta \pmod{M}.$$

Otrzymujemy przeto wszystkie liczby w Ω, do których kwadratów przystaje ζ według modułu M, jeżeli v_0 pomnożymy przez wszystkie pierwiastki pierwotne kongruencyi $w^2 \equiv 1 \pmod{M}$ i poszukamy w układzie Ω liczb, przystających do tych iloczynów według modułu M. Jeżeli więc $\varkappa$ jest liczbą pierwiastków pierwotnych tej kongruencyi, to w zbiorze J każde $\varkappa$ liczb zlewają się ze sobą, a $\frac{r}{\varkappa}$ liczb różnych daje nam wszystkie reszty kwadratowe modułu M, zachodzące w Ω; będzie tedy $2^\lambda = \varkappa$, i pozostaje jeszcze wyznaczyć $\varkappa$.

Jeżeli:

$$M = (1+i)^\sigma \mathfrak{p}^\alpha \mathfrak{q}^\beta,$$

gdzie $\mathfrak{p}, \mathfrak{q}, \ldots$ są liczby zespolone nieparzyste, to kongruencya $w^2 - 1 = 0$ musi mieć miejsce ze względu na każdy z modułów $(1+i)^\sigma$, $\mathfrak{p}^\alpha$, $\mathfrak{q}^\beta$, przeto w ze względu na te moduły przystaje odpowiednio do pierwiastków $\alpha, \beta, \gamma, \ldots$. kongruencyj:

$$z^2 \equiv 1 \pmod{(1+i)^\sigma}, \quad z^2 \equiv 1 \pmod{\mathfrak{p}^\alpha}, \quad z^2 \equiv 1 \pmod{\mathfrak{q}^\beta}, \ldots\ldots,$$

z których to pierwiastków α musi być pierwotnym, jeżeli w jest pierwiastkiem pierwotnym. Odwrotnie, jeżeli za α weźmiemy pierwiastek pierwotny pierwszej kongruencyi, za $\beta, \gamma, \ldots$ pierwiastki dowolne pozostałych kongruencyj, i następnie wyznaczymy w tak, aby zachodziły kongruencye:

$$w \equiv \alpha \pmod{(1+i)^\sigma}, \quad \equiv \beta \pmod{\mathfrak{p}^\alpha}, \quad \equiv \lambda \pmod{\mathfrak{q}^\beta}, \ldots\ldots$$

to w będzie pierwiastkiem pierwotnym kongruencyi $z^2 \equiv 1 \pmod{M}$. Jeżeli więc $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ są liczby pierwiastków pierwotnych α i pierwiastków $\beta, \gamma, \ldots$, będzie $\varkappa = \mathfrak{A}\mathfrak{B}\mathfrak{C}\ldots\ldots$ Jeżeli weźmiemy $\alpha = 1 + (1+i)^3\xi$, to kongruencya

$$\alpha^2 - 1 \equiv (\alpha - 1)(\alpha + 1) \equiv 0 \pmod{(1+i)^\sigma},$$

po zniesieniu czynnika $(1+i)^3$, przechodzi na kongruencyę:

$$2(1+i(1+i)\xi) = 0 \pmod{(1+i)^{\sigma-3}}.$$

Przeto ξ nie podlega żadnemu warunkowi, gdy $\sigma=3,4$; α w przypadku $\sigma=3$ ma jednę tylko wartość 1. w przypadku $\sigma=4$ dwie wartości 1, $1+(1+i)^3$. Począwszy od $\sigma=5$ mamy:

$$(1+i(1+i)\xi) \equiv 0 \pmod{(1+i)^{\sigma-5}},$$

i ξ musi być podzielne przez $(1+i)^{\sigma-5}$. Jeżeli położymy $\xi=(1+i)^{\sigma-5}\eta$, to będzie $\alpha=1+(1+i)^{\sigma-2}\eta$, gdzie η może przyjmować tylko cztery wartości: $0, i, 1, 1+i$, jeżeli wartości α mają być nieprzystającemi do siebie według modułu $(1+i)^\sigma$; α przeto ma cztery wartości.

Jeżeli liczba M jest podzielna przez potęgi $\mathfrak{p}^a, \mathfrak{q}^b$ liczb zespolonych nieparzystych, to kongruencya

$$\beta^2-1 = (\beta-1)(\beta+1) \equiv 0 \pmod{\mathfrak{p}^a}$$

może zachodzić tylko w ten sposób, że jeden z czynników $\beta-1$, $\beta+1$ jest podzielny przez $\mathfrak{p}^a$, gdyż ich różnica 2 jest niespółdzielna z liczbą $\mathfrak{p}$; istnieją więc tylko dwa pierwiastki $\beta=1$, $\beta=-1$. Podobnież i γ może mieć tylko dwa pierwiastki 1, -1 i t. d. Mamy zatem: $\mathfrak{A}=1,2,4$ dla $\sigma=3$, 4, >4 oraz $\mathfrak{B}=\mathfrak{C}=\ldots=2$.

Jeżeli przeto π jest liczbą czynników pierwszych nieparzystych modułu M, będzie $\varkappa=2^\pi$, $2^{\pi-1}$, $2^{\pi+2}$, stosownie do tego, czy $\sigma=3,4,>4$.

Stąd wynika:

$$\lambda=\pi \text{ dla } \sigma=3; \quad \lambda=\pi+1 \text{ dla } \sigma=4; \quad \lambda=\pi+2 \text{ dla } \sigma>4.$$

11. Niechaj $m=\xi+i\eta$ będzie liczbą nieparzystą pierwotną, ϑ dzielnikiem nieparzystym pierwotnym modułu M, nie zawierającym żadnego dzielnika kwadratowego prócz ± 1; $\left[\frac{m}{\vartheta}\right]$ niechaj będzie symbolem, utworzonym analogicznie do symbolu Legendre'a-Jacobi'ego w teoryi liczb zespolonych. Liczba różnych dzielników ϑ, a więc i różnych wyrażeń $\left[\frac{m}{\vartheta}\right]$, jest 2^π.

Niechaj dalej $\chi(m)$ oznacza: w przypadku $\sigma=3$ jedno którekolwiek z wyrażeń $\left[\frac{m}{\vartheta}\right]$; w przypadku $\sigma=4$ którekolwiek z wyrażeń:

$$\left[\frac{m}{\vartheta}\right], \quad (-1)^{\frac{\xi^2+\eta^2-1}{4}}\left[\frac{m}{\vartheta}\right];$$

w przypadku $\sigma>4$ którekolwiek z wyrażeń:

$$\left[\frac{m}{\vartheta}\right], \quad (-1)^{\frac{\xi^2+\eta^2-1}{4}}\left[\frac{m}{\vartheta}\right], \quad (-1)^{\frac{(\xi+\eta)^2-1}{8}}\left[\frac{m}{\vartheta}\right],$$
$$(-1)^{\frac{\xi^2+\eta^2-1}{4}}\cdot(-1)^{\frac{(\xi+\eta)^2-1}{8}}\left[\frac{m}{\vartheta}\right].$$

Liczba różnych wyrażeń $\chi(m)$ jest 2^λ i każde z nich ma własność $\chi(mm')=\chi(m)\chi(m')$, gdy m i m' są liczbami pierwotnemi nieparzystemi.

Do każdego z wyrażeń $\chi(m)$ z wyjątkiem $\left[\frac{m}{1}\right]$ można dobrać liczby pierwotne $m=\xi+i\eta$ czyniące zadość warunkowi $\chi(m)=-1$.

Jeżeli $\chi(m)$ ma czynnik $(-1)^{\frac{\xi^2+\eta^2-1}{4}}$, to szukajmy liczby m, czyniącej zadość kongruencyom:

$$m \equiv 1+(1+i)^3 \pmod{(1+i)^\sigma}, \quad m \equiv 1 \left(\mathrm{mod.}\ \frac{M}{(1+i)^\sigma}\right);$$

ta liczba jest pierwotna, a ponieważ jest tu $\sigma>3$, przeto:

$$\xi^2+\eta^2 = N(m) \equiv N(-1+2i) \equiv 5 \pmod 8,$$

a więc:

$$(-1)^{\frac{\xi^2+\eta^2-1}{4}} = -1.$$

Wszystkie inne czynniki, ewentualnie zachodzące w liczbie $\chi(m)$, mają wartość 1.

Dla czynnika $(-1)^{\frac{(\xi+\eta)^2-1}{8}}$, gdy zachodzi, wynika to stąd, że wtedy $\sigma>4$, a przeto ξ, η mają postać $-1+4(x-y)$, $2+4(x-y)$ i jest $\xi+\eta\equiv 1 \pmod 8$. Jeżeli zachodzi czynnik $(-1)^{\frac{\xi^2+\eta^2-1}{4}}$, niema zaś czynnika $(-1)^{\frac{\xi^2+\eta^2-1}{4}}$, to $\sigma>4$; położymy:

$$m \equiv 1+i(1+i)^3 \pmod{(1+i)^\sigma}: \quad m \equiv 1 \left(\mathrm{mod.}\ \frac{M}{(1+i)^\sigma}\right);$$

m jest liczbą pierwotną i będzie $\xi+\eta \equiv -3 \pmod\sigma$, a zatem $(-1)^{\frac{(\xi+\eta)^2-1}{8}} = -1$, gdy pozostałe ewentualne czynniki wyrażenia $\chi(m)$ mają wartość 1.

Jeżeli nakoniec $\chi(m)$ jest wyrażeniem $\left[\frac{m}{\vartheta}\right]$, $\mathfrak{p}$ czynnikiem pierwszym liczby ϑ, którego potęga a-ta jest dzielnikiem modułu, to niechaj będzie $\vartheta=p\vartheta'$, m_1 resztą kwadratową liczby $\mathfrak{p}$, i położymy:

$$m \equiv m_1 \pmod{\mathfrak{p}^a}. \qquad m \equiv 1 \left(\mathrm{mod.}\ \frac{M}{\mathfrak{p}^a}\right);$$

m jest liczbą pierwotną i będzie:

$$\left[\frac{m}{\vartheta}\right] = \left[\frac{m}{\mathfrak{p}}\right]\left[\frac{m}{\vartheta'}\right] = \left[\frac{m_1}{\mathfrak{p}}\right]\left[\frac{1}{\vartheta'}\right] = \left[\frac{m_1}{\mathfrak{p}}\right] = -1.$$

Ponieważ każda liczba pierwotna m, niespółdzielna z modułem M, czyni zadość kongruencyi:

$$m \equiv g_1^{\mathrm{ind}_1 m}\, g_2^{\mathrm{ind}_2 m} \ldots\ldots g_\nu^{\mathrm{ind}_\nu m} \pmod{M},$$

to:

$$\chi(m) = \chi(g_1^{\mathrm{ind}_1 m}\, g_2^{\mathrm{ind}_2 m} \ldots\ldots g_\nu^{\mathrm{ind}_\nu m}),$$
$$= \chi(g_1)^{\mathrm{ind}_1 m}\, \chi(g_2)^{\mathrm{ind}_2 m} \ldots\ldots \chi(g_\nu)^{\mathrm{ind}_\nu m}.$$

O ile $\nu > \lambda$, czynniki $\chi(g_{\lambda+1})^{\mathrm{ind}_{\lambda+1} m}, \ldots, \chi(g_\nu)^{\mathrm{ind}_\nu m}$ mają wszystkie wartość 1, jak to widać z równań:

$$\chi(g_{\lambda+1}) = \chi(g_{\lambda+1}^{1+\tau_{\lambda+1}}) = \chi(g_{\lambda+1})^{1+\tau_{\lambda+1}}, \ldots\ldots, \chi(g_\nu) = \chi(g_\nu^{1+\tau_\nu}) = \chi(g_\nu)^{1+\tau_\nu},$$

i będzie:

$$\chi(m) = \chi(g_1)^{\mathrm{ind}_1 m},\ \chi(g_2)^{\mathrm{ind}_2 m},\ \ldots\ldots,\ \chi(g_\lambda)^{\mathrm{ind}_\nu m}.$$

Jeżeli przeto $\chi(m)$ jest różne od $\left[\frac{m}{1}\right]$, to przynajmniej jedna z liczb $\chi(g_1), \chi(g_2), \ldots, \chi(g_\lambda)$ musi być ujemna, a liczby $\chi(_1), \chi(g_2), \ldots, \chi(g_\nu)$ tworzą połączenie pierwiastków $\omega_1, \omega_2, \ldots, \omega_\nu$, w którem wszystkie pierwiastki mają jednę z wartości 1, -1, ale nie wszystkie wartość 1. Jeżeli to połączenie pierwiastków jest h-tem, to $h > 0$, $c_{h,m} = \chi(m)$.

Różnym wyrażeniom $\chi(m)$ odpowiadają różne liczby h. Iloczyn bowiem dwóch różnych wyrażeń $\chi(m)$, np. wyrażeń $\chi_1(m)$ i $\chi_2(m)$ jest znów wyrażeniem $\chi(m)$, różnem od $\left[\frac{m}{1}\right]$, i dlatego można znaleść liczbę pierwotną m, niespółdzielną z modułem M, która czyni zadość kongruencyi $\chi_1(m)\,\chi_2(m) \equiv -1$, tak że nie dla każdego m może być $\chi_1(m) = \chi_2(m)$.

Ponieważ tedy tak liczba połączeń pierwiastków $\omega_1, \omega_2, \ldots, \omega_\nu$, składających się tylko z pierwiastków rzeczywistych ± 1, z wyłączeniem połączenia 0-ego, jak i liczba wszystkich wyrażeń $\chi(m)$ różnych od $\left[\frac{m}{1}\right]$ wynosi $2^\lambda - 1$, przeto jest jasnem, że każde wyrażenie $c_{h,m}$ odpowiadające rzeczonym połączeniom pierwiastków, jest identyczne zjednem z wyrażeń $\chi(m)$ dla wszystkich liczb pierwotnych m, niespółdzielnych z modułem M.

12. Jeżeli q jest liczbą pierwszą rzeczywistą $4n+3$, $m = \xi + i\eta$ liczbą niespółdzielną z q, to:

$$(\xi + i\eta)^q \equiv \xi^q + i^q \eta^q \equiv \xi - i\eta \pmod{q},$$

a więc po pomnożeniu przez $\xi + i\eta$;

$$(\xi + i\eta)^{q+1} \equiv \xi^q \equiv \xi^2 + \eta^2 \pmod{q}.$$

Jeżeli podniesiemy obie strony do potęgi $\frac{q-1}{2}$, będzie:

$$(\xi + i\eta)^{\frac{1}{2}(q^2-1)} \equiv (\xi^2 + \eta^2)^{\frac{1}{2}(q-1)} \pmod{q},$$

a stąd:

$$\left[\frac{\xi + i\eta}{q}\right] = \left(\frac{\xi^3 + \eta^2}{q}\right),$$

gdzie $\left(\frac{\xi^2+\eta^2}{q}\right)$ jest zwykłym symbolem Legendre'a.

Niechaj $\mathfrak{p}$ będzie dwuwyrazową liczbą zespoloną, $\mathfrak{p}'$ liczbą z nią sprzężoną, $m = \xi + i\eta$ liczbą niespółdzielną z $\mathfrak{p}\mathfrak{p}' = p$, to:

$$(\xi + i)^{\frac{1}{2}(p-1)} \equiv \left[\frac{m}{\mathfrak{p}}\right] \pmod{\mathfrak{p}}.$$

Po pomnożeniu obu stron przez $(\xi - i\eta)^{\frac{1}{2}(p-1)}$, otrzymujemy:

$$(\xi^2 + \eta^2)^{\frac{1}{2}(p-1)} \equiv \left[\frac{m}{\mathfrak{p}}\right] (\xi - i\eta)^{\frac{1}{2}(p-1)} \pmod{\mathfrak{p}},$$

ale ponieważ:

$$(\xi^2 + \eta^2)^{\frac{1}{2}(p-1)} \equiv \left(\frac{\xi^2+\eta^2}{p}\right) \pmod{\mathfrak{p}};$$

będzie przeto:

$$\left(\frac{\xi^2+\eta^2}{p}\right) \equiv \left[\frac{m}{\mathfrak{p}}\right] (\xi - i\eta)^{\frac{1}{2}(p-1)} \pmod{\mathfrak{p}},$$

tak: że, jeżeli zamiast i weźmiemy $-i$:

$$\left(\frac{\xi^2+\eta^2}{p}\right) \equiv \left[\frac{m}{\mathfrak{p}}\right] m^{\frac{1}{2}(p-1)} \pmod{\mathfrak{p}'}.$$

Ze względu zaś na kongruencyę:

$$m^{\frac{1}{2}(p-1)} \equiv \left[\frac{m}{\mathfrak{p}'}\right] \pmod{\mathfrak{p}'},$$

będzie stąd:

$$\left(\frac{\xi^2+\eta^2}{p}\right) \equiv \left[\frac{m}{\mathfrak{p}}\right]\left[\frac{m}{\mathfrak{p}'}\right] \pmod{\mathfrak{p}'}$$

$$= \left[\frac{m}{\mathfrak{p}}\right]\left[\frac{m}{\mathfrak{p}'}\right] = \left[\frac{m}{p}\right],$$

Dla każdej liczby rzeczywistej nieparzystej k jest przeto [1]):

$$\left[\frac{\xi+i\eta}{k}\right] = \left(\frac{\xi^2+\eta^2}{k}\right).$$

13. Można wykazać, że każdy z szeregów $L_h(1)$, odpowiadających połączeniom pierwiastków $\omega_1, \omega_2, \ldots, \omega_\nu$, składającym się z samych pierwiastków rzeczywistych, prócz połączenia 0-ego, ma sumę różną od zera

Wyrażenie $\chi(m)$, zlewające się z $c_{h,m}$ dla wszystkich liczb pierwotnych m, nie spółdzielnych z modułem M, może albo być funkcyą liczby Nm, albo nią nie być.

Jeżeli $\chi(m)$ jest jednem z wyrażeń:

$$(-1)^{\frac{Nm-1}{4}}, \quad \left[\frac{m}{k}\right], \quad (-1)^{\frac{Nm-1}{4}}\left[\frac{m}{k}\right],$$

gdzie k oznacza dzielnik rzeczywisty jednowyrazowy nieparzysty modułu M i jeżeli położymy odpowiednio:

$$\vartheta(n) = (-1)^{\frac{n^2-1}{8}}, \quad = \left(\frac{n}{k}\right), \quad = (-1)^{\frac{n^2-1}{8}}\left(\frac{n}{k}\right),$$

będzie:

$$\chi(m) = \vartheta(Nm).$$

Jeżeli nadto napiszemy:

$$f(n) = \Sigma(-1)^{\frac{1}{2}(\delta-1)}, \quad \Pi\left(1 - \frac{\vartheta(N\mathfrak{p})}{N\mathfrak{p}}\right) = Q,$$

gdzie suma Σ rozciąga się na wszystkie dzielniki δ nieparzystej liczby n,

[1]) Lejeune-Dirichlet l. c.

iloczyn Π na wszystkie dzielniki pierwsze zespolone nieparzyste modułu M, to $f(n)$ będzie liczbą przedstawień liczby n, jako normy liczby pierwotnej zespolonej, i będzie:

$$L_h(1) = Q\,\Sigma\,\frac{f(n)\,\vartheta(1)}{n},$$

gdzie n przyjmuje wszystkie wartości dodatnie nieparzyste. Lecz mamy [1]):

$$\sum \frac{\vartheta(n)\,f(n)}{n} = \sum \frac{\vartheta(n)}{n} \cdot \sum \frac{(-1)^{\frac{1}{2}(n-1)}\vartheta(n)}{n},$$

a przeto:

$$L_h(1) = Q \sum \frac{\vartheta(n)}{n} \cdot \sum (-1)^{\frac{1}{2}(n-1)} \frac{\vartheta(n)}{n}.$$

Z dowodu zaś twierdzenia o istnieniu nieskończenie wielu liczb pierwszych w szeregu arytmetycznym rzeczywistym wiemy [2]), że szeregi

$$\frac{\vartheta(1)}{1} + \frac{\vartheta(3)}{3} + \frac{\vartheta(5)}{5} + \frac{\vartheta(7)}{7} + \ldots\ldots,$$

$$\frac{\vartheta(1)}{1} - \frac{\vartheta(3)}{3} + \frac{\vartheta(5)}{5} - \frac{\vartheta(7)}{7} + \ldots\ldots,$$

mają sumy różne od zera.

Jeżeli $\chi(m)$ jest jednem z wyrażeń:

$$(-1)^{\frac{(\xi+\eta)^2-1}{8}}, \quad \left[\frac{m}{\alpha+i\beta}\right], \quad (-1)^{\frac{(\xi+\eta)^2-1}{8}}\left[\frac{m}{\alpha+i\beta}\right],$$

gdzie $\xi+i\eta=m$, $\alpha+i\beta$ zaś przedstawia dzielnik dwuwyrazowy zespolony liczby M, to $\chi(m)$ nie jest funkcyą liczby Nm. Niechaj będzie w tym przypadku $H=\frac{N(M)}{2^\sigma}$, m' liczbą sprzężoną z m i odpowiednio do powyższych trzech wyrażeń:

$$\vartheta(n) = (-1)^{\frac{n^2-1}{8}}\left(\frac{n}{H^2}\right), \quad \vartheta(n) = \left(\frac{n}{k}\right)\left(\frac{n}{H^2}\right),$$

$$\vartheta(n) = (-1)^{\frac{n^2-1}{8}}\left(\frac{n}{k}\right)\left(\frac{n}{H^2}\right),$$

[1]) Mertens, Ueber Dirichlet'sche Reihen, Wien. Sitzungsber. CIV. Ueber Multiplication und Nichtverschwinden Dirichlet'scher Reihen, Crelle's Journal CXVII.

[2]) Mertens, Eine asymptotische Aufgabe, Wien. Sitzungsber. CVIII.

gdzie $k=N\left(\frac{\alpha+\gamma\beta}{\gamma}\right)$, γ zaś oznacza największy wspólny dzielnik α i β. Mamy wtedy ogólnie:

$$c_{hm}\,.\,c_{hm'}=c_{h,mm'}=\vartheta(Nm).$$

Jeżeli napiszemy:

$$L(1+\varrho)=\Pi\frac{1}{1-\frac{1}{(N\mathfrak{p})^{1+\varrho}}},$$

gdzie iloczyn rozciąga się na wszystkie liczby zespolone pierwsze nieparzyste i pierwotne $\mathfrak{p}$, to będzie:

$$\log L_h(1+\varrho)+\frac{1}{2}\log L(1+\varrho)$$

$$=\sum\frac{\frac{1}{2}+c_{h,\mathfrak{p}}}{(N\mathfrak{p})^{1+\varrho}}+\sum\frac{\frac{1}{2}+c^2_{h,\mathfrak{p}}}{(N\mathfrak{p})^{2+2\varrho}}+\ldots\ldots,$$

gdzie sumy odnoszą się dla rzeczonych liczb pierwszych. Dla każdej pary liczb dwuwyrazowych pierwotnych sprzężonych $\mathfrak{p}$, $\mathfrak{p}'$ jest atoli:

$$\frac{1}{2}+c^{\mu}_{h,\mathfrak{p}}+\frac{1}{2}+c^{\mu}_{h,\mathfrak{p}'}=(1+c^{\mu}_{h,\mathfrak{p}})(1+c^{\mu}_{h,\mathfrak{p}'})-c^{\mu}_{h,\mathfrak{p}\mathfrak{p}'}$$

$$\leqq-c^{\mu}_{h,\mathfrak{p}\mathfrak{p}'}\geqq-\vartheta(N\mathfrak{p})^{\mu},$$

a dla każdej jednowyrazowej liczby zespolonej $\mathfrak{p}$ jest:

$$\frac{1}{2}+c^{\mu}_{h,\mathfrak{p}}=\frac{1}{2}(1+c^{\mu}_{h,\mathfrak{p}})^2-\frac{1}{2}(c^{\mu}_{h,\mathfrak{p}})^2\geqq-\frac{1}{2}c^{\mu}_{h,\mathfrak{p}\mathfrak{p}}\geqq-\frac{1}{2}\vartheta(N\mathfrak{p})^{\mu}$$

Jeżeli więc pomyślimy sobie ściągnięte każde dwa wyrazy, odpowiadające dwom liczbom pierwszym dwuwyrazowym sprzężonym, otrzymamy:

$$\sum\frac{\frac{1}{2}+c^{\mu}_{h,\mathfrak{p}}}{(N\mathfrak{p})^{\mu+\mu\varrho}}\geqq-\frac{1}{2}\sum\frac{\vartheta(N\mathfrak{p})^{\mu}}{(N\mathfrak{p})^{\mu+\varrho\mu}},$$

gdzie $\mathfrak{p}$ w obu sumach przebiega przez wszystkie liczby pierwsze zespolone pierwotne nieparzyste, i będzie:

$$\log L_h(1+\varrho)+\frac{1}{2}\log L(1+\varrho)\geqq-\frac{1}{2}\log\Pi\frac{1}{1-\frac{\vartheta(N\mathfrak{p})}{(N\mathfrak{p})^{1+\varrho}}},$$

a więc także:

$$L_h(1+\varrho)\,L(1+\varrho)^{\frac{1}{2}}\left(\Pi\frac{1}{1-\frac{\vartheta N\mathfrak{p}}{(N\mathfrak{p})^{1+\varrho}}}\right)^{\frac{1}{2}}\geqq 1.$$

Lecz gdy n przebiega przez wszystkie liczby dodatnie nieparzyste, jest:

$$\Pi\frac{1}{1-\frac{\vartheta N\mathfrak{p}}{(N\mathfrak{p})^{1+\varrho}}}=\sum\frac{\vartheta(n)\,f(n)}{n^{1+\varrho}}$$

$$=\sum\frac{\vartheta(n)}{n^{1+\varrho}}\cdot\sum\frac{(-1)^{\frac{n-1}{2}}\vartheta(n)}{n^{1+\varrho}}.$$

Ponieważ sumy:

$$\vartheta(1)+\vartheta(3)+\vartheta(5)+\ldots\ldots+\vartheta(2s-1),$$

$$\vartheta(1)-\vartheta(3)+\vartheta(5)-\ldots\ldots\pm\vartheta(2s-1)$$

dla żadnej wartości s nie przekraczają liczby wyznaczyć się dającej C_1, to znajdujemy sposobem znanym:

$$\left|\sum\frac{\vartheta(n)}{n^{1+\varrho}}\right|<C_1,\quad\left|\sum(-1)^{\frac{n-1}{2}}\frac{\vartheta(n)}{n^{1+\varrho}}\right|<C_1.$$

a zatem:

$$\Pi\frac{1}{1-\frac{\vartheta N\mathfrak{p}}{(N\mathfrak{p})^{1+\varrho}}}<C_1{}^2.$$

Ponieważ dalej:

$$L(1+\varrho)=\sum\frac{1}{n^{1+\varrho}}\cdot\sum\frac{(-1)^{\frac{n-1}{2}}}{n^{1+\varrho}}<\frac{1+\varrho}{\varrho},$$

a według ust. 7:

$$L_h(1+\varrho)<|L_h(1)|+12\,C\varrho,$$

to będzie:

$$(|L_h(1)|+12\,C\varrho)\sqrt{\frac{1+\varrho}{\varrho}}\,.\,C_1>1,$$

a stąd:

$$|L_h(1)|>\sqrt{\frac{\varrho}{1+\varrho}}\frac{1}{C_1}-12\,C\varrho.$$

W szczególności, gdy $\varrho = \frac{1}{2 \cdot 24^2 C^2 C_1^2}$, otrzymujemy:

$$|L_h(1)| > \frac{1}{96\, C\, C_1^2}.$$

14. Niechaj będzie:

$$A_h(s) = \sum_1^s \frac{c_{h,\mathfrak{p}} \log N\mathfrak{p}}{N\mathfrak{p}}, \quad H_h(s) = \sum_1^s \frac{c_{h,m} \log Nm}{Nm},$$

$$K_h(s) = \sum_1^s \frac{c_{h,m}}{Nm},$$

gdzie $\mathfrak{p}$ przebiega przez wszystkie liczby zespolone pierwsze nieparzyste, m przez wszystkie liczby zespolone pierwotne, których normy nie są większe od s. Przez rozkład każdej liczby m na jej czynniki pierwsze pierwotne znajdujemy znanym sposobem:

$$H_h(s) = \sum \frac{c_{h,\mathfrak{p}} \log N\mathfrak{p}}{N\mathfrak{p}} K_h\left(\frac{s}{N\mathfrak{p}}\right) + \sum \frac{c^2_{h,\mathfrak{p}} \log N\mathfrak{p}}{(N\mathfrak{p})^2} K_h\left(\frac{s}{N^2\mathfrak{p}}\right)$$
$$+ \sum \frac{c^3_{h,\mathfrak{p}} \log N\mathfrak{p}}{(N\mathfrak{p})^3} K_h\left(\frac{s}{N^3\mathfrak{p}}\right) + \ldots\ldots,$$

gdzie suma pierwsza, druga, trzecia, ... obejmują wszystkie liczby pierwsze pierwotne $\mathfrak{p}$, których normy nie przekraczają potęgi pierwszej drugiej, trzeciej . . . . . liczby s. Lecz jest:

$$K_h\left(\frac{s}{N\mathfrak{p}}\right) = L_h(1) + [4\,C] \sqrt{\frac{N\mathfrak{p}}{s}},$$

a przeto:

$$\sum \frac{c_{h,\mathfrak{p}} \log N\mathfrak{p}}{N\mathfrak{p}} K_h\left(\frac{s}{N\mathfrak{p}}\right) = L_h(1) A_h(s) = \frac{4\,C}{\sqrt{s}} \left| \sum \frac{\log N\mathfrak{p}}{\sqrt{N\mathfrak{p}}} \right|.$$

Ponieważ $N\mathfrak{p}$ jest albo liczbą rzeczywistą pierwszą $4n+1$ albo kwadratem p^2 liczby pierwszej rzeczywistej $4n+3$, a w tym ostatnim przypadku $\frac{1}{\sqrt{N\mathfrak{p}}} < \frac{1}{\sqrt{p}}$, otrzymujemy więc:

$$\sum \frac{\log N\mathfrak{p}}{\sqrt{N\mathfrak{p}}} \leqq 2 \sum \frac{\log p}{\sqrt{p}},$$

gdzie p przebiega przez wszystkie liczby pierwsze aż do granicy s.

Położymy $\sum_1^z \log p = F(z)$, to będzie:

$$\sum \frac{\log p}{\sqrt{p}} = \frac{F(2)}{\sqrt{2}} + \frac{F(3)-F(2)}{\sqrt{3}} + \frac{F(4)-F(3)}{\sqrt{4}} + \ldots + \frac{F(s)-F(s-1)}{\sqrt{s}}$$
$$= F(2)\left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{3}}\right) + F(3)\left(\frac{1}{\sqrt{3}} - \frac{1}{\sqrt{4}}\right) + \ldots + F(s-1)\left(\frac{1}{\sqrt{s-1}} - \frac{1}{\sqrt{s}}\right) + \frac{F(1)}{\sqrt{s}};$$

ponieważ wszakże [1]) $F(z) < 2z$, przeto:

$$F(k)\left(\frac{1}{\sqrt{k}} - \frac{1}{\sqrt{k+1}}\right) < \frac{2k}{\sqrt{k}\sqrt{k+1}\,(\sqrt{k}+\sqrt{k+1})} < \frac{1}{\sqrt{k+1}},$$
$$< 2\sqrt{k+1} - 2\sqrt{k};$$

wynika stąd:

$$\sum_1^s \frac{\log p}{\sqrt{p}} < 4\sqrt{s}, \qquad \sum \frac{\log N\mathfrak{p}}{\sqrt{N\mathfrak{p}}} < 8\sqrt{s},$$

a więc:

$$\sum \frac{c_{h,\mathfrak{p}} \log N\mathfrak{p}}{N\mathfrak{p}} K_h\left(\frac{s}{N\mathfrak{p}}\right) = L_h(1) A_h(s) + [32\,C].$$

Jeżeli p oznacza każdą liczbę pierwszą $4n+1$, q każdą liczbę pierwszą $4n+3$, mamy:

$$\sum \frac{c^2_{h,\mathfrak{p}}}{(N\mathfrak{p})^2} \log N\mathfrak{p}\, K_h\left(\frac{s}{N\mathfrak{p}^2}\right) = \left[\sum \frac{\log N\mathfrak{p}}{(N\mathfrak{p})^2} \cdot 3\,C\right]$$
$$= 6\,C\left[\sum_2^\infty \frac{\log p}{p^2} + \sum_2^\infty \frac{\log q}{q^4}\right],$$

$$\sum \frac{c^3_{h,\mathfrak{p}}}{(N\mathfrak{p})^3} \log N\mathfrak{p}\, K_h\left(\frac{s}{N^3\mathfrak{p}}\right) = \left[\sum \frac{\log N\mathfrak{p}}{(N\mathfrak{p})^3} 3\,C\right]$$
$$= 6\,C\left[\sum_2^\infty \frac{\log p}{p^3} + \sum_2^\infty \frac{\log q}{q^6}\right]$$

. . . . . .

[1]) Mertens, Ein Beitrag zur analytischen Zahlentheorie, Crelle's Journal LXXVIII.

Znajdujemy stąd:

$$H_h(s) = L_h(1)\,\Lambda_h(s) + \left[32C + 6C\sum_2^p \frac{\log p}{p(p-1)} + 6C\sum_2^\infty \frac{\log q}{q^2(q^2-1)}\right],$$

i ponieważ $L_h(1)$ jest różne od zera, można wyznaczyć granicę G tak, aby było:

$$\Lambda_h(s) = [G].$$

15. Jeżeli wyznaczymy l z kongruencyi:

$$Ll \equiv 1 \pmod{M},$$

będzie:

$$\sum \frac{\log Np}{Np} = \frac{1}{r}\cdot\left(c_{0,l}\Lambda_0(s) + c_{2,l}\Lambda_1(s) + \ldots + c_{r+1,l}\Lambda_{r-1}(s)\right),$$

gdzie suma rozciąga się na wszystkie liczby pierwotne nieparzyste p, przedstawialne za pomocą formy $L+Mz$ i o normie, nie przekraczającej granicy s.

Otóż, jeżeli p oznacza każdą liczbę rzeczywistą $4n+1$, q każdą liczbę rzeczywistą pierwszą $4n+3$, $\mathfrak{p}_0$ każdą liczbę pierwszą zespoloną pierwotną dwuwyrazową, przedstawialną przez formę $L+Mz$, jest:

$$\sum_1^s \frac{\log N\mathfrak{p}}{N\mathfrak{p}} = \sum_2^\infty \frac{\log N\mathfrak{p}_0}{N\mathfrak{p}_0} + \left[2\sum \frac{\log q}{q^2}\right]$$

$$\Lambda_0(s) = 2\sum_1^s \frac{\log p}{p} + 2\sum_1^s \frac{\log q}{q^2} - \sum_1^s \frac{\log N\varphi_1}{N\varphi_1},$$

gdzie $N\varphi_1$ przebiega przez wszystkie dzielniki pierwsze zespolone modułu M, których normy nie przekraczają liczby s. Można przeto wyznaczyć [1]) granicę G_0 taką, aby było:

$$\Lambda_0(s) - \log s = [G_0].$$

Stąd otrzymujemy:

$$\sum_1^s \frac{\log N\mathfrak{p}_0}{N\mathfrak{p}_0} = \frac{1}{r}\log s + \left[\frac{1}{r}G_0 + \frac{r-1}{r}G + 2\sum_1^\infty \frac{\log q}{q^2}\right].$$

---

[1]) Mertens, l. c.

SPRAWOZDANIA Z PIŚMIENNICTWA POLSKIEGO

W DZIEDZINIE NAUK MATEMATYCZNO-FIZYCZNYCH.

ROK 1898.

I. MATEMATYKA.

1. **Arvay W.** *Wyznaczenie paru granic w teoryi powierzchni.* Prace matem. fiz, t. IX, str. 164—169.

Miara krzywizny Gaussa i miara krzywizny Casorati'ego są granicami stosunków pewnych całek powierzchniowych, gdy pole, na które całki te są rozpostarte, dąży do zera. Wyznaczenie takich granic w innych przypadkach prowadzi do funkcyj zależnych tylko od głównych promieni krzywizny powierzchni. Autor podaje przykłady takich przypadków i wykonywa odnoszące się do nich rachunki. *K. Ż.*

2. **Bilger A.** *Przewodnik do udzielania nauki o formach geometrycznych w szkołach.* Lwów, 1898, 8⁰ str. 34, 5, tabl 16.

3. **Danielewicz B.** *Ubezpieczenie kapitału z rentą.* Wiad. mat. II, s. 31—36.

W artykule tym wyprowadza autor wzory na premie jednorazowe i roczne dla następującego rodzaju ubezpieczenia: Osoba x-letnia ubezpiecza kapitał płatny bezwarunkowo po upływie n lat; jeżeli osoba ubezpieczona umrze przed upływem n lat, premie—o ile są wnoszone rocznie—przestają być nadal płacone, a kapitał nietylko zostaje wydany w czasie właściwym, ale nadto jeszcze towarzystwo ubezpieczeń wypłaca corocznie z góry $s^0/_0$ od kapitału ubezpieczonego, począwszy od chwili śmierci osoby ubezpieczonej aż do terminu płatności kapitału. *S. D.*