ATTI

DELLA

REALE ACCADEMIA NAZIONALE

DEI LINCEI

ANNO CCCXX

1923

SERIE QUINTA

RENDICONTI

Classe di scienze fisiche, matematiche e naturali.

VOLUME XXXII.

1° SEMESTRE.

ROMA

TIPOGRAFIA DELLA R. ACCADEMIA NAZIONALE DEI LINCEI

PROPRIETÀ DEL DOTT. PIO BEFANI

1923

NOTE PRESENTATE DA SOCI

Matematica. — *Algoritmo del massimo comun divisore nel corpo delle radici quinte dell'unità.* Nota della signorina GEMMA BRANCHINI [1], presentata dal Socio L. BIANCHI.

Vogliamo stabilire che per gli interi di questo corpo sussiste un algoritmo analogo a quello delle successive divisioni.

Siano μ, ν due interi qualunque del corpo e sia per es. $N(\mu) \geq N(\nu)$. Formiamo il loro quoziente $\frac{\mu}{\nu}$ che potrà, in innumerevoli modi, essere posto sotto la forma:

$$\frac{\mu}{\nu} = A + \alpha , \tag{1}$$

dove A indica un intero ed α un numero che in generale sarà fratto. Si avrà allora:

$$\mu = A\nu + \alpha\nu ,$$

e ponendo

$$\alpha\nu = R$$
$$\mu = A\nu + R ,$$

con R intero. Si tratta di dimostrare che è sempre possibile fare la decomposizione (1) in modo che risulti $N(\alpha) < 1$, cioè $N(R) < N(\nu)$, purchè ove occorra si sostituisca a μ un intero associato. Possiamo subito osservare che se

$$\frac{\mu}{\nu} = \bar{a}\varepsilon + \bar{b}\varepsilon^{-1} + \bar{c}\varepsilon^{2} + \bar{d}\varepsilon^{-2} ,$$

si potranno estrarre dai numeri razionali $\bar{a}, \bar{b}, \bar{c}, \bar{d}$ le parti intere in modo che le residue parti fratte a, b, c, d siano positive o negative, ma in valore assoluto $\leq \frac{1}{2}$, in modo che risulti $\frac{\mu}{\nu} = A + \alpha$, dove A è un intero ed è $\alpha = a\varepsilon + b\varepsilon^{-1} + c\varepsilon^{2} + d\varepsilon^{-2}$ con $|a|, |b|, |c|, |d| \leq \frac{1}{2}$.

[1] Dell'algoritmo Euclideo per gli interi formati con la radice quinta dell'unità si trova traccia nel *Nachlass* di Gauss (Werke Bd. II. Zur Theorie der complexen Zahlen, S. 391-395). Ved. le annesse *Bemerkungen* di Schering. Il semplice procedimento qui esposto è stato presentato dalla signorina Branchini nella sua tesi di laurea. (L. B).

In ciò che segue supponiamo che α sia preso in modo da soddisfare a questa condizione. Evidentemente:

$$\alpha\varepsilon = a\varepsilon^2 + b + c\varepsilon^{-2} + d\varepsilon^{-1} = -b\varepsilon + (d-b)\varepsilon^{-1} + (a-b)\varepsilon^2 + (c-b)\varepsilon^{-2}$$
$$\alpha\varepsilon^2 = a\varepsilon^{-2} + b\varepsilon + c\varepsilon^{-1} + d = (b-d)\varepsilon + (c-d)\varepsilon^{-1} - d\varepsilon^2 + (a-d)\varepsilon^{-2}$$
$$\alpha\varepsilon^{-1} = a + b\varepsilon^{-2} + c\varepsilon + d\varepsilon^2 = (c-a)\varepsilon - a\varepsilon^{-1} + (d-a)\varepsilon^2 + (b-a)\varepsilon^{-2}$$
$$\alpha\varepsilon^{-2} = a\varepsilon^{-1} + b\varepsilon^2 + c + d\varepsilon = (d-c)\varepsilon + (a-c)\varepsilon^{-1} + (b-c)\varepsilon^2 - c\varepsilon^{-2}.$$

Facciamo le seguenti osservazioni:

1°) Si possono aumentare o diminuire (separatamente) le coordinate a, b, c, d di α di 1, pur di mutare convenientemente A con l'aggiunta di $\pm\varepsilon^u (u = 1, 2, 3, 4)$.

2°) Si può ad α sostituire αE, essendo E un'unità, pur di cambiare A in AE e μ in μE.

Calcoliamo:

$$N(\alpha) = \alpha \,.\, s^2\alpha \,.\, s\alpha \,.\, s^3\alpha = P \,.\, \overline{P}$$

dove

$$P = \alpha \,.\, s^2 \,.\, \alpha \quad , \quad \overline{P} = s\alpha \,.\, s^3\alpha \ (^1).$$

Si trova subito:

$$P = (a^2 + b^2 + c^2 + d^2 - ab - ad - bc) + (ac + bd + cd - ab - ad - bc)\,\eta$$
$$\overline{P} = (a^2 + b^2 + c^2 + d^2 - ab - ad - bc) + (ac + bd + cd - ab - ad - bc)\,\overline{\eta},$$

e ne ricaviamo:

$$P + \overline{P} = 2(a^2 + b^2 + c^2 + d^2 - ab - ad - bc) + (ac + bd + cd - ab - ad - bc)(\eta + \overline{\eta}) =$$
$$[\text{dove} \quad \eta = \varepsilon + \varepsilon^{-1} \ , \ \overline{\eta} = \varepsilon^2 + \varepsilon^{-2}]$$
$$= 2(a^2 + b^2 + c^2 + d^2 - ab - ad - bc) - ac - bd - cd + ab + ad + bc =$$
$$= 2(a^2 + b^2 + c^2 + d^2) - ab - ad - bc - ac - bd - cd;$$

quindi:

$$2(P + \overline{P}) = 4(a^2 + b^2 + c^2 + d^2) - 2ab - 2ad - 2bc - 2ac - 2bd - 2cd =$$
$$= 5(a^2 + b^2 + c^2 + d^2) - (a + b + c + d)^2 \quad (^2).$$

P, $\overline{P}$ sono positivi, essendo rispettivamente quadrati dei moduli di α e di $s\alpha$.

Facciamo vedere che pur di sostituire, ove occorra, a μ uno dei suoi particolari associati si può sempre ricadere in uno dei seguenti casi:

1°) *Due delle coordinate di* α *in modulo* $\leq \frac{1}{4}$.

(1) $s\alpha$ indica quel coniugato di α che si ottiene cangiando ε in ε^2.

(2) Ved. Gauss, Werke-Zweiter Band. s. 394.

2°) *Una delle coordinate di* α *in modulo* $\leq \frac{1}{4}$, *la somma dei moduli di due delle rimanenti* $\leq \frac{3}{4}$ (mentre ciascuno di essi si suppone $> \frac{1}{4}$, altrimenti saremmo nel 1° caso).

Osserviamo, anzitutto, che una delle coordinate di α si può sempre prendere in modulo $\leq \frac{1}{4}$. Infatti, se tutti i moduli delle coordinate superassero $\frac{1}{4}$, scelte due delle coordinate di segno uguale (che certo ci sono) ad es. b, d basterà ad α sostituire $\alpha\varepsilon$ (2ª oss.); il parametro $d - b$ risulterà $\leq \frac{1}{4}$ in modulo e gli altri $-b, a-b, c-b$ potranno rendersi (ove già non lo siano) in modulo $\leq \frac{1}{2}$ con l'aggiunta di ± 1 (1ª oss.). Se un'altra delle coordinate è in modulo $\leq \frac{1}{4}$ si cade nel 1° caso.

In caso contrario tre delle coordinate saranno in modulo $> \frac{1}{4}$; se tutte tre sono dello stesso segno, ad es. a, b, c, sostituendo ad $\alpha, \alpha\varepsilon^{-1}$ abbiamo due coordinate $c - a$, $b - a$ in modulo $< \frac{1}{4}$ e le altre due $a, d - a$ si potranno far cadere nell'intervallo $\left(-\frac{1}{2}, \frac{1}{2}\right)$ con togliere o aggiungere, ove occorra, un'unità ricadendo nel 1° caso.

Resta da esaminare il caso di tre coordinate a, b, c in modulo $> \frac{1}{4}$ con due a, b di uno stesso segno ed una c di segno contrario, di più $|d| \leq \frac{1}{4}$. Ora, se $|a| + |c| \leq \frac{3}{4}$ cadiamo nel 2° caso; se invece $|a| + |c| > \frac{3}{4}$ sostituendo ad $\alpha, \alpha\varepsilon^{-1}$ troviamo una coordinata $b - a$ in modulo $< \frac{1}{4}$ e la coordinata $c - a$ in modulo $> \frac{3}{4}$; questa con l'aggiunta di ± 1 diviene in modulo $\leq \frac{1}{4}$ e si cade nel 1° caso.

Dimostriamo ora che nei due casi sopra detti $N(\alpha) < 1$ ed è quindi sempre possibile decomporre il quoto $\frac{\mu}{\nu}$ nel modo richiesto. Difatti nel 1° caso, essendo

$$2(P + \bar{P}) \leq 5(a^2 + b^2 + c^2 + d^2),$$

sarà:

$$2(P+\overline{P}) \leq 5\left(\frac{1}{4}+\frac{1}{4}+\frac{1}{16}+\frac{1}{16}\right)=5\left(\frac{1}{2}+\frac{1}{8}\right)=\frac{25}{8}$$

e

$$P+\overline{P} \leq \frac{25}{16}.$$

È noto che « *se due quantità positive hanno somma costante il loro prodotto diventa massimo quando queste due quantità sono uguali* ».

Quindi per un dato valore di $s = P+\overline{P}$ il prodotto $P.\overline{P}$ diviene massimo per $P=\overline{P}=\frac{s}{2}$ ed il valore massimo del prodotto è $\left(\frac{s}{2}\right)^2$. Poichè il valore massimo di s è $\frac{25}{16}$, il valore massimo di $N(\alpha) = P.P$ sarà:

$$\left(\frac{25}{32}\right)^2 < 1.$$

Nel 2° caso invece, per un dato valore della somma s di due dei moduli delle coordinate $\left(\text{somma che, come sappiamo, si suppone } \leq \frac{3}{4}\right)$, il valore massimo della somma dei loro quadrati si ha quando i due moduli si scostano l'uno dall'altro più che è possibile, ciò che accade quando uno dei due è uguale a $\frac{1}{4}$ e l'altro a $s-\frac{1}{4}$ ed allora la somma dei quadrati dei moduli diviene $\left(\frac{1}{4}\right)^2+\left(s-\frac{1}{4}\right)^2$ e variando s raggiungerà il suo massimo valore per $s=\frac{3}{4}$. Questo valore massimo ha luogo quando uno dei due detti moduli prende il valore $\frac{1}{2}$ e l'altro il valore $\frac{1}{4}$, ed allora si ha:

$$2(P+\overline{P}) \leq 5\left(\frac{1}{4}+\frac{1}{16}+\frac{1}{4}+\frac{1}{16}\right)=\frac{25}{8}$$

quindi:

$$P+\overline{P} \leq \frac{25}{16}$$

e, come nel 1° caso,

$$N(\alpha)=P.\overline{P} \leq \left(\frac{25}{32}\right)^2 < 1.$$

Abbiamo, per ora, dimostrato che:

« *Dati due interi* μ, ν *del corpo con* $N(\mu) \geq N(\nu)$, *si può trovare un altro intero* A *tale che sia* $N(\mu-\nu A) < N(\nu)$ *od anche* $N(R) < N(\nu)$ » (ponendo $\mu-\nu A = R$) [1].

[1] Ved. Bianchi, *Teoria dei numeri*, pag. 10-11.

Se nella $\mu = \nu A + R$ non è $R = 0$ si può proseguire nello stesso modo la divisione di ν per R e si troverà:

$$\nu = RA_1 + R_1 \qquad \text{con} \qquad N(R_1) < N(\nu)$$

e così di seguito. L'operazione termina certamente con un resto R_n che divide il precedente R_{n-1} e questo perchè i numeri interi positivi

$$N(\nu)\ ,\ N(R)\ ,\ N(R_1) \ldots$$

formano una serie decrescente, che perciò si arresta.

Scriviamo la catena limitata d'uguaglianze:

$$\left\{\begin{array}{ll} \mu = \nu A + R & N(R) < N(\nu) \\ \nu = RA_1 + R_1 & N(R_1) < N(R) \\ R = R_1 A_2 + R_2 & N(R_2) < N(R_1) \\ \ldots\ldots\ldots & \ldots\ldots\ldots \\ R_{n-2} = R_{n-1} A_n + R_n & N(R_n) < N(R_{n-1}) . \end{array}\right.$$

Vediamo così che ogni divisore comune di μ, ν divide per la 1ª anche R, quindi per la 2ª R_1 ecc. e infine R_n. È pure chiaro che R_n dividendo R_{n-1} divide R_{n-2}, divide $R_{n-3} \ldots$ e infine μ, ν.

Si conclude che R_n è il divisore comune di massima norma di μ, ν e dicesi perciò il loro *massimo comun divisore*.

Resta così dimostrato che:

« *Nel corpo delle radici quinte dell'unità vale sempre l'algoritmo delle successive divisioni* ».

Matematica. — *Genesi cinematica intrinseca del parallelismo di Levi-Civita per le superficie a curvatura costante.* Nota di GIUSEPPE CORBELLINI, presentata dal Socio CASTELNUOVO.

1. Prendiamo le mosse dalla definizione costruttiva del parallelismo superficiale di Levi-Civita [1] nella forma riproducente nel campo infinitesimale il comportamento delle parallele euclidee.

Sopra una superficie, dati due punti P e P′ infinitamente vicini ed una direzione uscente da P e appartenente alla superficie, si dirà parallela ad essa in P′ quella direzione uscente da P′ che forma in P′ con la geodetica PP′ lo stesso angolo che la direzione data forma in P con la geodetica stessa.

Supposta ora tracciata sopra una superficie una curva t passante per P e per P′, sulla quale sia assegnato come verso positivo quello che va da P

[1] T. Levi-Civita, *Nozione di parallelismo* ecc. Rend. Circ. Palermo, tomo 42°, 1917, pp. 173 e seg.; F. Severi, *Sulla curvatura* ecc. ibid, pp. 227 e seg.