MARCO CUGIANI (*)

Sull'Aritmetica additiva dei numeri liberi da potenze. (**)

§ I. – Introduzione.

Il problema di decidere sulla possibilità di rappresentare un numero N abbastanza grande nella forma

$$N = x^g + l_t , \tag{1}$$

(dove x è un intero positivo; l_t un intero positivo libero da potenze t-esime (1); g, t sono interi positivi con $t \geqslant g$, $t \geqslant 2$) e di indagare circa il numero di cosiffatte rappresentazioni è stato già largamente trattato, anche nel caso in cui si impongano ad x particolari limitazioni (si richieda ad esempio che x sia primo, oppure libero da quadrati, oppure primo con N) (2). Recentemente ROTH ha trattato la questione per $g = t = 2$ nel caso che x sia libero da quadrati (3).

Ora noi vogliamo affrontare la trattazione del problema, sempre nel caso che x sia libero da quadrati, per un g qualunque, e più precisamente ci riproMettiamo di dimostrare il seguente teorema:

I) *Fissato* $g \geqslant 2$ *e posto* $t = g$, *diciamo* $E(N)$ *il numero delle rappresentazioni dell'intero* N *nella forma* (1), *con* x *libero da quadrati*; *per* N *abbastanza grande il numero* $E(N)$ *soddisfa alla limitazione*

$$E(N) > \gamma_1 N^{1/g} (\log \log N)^{-1} , \tag{2}$$

(dove γ_1 è una costante > 0), *mentre esiste un'altra costante* γ_2 *tale che per infi-*

(*) Indirizzo: Istituto Matematico della Università, Via C. Saldini 50, Milano (Italia).

(**) Ricevuto il 15-VII-1951.

(1) Ricordiamo che un intero si dice « libero da potenze t-esime » quando non è divisibile per la potenza t-esima di alcun intero diverso da 1.

(2) Più ampie notizie sull'argomento si potranno trovare in un'altra nostra Nota (in corso di stampa): « Sulla rappresentazione degli interi come somme di una potenza e di un numero libero da potenze », in corso di stampa su « Ann. Mat. Pura Appl. ».

(3) La Nota di ROTH figura al n. 8 della bibliografia alla fine del presente lavoro.

niti valori di N si ha:

$$E(N) < \gamma_2 N^{1/g} (\log\log N)^{-1} . \tag{3}$$

Questa prima parte del teorema si può riassumere scrivendo

$$0 < \varlimsup \frac{E(N)\log\log N}{N^{1/g}} < \infty .$$

II) *Esiste ancora un'altra costante $\gamma_3 > 0$ tale che per infiniti valori di N si ha*:

$$E(N) > \gamma_3 N^{1/g} , \tag{4}$$

il che si può esprimere scrivendo [poichè evidentemente $E(N) \leqslant N^{1/g}$]

$$0 < \varlimsup \frac{E(N)}{N^{1/g}} \leqslant 1 .$$

§ II.

Alla dimostrazione del nostro teorema premettiamo i seguenti due lemmi.

Lemma I. Detto Q il numero dei termini della progressione aritmetica

$$l , \quad l+k , \quad l+2k , \quad \ldots , \quad l+nk , \ldots$$

(dove si suppone $k > l > 0$) che sono liberi da quadrati e $\leqslant \xi$ si ha (le costanti implicate negli O sono indipendenti da ξ e δ):

1°) $$Q = \frac{6}{\pi^2}\frac{\xi}{k}\prod_{p\mid k}\left(1-\frac{1}{p^2}\right)^{-1} + O(\xi^{1/2}) \qquad \text{se } (l,k) = 1 ,$$

2°) $$Q = \frac{6}{\pi^2}\frac{\xi}{k}\prod_{p\mid k}\left(1-\frac{1}{p^2}\right)^{-1}\cdot\frac{\varphi(\delta)}{\delta} + O(\sqrt{\xi\delta}) \qquad \text{se } (l,k) = \delta \text{ con } \mu(\delta) \neq 0 ,$$

3°) $$Q = 0 \qquad \text{se } (l,k) = \delta \qquad \text{con } \mu(\delta) = 0 .$$

La prima parte è dimostrata da ROTH [4], la terza è ovvia. Dimostriamo dunque la seconda.

---

[4] Vedasi ROTH, Nota citata: la nostra proposizione, nel caso 1°), si deduce immediatamente dalla (9) a pag. 232, ponendo ivi $m = 1$.

Supponiamo dapprima $(l, k) = p$ primo. Allora in ogni gruppo di p termini consecutivi della progressione ve ne sarà uno divisibile per p^2. Se noi sopprimiamo tutti i termini divisibili per p^2 e dividiamo gli altri per p accadrà che i quozienti ottenuti si distribuiranno in $p-1$ classi di numeri rispetto al mod p. Ciascuna di queste classi costituisce una progressione aritmetica di ragione k i cui elementi sono minori o uguali di ξ/p. Ognuna di queste progressioni conterrà un numero Q_1 di termini liberi da quadrati, dove Q_1 per la prima parte del lemma sarà dato da

$$Q_1 = \frac{6}{\pi^2}\frac{\xi}{kp}\prod_{p|k}\left(1-\frac{1}{p^2}\right)^{-1} + O\left(\sqrt{\frac{\xi}{p}}\right),$$

ed avremo perciò

$$Q = \frac{6}{\pi^2}\frac{\xi}{k}\frac{p-1}{p}\prod_{p|k}\left(1-\frac{1}{p^2}\right)^{-1} + O\left(\sqrt{\frac{\xi}{p}\cdot(p-1)}\right).$$

Da questa formula si passa facilmente per induzione alla formula generale, per $\delta = pq \ldots r$,

$$Q = \frac{6}{\pi^2}\frac{\xi}{k}\frac{\varphi(\delta)}{\delta}\prod_{p|k}\left(1-\frac{1}{p^2}\right)^{-1} + O\left(\sqrt{\frac{\xi}{\delta}\cdot\varphi(\delta)}\right),$$

ed essendo $\varphi(\delta) < \delta$ si può scrivere il termine complementare nella forma $O(\sqrt{\xi\delta})$.

Lemma II. Sia $q_1, q_2, \ldots, q_n, \ldots$ una qualunque successione crescente di numeri primi $(q_i < q_{i+1})$ e sia $\nu_1, \nu_2, \ldots, \nu_n, \ldots$ una successione di interi soddisfacenti alle condizioni: $0 \leqslant \nu_i < q_i$, $\nu_i \leqslant g$ (g fisso). Allora l'espressione

$$(5) \qquad \frac{\prod_{q_i \leqslant \gamma}\left(1-\frac{\nu_i}{q_i}\right)}{\prod_{q_i \leqslant \gamma}\left(1-\frac{\nu_i q_i}{q_i^2-1}\right)}\sum_{q_i>\gamma}\frac{\nu_i}{q_i^2}$$

tende a zero per $\gamma \to +\infty$.

L'espressione (5) si può scrivere infatti

$$\prod_{q_i \leqslant \gamma}\left(1+\frac{\nu_i}{q_i^3-\nu_i q_i^2-q_i}\right)\cdot\sum_{q_i>\gamma}\frac{\nu_i}{q_i^2},$$

ed è chiaro che per la convergenza di $\sum\frac{1}{n^2}$ e per il fatto che $\nu_i \leqslant g$ la sommatoria che costituisce il secondo fattore tende a zero per $\gamma \to +\infty$.

In quanto al prodotto si ha [ponendo $A_i = 1 + \nu_i/(q_i^3 - \nu_i q_i^2 - q_i)$]

$$\prod_{q_i \leqslant \gamma} A_i = \prod_{q_i \leqslant g} A_i \cdot \prod_{g < q_i \leqslant \gamma} A_i = \prod_1 \cdot \prod_2 .$$

Ora $\prod_1$ risulta maggiorato ponendo $\nu_i = q_i - 1$ e quindi

$$\prod_1 \leqslant \prod_{q_i \leqslant g} \frac{q_i + 1}{q_i} \leqslant \frac{3}{2} \cdot \frac{4}{3} \cdot \frac{5}{4} \cdots \frac{g+1}{g} = \frac{g+1}{2};$$

mentre $\prod_2$ risulta maggiorato ponendo $\nu_i = g$ ed estendendo il prodotto a tutti i numeri primi $p_i > g$, quindi

$$\prod_2 \leqslant \prod_{p_i > g} \left(1 + \frac{g}{p_i^3 - g p_i^2 - p_i}\right) = G ,$$

dove G è finito e dipende solo da g. Avremo allora

$$\prod_{q_i \leqslant \gamma} A_i \leqslant G \cdot \frac{g+1}{2} = H ,$$

dove H è finito e dipende da g, ma è indipendente da γ e dalla particolare successione $q_1, q_2, \ldots, q_n, \ldots$ prescelta. Il nostro lemma è così dimostrato.

Osserviamo inoltre che dalla dimostrazione risulta anche il seguente fatto:

Fissato g, è possibile in conseguenza determinare un $\bar{\gamma}$ tale che, per $\gamma = \bar{\gamma}$, la (5) risulti minore di una costante prefissata, anzi ciò è possibile anche se alla (5) si sostituisce l'espressione

$$H \cdot \sum_{q_i > \bar{\gamma}} \frac{\nu_i}{q_i^2} , \tag{6}$$

dove $\bar{\gamma}$ dipende solo da g e dalla costante prescelta, ed è indipendente dalla successione dei q_i. Nel seguito ci converrà scegliere $\bar{\gamma}$ in modo che la (6) risulti minore di $6/\pi^2$. Osserviamo che si può sempre scegliere $\bar{\gamma}$ in modo che risulti inoltre $\bar{\gamma} \geqslant g$, relazione che noi supporremo sempre soddisfatta nel seguito.

§ III.

Siano ora $t_1, t_2, \ldots, t_n$ i fattori primi di N e sia:

$$N = t_1^{k_1} t_2^{k_2} \ldots t_n^{k_n}$$

la decomposizione canonica di N in fattori primi. Pensiamo alla successione dei rimanenti numeri primi, che indicheremo con q_i e scegliamo $\bar{\gamma}$ in modo che risultino soddisfatte le condizioni fissate alla fine del § precedente. Sappiamo che $\bar{\gamma}$ risulta indipendente dalla successione dei q_i e quindi da N.

Indichiamo ora con $u_1, u_2, \ldots, u_f$ i q_i minori o uguali di $\bar{\gamma}$ e con $v_1, v_2, \ldots, v_n, \ldots$ i q_i maggiori di $\bar{\gamma}$. Varranno le relazioni

$$u_i < u_{i+1}\,, \qquad v_i < v_{i+1}\,, \qquad u_f \leqslant \bar{\gamma} < v_1\,, \qquad f < \bar{\gamma}\,.$$

Scelto poi η ($0 < \eta < 1$ e del resto qualunque) determiniamo in conseguenza k in modo che risulti

$$v_k \leqslant N^{1/(g+\eta)} < v_{k+1}\,,$$

ponendo $k = 0$ se è già $v_1 > N^{1/(g+\eta)}$.

Indichiamo ora con $\nu(m)$ il numero delle soluzioni (mod m) della congruenza

$$x^g - N \equiv 0 \pmod{m}$$

ed andiamo a dimostrare anzitutto che i valori assunti dall'espressione seguente:

$$K(N) = \left\{ \frac{6}{\pi^2} - H \sum_{m=1}^{k} \frac{\nu(v_m^2)}{v_m^2} \right\} \prod_{j=1}^{f} \left(1 - \frac{u_j \cdot \nu(u_j)}{u_j^2 - 1}\right) \cdot \prod_{i=1}^{n} \left(1 - \frac{1}{t_i}\right) \cdot \log\log N$$

costituiscono, al variare di N ($N > 3$), un insieme che ammette un limite inferiore positivo (non nullo) indipendente da N.

Suddividiamo la dimostrazione in tre parti.

1°) Si ha

$$\nu(v_m) = \nu(v_m^2) \leqslant g < v_m\,, \qquad \text{poichè} \qquad (v_m,\, gN) = 1\,,$$

quindi per il lemma II del § precedente (osservazione finale) si ha

$$\left\{ \frac{6}{\pi^2} - H \sum_{m=1}^{k} \frac{\nu(v_m^2)}{v_m^2} \right\} > H_1 > 0\,.$$

2°) Si ha per $u_1, u_2, \ldots, u_\mu \leqslant g$ [essendo $\nu(u_j) \leqslant u_j - 1$]

$$\prod_{j=1}^{\mu} \left(1 - \frac{u_j \nu(u_j)}{u_j^2 - 1}\right) \geqslant \prod_{j=1}^{\mu} \left(1 - \frac{u_j(u_j - 1)}{u_j^2 - 1}\right) = \prod_{j=1}^{\mu} \left(1 - \frac{u_j}{u_j + 1}\right) \geqslant \left(\frac{1}{g+1}\right)^{\mu}$$

ed inoltre (si ha $\nu(u_3) \leqslant g$)

$$\prod_{j=\mu+1}^{f} \left(1 - \frac{u_j \nu(u_j)}{u_j^2 - 1}\right) \geqslant \prod_{j=\mu+1}^{f} \left(1 - \frac{g u_j}{u_j^2 - 1}\right) \geqslant \prod_{j=\mu+1}^{f} \frac{1}{u_j + 1} > \left(\frac{1}{\bar{\gamma} + 1}\right)^{f-\mu}$$

e perciò

$$\prod_{j=1}^{f}\left(1-\frac{u_j\cdot v(u_j)}{u_j^2-1}\right)>\left(\frac{1}{\bar{\nu}+1}\right)^f>H_2>0\,.$$

3°) Abbiamo infine (p_i è l'i-esimo numero primo):

$$\sum_{i=1}^{n}\log p_i\leqslant\sum_{i=1}^{n}k_i\log t_i=\log N\,,\qquad \sum_{i=1}^{n}\log p_i\sim p_n=p_n+o(p_n)$$

e quindi

$$p_n\leqslant\log N+o(\log N)\,.$$

Ora potremo scrivere, per un noto teorema di MERTENS:

$$\prod_{i=1}^{n}\left(1-\frac{1}{t_i}\right)\geqslant\prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right)=\frac{e^{-C}}{\log p_n}\,(1+o(1))\geqslant\frac{e^{-C}}{\log\log N}\,(1+o(1))$$

e quindi

$$\prod_{i=1}^{n}\left(1-\frac{1}{t_i}\right)\geqslant\frac{H_3}{\log\log N}\,,\qquad (H_3>0)\,.$$

Posto quindi $K_0=H_1H_2H_3$ si ha $K(N)>K_0$ per ogni $N>3$.

Osservazione. Se noi supponiamo di far variare N, anzichè in un modo qualunque, seguendo una legge opportuna (p. es. N fosse sempre scelto uguale ad un numero primo, oppure composto con al più h fattori primi, con h fisso) allora è ovvio che la precedente dimostrazione si potrebbe condurre anzichè sulla espressione $K(N)$ definita come sopra anche su un'altra espressione $K^*(N)$ così definita:

$$K^*(N)=\left\{\frac{6}{\pi^2}-H\sum\frac{\nu(v_m^2)}{v_m^2}\right\}\prod_{j=1}^{f}\left(1-\frac{\nu(u_j)u_j}{u_j^2-1}\right)\cdot\prod_{i=1}^{n}\left(1-\frac{1}{t_i}\right).$$

Osserviamo infine che la dimostrazione condotta sia a proposito della $K(N)$ sia della $K^*(N)$ vale a maggior ragione se nel $\prod(1-1/t_i)$ figura solo una parte dei fattori primi di N anzichè tutti, come avevamo supposto prima.

§ IV.

Passiamo ora a dimostrare il nostro teorema cominciando dalla formula (3) che si può provare immediatamente in base alle seguenti considerazioni.

Supponiamo di far variare N secondo valori definiti al variare di n dalla

relazione:

$$N = \prod_{i=1}^{n} p_i^g ,$$

da cui si deduce

$$\log N = g \sum_{i=1}^{n} \log p_i \sim g p_n$$

e quindi

$$p_n = \frac{\log N}{g} + o(\log N) .$$

Affinchè nella (1) l_t risulti libero da potenze g-esime dovrà ora essere l_t e quindi x primo con N, mentre d'altra parte si ha $x < N^{1/g}$.

Ora si può dimostrare che il numero dei numeri minori di $N^{1/g}$ e composti esclusivamente con fattori primi maggiori di $(\log N)/g + o(\log N)$ ha l'ordine di grandezza (5)

$$\frac{N^{1/g}}{\log \log N}$$

da cui resta provata la validità della (3).

Volendo ora passare a dimostrare la (2), cominceremo col fissare una costante ε e una costante K_1, positive e tali da soddisfare alla limitazione

(7) $$\varepsilon < K_1 < K_0, \qquad (k_0 \text{ ha il significato precisato al § III}),$$

ed andiamo a decomporre il numero N ponendo

$$N = N' N'' N''' \qquad (N', N'' \text{ ed } N''' \text{ primi fra loro a due a due}),$$

dove in N' abbiamo posto i fattori primi di N che compaiono nella sua decomposizione canonica con esponente minore di g, in N'' quelli che vi compaiono alla g-esima potenza, in N''' quelli che vi compaiono con esponente $> g$. Avremo cioè

$$N' = r_1^{\varrho_1} r_2^{\varrho_2} \dots r_h^{\varrho_h} \qquad \text{con } \varrho_i < g,$$
$$N'' = s_1^g s_2^g \dots s_l^g ,$$
$$N''' = z_1^{\tau_1} z_2^{\tau_2} \dots z_\lambda^{\tau_\lambda} \qquad \text{con } \tau_i > g ,$$

(uno o al più due dei numeri h, l, λ possono essere nulli).

---

(5) Vedi, ad es.: G. Ricci, *Ricerche aritmetiche sui polinomi*, Rend. Circ. Mat. Palermo **27**, 433-475 (1933); cfr. § 6.

Una considerazione del tutto analoga a quella svolta da noi a questo punto si trova al § III dell'altro nostro lavoro già citato in (2).

Scegliamo allora σ in modo da aversi

$$s_1 s_2 \dots s_\sigma < N^{1/(g+\varepsilon)}, \qquad s_1 s_2 \dots s_\sigma s_{\sigma+1} \geqslant N^{1/(g+\varepsilon)}.$$

Si osservi che σ così definito esisterà solo se $N'' \geqslant N^{1/(g+\varepsilon)}$, in caso contrario poniamo $\sigma = l$.

Sulla decomposizione di N così effettuata facciamo ora alcune osservazioni che ci saranno utili per il seguito.

Osservazione 1ª. Nella relazione $N = x^g + L$ ogni fattore primo r_i il quale entrasse eventualmente anche in L, e quindi necessariamente anche in x, figurerebbe certo in L con un esponente $\leqslant g-1$.

Osservazione 2ª. Viceversa un fattore primo s_i il quale entrasse eventualmente anche in L vi figurerebbe almeno alla g-esima potenza. Noi dimostreremo adesso che il numero degli L per cui può verificarsi questa circostanza è minore di $K_1 N^{1/g}/\log\log N$ [K_1 è fissato come in (7)] quando si considerino solo quegli s_i per cui $i > \sigma$, e per $N > N_0$.

Infatti detto $\varrho(N)$ il numero di tali L, avremo che a ognuno di essi corrisponderà una soluzione x di una congruenza del tipo

$$x^g - N \equiv 0 \pmod{s_i}, \qquad (i > \sigma,\ x < N^{1/g}). \tag{8}$$

Poichè il numero di soluzioni della (8) non supera $N^{1/g}/s_i$ (si ricordi che $s_i | N$) ed è $\sigma < i \leqslant l$, sarà

$$\varrho(N) \leqslant \frac{N^{1/g}}{s_{\sigma+1}} (l - \sigma).$$

Ora abbiamo

$$\prod_{i=1}^{\sigma+1} s_i \geqslant N^{1/(g+\varepsilon)}, \quad \sum_{i=1}^{\sigma+1} \log s_i \geqslant \log N^{1/(g+\varepsilon)}, \quad \sum_{p \leqslant s_{\sigma+1}} \log p \geqslant \log N^{1/(g+\varepsilon)},$$

$$\sum_{p \leqslant s_{\sigma+1}} \log p \sim s_{\sigma+1}, \quad s_{\sigma+1} \geqslant \log N^{1/(g+\varepsilon)} + o(\log N^{1/(g+\varepsilon)}) > (1-\varepsilon_1) \log N^{1/(g+\varepsilon)}$$

(per $N > N_0$) e d'altra parte:

$$\prod_{i=\sigma+2}^{l} s_i \leqslant \frac{N^{1/g}}{N^{1/(g+\varepsilon)}} = N^{\varepsilon/[g(g+\varepsilon)]}, \qquad \sum_{\sigma+2}^{l} \log s_i \leqslant \log N^{\varepsilon/[g(g+\varepsilon)]},$$

$$\sum_{\sigma+2}^{l} \log s_i > (l-\sigma-1) \log s_{\sigma+1}, \qquad (l-\sigma-1) \log s_{\sigma+1} < \log N^{\varepsilon/[g(g+\varepsilon)]},$$

$$l - \sigma < \frac{\varepsilon \log N}{g(g+\varepsilon) \log\log N} (1 + o(1))$$

e quindi:

$$\varrho(N) \leqslant \frac{N^{1/g}}{(1-\varepsilon_1)\log N}(g+\varepsilon)\frac{\varepsilon \log N}{g(g+\varepsilon)\log\log N}(1+o(1)) \leqslant \varepsilon \frac{N^{1/g}}{\log\log N}(1+o(1)),$$

purchè si scelga, come è sempre possibile, ε_1 tale che $(1-\varepsilon_1)g > 1$.

Ricordando la (7) possiamo affermare che il nostro asserto è così dimostrato.

Osservazione 3ª. Nelle precedenti osservazioni ci siamo occupati dei fattori comuni ad N e ad L. A proposito dei fattori primi di L che non dividono N facciamo adesso le seguenti considerazioni.

Chiamiamo L' quelli fra gli L che soddisfano alle condizioni (gli u_j e i v_m sono definiti come al § III):

$$u_j \nmid L', \quad (1 \leqslant j \leqslant f); \qquad v_m^2 \nmid L', \quad (1 \leqslant m \leqslant k).$$

Ne consegue che se un L' è divisibile per la potenza g-esima di un primo che non divide N, tale primo dovrà essere un v_m (con $m > k$) e si avrà

$$v_m^g \mid N, \quad v_m^{g+1} \nmid N, \quad \text{poichè altrimenti sarebbe } v_m^{g+1} > N^{g+1/(g+\eta)} > N$$

e quindi $L' > N$. Orbene andiamo a dimostrare che il numero, diciamo $R(N)$, degli L' che sono divisibili per qualche v_m^g, è $O(N^{1/g}/\log N)$.

Posto infatti:

$$L' = y V^g,$$

$(y, V) = 1$, V composto con fattori v_m $(m > k)$ si vede anzitutto che deve essere V un numero primo. Se infatti fosse, ad es., $V = v_s v_t$ sarebbe $V > N^{2/(g+\eta)}$ e quindi $L' > N$. Perciò ad ogni L' corrisponderà un x soluzione di una congruenza del tipo:

$$x^g - N \equiv 0 \pmod{v_m^g}, \qquad (m > k)$$

e tale congruenza ha al più g radici $(\bmod v_m^g)$ poichè $v_m > \bar{\gamma}$ è primo con gN e dovendo essere $x < N^{1/g} < v_m^g$ gli L' corrispondenti ad ogni v_m non sono più di g.

Avremo perciò (poichè deve essere $v_m < N^{1/g}$)

$$R(N) \leqslant g \cdot \pi(N^{1/g}) = g \cdot \sum_{p \leqslant N^{1/g}} 1 = g \cdot O\left(\frac{N^{1/g}}{\log N^{1/g}}\right) = O\left(\frac{N^{1/g}}{\log N}\right).$$

§ V.

Per dimostrare completamente la (3) ci serviremo ora della seguente proposizione:

«Il numero delle rappresentazioni di N, che chiameremo $E_1(N)$, nella forma $x^g + L$ dove L ha in comune con N solo fattori r_i oppure fattori s_h (con $h > \sigma$), e dove inoltre L, primo con gli u_j, non è divisibile pel quadrato di alcun v_m (con $m \leqslant k$), soddisfa alla limitazione [K_1 definito come in (7)]

$$E_1(N) \geqslant K_1 \frac{N^{1/g}}{\log\log N}, \qquad \text{(per } N > N_0\text{).»}$$

È evidente che da questa proposizione, ove si ricordino le osservazioni del § precedente segue senz'altro la (3). Passiamo dunque a dimostrare la proposizione annunziata.

Poniamo:

$$d = 1, \quad \text{oppure} \quad d = \prod_a u_a \cdot \prod_b s_b \cdot \prod_c z_c$$

(a può assumere valori scelti in un qualunque gruppo estratto da 1, 2, ..., f; b analogamente da 1, 2,..., σ; c analogamente da 1, 2,..., λ) ed indichiamo con $C'(d, \xi)$ il numero degli intero $x (0 < x < \xi)$ liberi da quadrati che soddisfano alla congruenza:

$$x^g - N \equiv 0 \pmod{d}.$$

Se x_0 è una radice di tale congruenza ($x_0 < d$), sarà:

$$\delta = (x_0, d) = \prod_b s_b \cdot \prod_c z_c < N^{1/g - \varepsilon_1}, \qquad \left(\varepsilon_1 \geqslant \frac{\varepsilon}{g(g+\varepsilon)}\right),$$

e perciò per il lemma I del § II:

$$C'(d, \xi) = \left\{ \frac{6}{\pi^2} \frac{\xi}{d} \prod_b \left(1 - \frac{1}{s_b}\right) \prod_c \left(1 - \frac{1}{z_c}\right) \cdot \prod_{p|d} \left(1 - \frac{1}{p^2}\right)^{-1} + O(\sqrt{\xi\delta}) \right\} \nu(d) =$$

$$= \frac{6}{\pi^2} \xi \prod_b \left(\frac{1}{s_b + 1}\right) \prod_c \left(\frac{1}{z_c + 1}\right) \cdot \prod_a \left(\frac{u_a \cdot \nu(u_a)}{u_a^2 - 1}\right) + O(\sqrt{\xi\delta}) \cdot \prod_a \nu(u_a) \quad (6).$$

---

(6) Si ricordi che $\nu(s_b) = \nu(z_c) = 1$.

Indichiamo con $C(v_m^2 d, \xi)$ il numero degli interi x $(0 < x < \xi)$ che soddisfano alla congruenza

$$x^g - N \equiv 0 \pmod{v_m^3 d},$$

ed avremo (essendo $|\theta| < 1$):

$$C(v_m^2\, d, \xi) = \xi \frac{\nu(v_m^2) \prod_a \nu(u_a)}{v_m^2 \prod_b s_b \cdot \prod_c z_c \cdot \prod_a u_a} + \theta \nu(v_m^2) \prod_a \nu(u_a)\,.$$

Indichiamo infine con $A(\xi)$ il numero degli interi x $(0 < x < \xi)$ per i quali si verificano le condizioni I) e II) sottoindicate [$\mu(x)$ è la funzione di MÖBIUS]:

I)
$$\begin{cases} x^g - N \text{ non congruo a zero } \pmod{s_b}, & b = 1, 2, \ldots, \sigma, \\ x^g - N \quad \text{»} \quad \text{»} \quad \text{»} \pmod{z_c}, & c = 1, 2, \ldots, \lambda, \\ x^g - N \quad \text{»} \quad \text{»} \quad \text{»} \pmod{u_j}, & j = 1, 2, \ldots, f, \\ x^g - N \quad \text{»} \quad \text{»} \quad \text{»} \pmod{v_m^2}, & m = 1, 2, \ldots, k, \end{cases}$$

II) $$\mu(x) \neq 0\,,$$

ed andiamo a dimostrare che

$$A(\xi) \geqslant \sum_d \mu(d) C'(d, \xi) - \sum_d \sum_{m=1}^{k} \mu(d) C(v_m^2 d, \xi)\,. \tag{9}$$

Infatti se uno degli interi y appartenenti all'insieme $0 < y < \xi$ è computato in $A(\xi)$, esso è computato nel secondo membro di (9) una sola volta in $C'(1, \xi)$ e in nessun altro termine delle due sommatorie.

Se un numero y non è computato in $A(\xi)$ tre casi possono darsi: 1°) y soddisfa I) e non II); 2°) y soddisfa II) e non I); 3°) y non soddisfa nè I) nè II).

Nel primo caso y non è computato in nessuno dei $C'(d, \xi)$ perchè non soddisfa II) e in nessuno dei $C(v_m^2 d, \xi)$ perchè soddisfa I).

Nel secondo caso esiste un massimo numero Q, composto con fattori s_b, z_c, u_j, v_m^2 tale che $y^g - N \equiv 0 \pmod{Q}$, e potremo porre $Q = d' \cdot \prod v_m^2$, dove d' è primo con ciascuno dei v_m. Se Q non contiene fattori v_m allora sarà $\prod v_m^2 = 1$ e quindi $d' > 1$ ed y sarà computato una volta in ogni $C'(d, \xi)$ quando $d \mid d'$ e quindi complessivamente un numero di volte dato da

$$\sum_{d\,|\,d'} \mu(d) = 0\,.$$

Se poi $\prod v_m$ non è vuoto ma contiene h diversi fattori v_m, allora y è computato un numero di volte dato da:

$$\sum_{d\,|\,d'} \mu(d) - h \sum_{d\,|\,d'} \mu(d)\,,$$

e questa espressione è nulla per $d' > 1$, negativa o nulla per $d' = 1$.

Nel terzo caso infine si ha che se $\prod v_m^2$ risulta vuoto, allora y non è mai computato al secondo membro della (9), se poi $\prod v_m^2$ contiene h diversi fattori v_m, allora y è computato un numero di volte dato da:

$$-h\sum_{d|d'}\mu(d)=\begin{cases}0 & \text{se } d'>1\,,\\ -h & \text{se } d'=1\,.\end{cases}$$

Dimostrata così la (9), possiamo scrivere [ricordando l'espressione di $C'(d,\xi)$ e che $\delta<N^{(1/g)-\varepsilon_1}$] per $\xi=N^{1/g}$:

$$\sum_d \mu(d)C'(d,\xi)=\frac{6}{\pi^2}\xi\prod_{i=1}^{\sigma}\left(1-\frac{1}{s_i+1}\right)\cdot\prod_{h=1}^{\lambda}\left(1-\frac{1}{z_h+1}\right)\cdot\prod_{j=1}^{f}\left(1-\frac{u_j\cdot v(u_j)}{u_j^2-1}\right)+$$

$$+O(\sqrt{\xi N^{(1/g)-\varepsilon_1}}\,2^{\sigma+\lambda}\prod_{i=1}^{f}(1+v(u_j))>$$

$$>\frac{6}{\pi^2}N^{1/g}\prod_{i=1}^{\sigma}\left(1-\frac{1}{s_i}\right)\cdot\prod_{h=1}^{\lambda}\left(1-\frac{1}{z_h}\right)\cdot\prod_{j=1}^{f}\left(1-\frac{u_j\cdot v(u_j)}{u_j^2-1}\right)+$$

$$+O(\sqrt{N^{(2/g)-\varepsilon_1}})2^{\sigma+\lambda}\prod_{i=1}^{f}(1+v(u_j))\,,$$

e d'altra parte (H ha il significato precisato al lemma II del § II):

$$\sum_d \mu(d)C(v_m^2d,\xi)\leqslant N^{1/g}H\frac{v(v_m^2)}{v_m^2}\prod_{i=1}^{\sigma}\left(1-\frac{1}{s_i}\right)\cdot\prod_{h=1}^{\lambda}\left(1-\frac{1}{z_h}\right)\cdot\prod_{j=1}^{f}\left(1-\frac{u_j\cdot v(u_j)}{u_j^2-1}\right)+$$

$$+v(v_m^2)2^{\sigma+\lambda}\prod_{j=1}^{f}(1+v(u_j))\,.$$

Possiamo allora scrivere (sempre per $\xi=N^{1/g}$):

$$A(\xi)\geqslant N^{1/g}\left(\frac{6}{\pi^2}-H\sum_{m=1}^{h}\frac{v(v_m^2)}{v_m^2}\right)\prod_{i=1}^{\sigma}\left(1-\frac{1}{s_i}\right)\cdot\prod_{h=1}^{\lambda}\left(1-\frac{1}{z_h}\right)\cdot\prod_{j=1}^{f}\left(1-\frac{u_j\cdot v(u_j)}{u_j^2-1}\right)+$$

$$+\left\{O(\sqrt{N^{2/g-\varepsilon_1}})+\sum_{m=1}^{h}v(v_m^2)\right\}2^{\sigma+\lambda}\prod_{j=1}^{f}(1+v(u_j))\geqslant$$

$$\geqslant K_0\frac{N^{1/g}}{\log\log N}+\left\{O(N^{1/g-\varepsilon_2})+\sum_{m=1}^{h}v(v_m^2)\right\}2^{\sigma+\lambda}\prod_{j=1}^{f}(1+v(u_j))\,,$$

dove K_0 ha il significato fissato al § III.

Ora abbiamo:

$$k=\sum_{\varrho\leqslant N^{1/(g+\eta)}}1=\frac{(g+\eta)N^{1/(g+\eta)}}{\log N}(1+o(1))=O\left(\frac{N^{1/(g+\eta)}}{\log N}\right)$$

e quindi, essendo $v_m \nmid gN$:

$$\sum_{m=1} \nu(v_m^2) \leqslant gk = O\left(\frac{N^{1/(g+\eta)}}{\log N}\right).$$

In quanto a $\sigma + \lambda$ abbiamo notato al § III (n. 3°)) che, detto n il numero dei fattori primi di N, si ha:

$$p_n \leqslant \log N + o(\log N)$$

e quindi

$$n \leqslant \sum_{p \leqslant p_n} 1 \leqslant \frac{\log N}{\log\log N}(1 + o(1)),$$

ed essendo $\sigma + \lambda \leqslant n$ avremo

$$2^{\sigma+\lambda} \leqslant N^{\frac{\log 2}{\log\log N}(1+o(1))} = N^{o(1)}.$$

Si ha poi:

$$\prod_{j=1}^{f} (1 + \nu(u_j)) \leqslant (1 + g)^f = O(1),$$

e potremo perciò scrivere, per $\xi = N^{1/g}$,

$$A(\xi) \geqslant K_0 \frac{N^{1/g}}{\log\log N} + \left\{ O\left(N^{1/g-\varepsilon_2} + \frac{N^{1/(g+\eta)}}{\log N}\right)\right\} N^{o(1)} O(1)$$

e quindi certo [K_1 è definito come in (7)]:

$$A(\xi) > K_1 \frac{N^{1/g}}{\log\log N} \qquad \text{per} \quad N > N_0.$$

Osserviamo infine che, nei casi previsti al § III (osservazione finale) la precedente dimostrazione può essere modificata, risultando allora molto più semplice nei suoi sviluppi e conducendo ovviamente ad un risultato del tipo:

$$A(\xi) > K_1 N^{1/g},$$

il che porta senz'altro a concludere anche per la validità della (4), con che il nostro teorema è pienamente dimostrato.

Bibliografia.

1. T. ESTERMANN, *Einige Sätze über quadratfreie Zahlen*, Math. Ann. **105**, 653-662 (1931).

2. T. ESTERMANN, *On the representations of a number as the sum of a prime and a quadratfrei number*, J. London Math. Soc. **6**, 219-221 (1931).

3. P. ERDOS, *The representation of an integer as the sum of the square of a prime and of a square-free integer*, J. London Math. Soc. **10**, 243-245 (1935).

4. L. MIRSKY, *The number of representations of an integer as the sum of a prime and a k-free integer*, Amer. Math. Monthly **56**, 17-19 (1949).

5. A. PAGE, *On the number of primes in an arithmetic progression*, Proc. London Math. Soc. (2) **39**, 116-141 (1935).

6. S. PILLAI, *On the number of representations of a number as the sum of the square of a prime and a squarefree integer*, Proc. Indian Acad. Sci., Sect. A. **10**, 390-391 (1939).

7. G. RICCI, *Sull'aritmetica additiva degli interi liberi da potenze*, Tôhoku Math. J. **41** (Part I), 20-26 (1935).

8. K. F. ROTH, *A theorem involving squarefree numbers*, J. London Math. Soc. **22** 231-237 (1947).

9. K. SAMBASIVA RAO, *On the representation of a number as the sum of the k-th power of a prime and an l-th power-free integer*, Proc. Indian Acad. Sci., Sect. A. **11** 429-436 (1940).

10. A. WALFISZ, *Zur additiven Zahlentheorie*, Math. Z. **40**, 592-697 (1935).