ATTI

DELLA

REALE ACCADEMIA NAZIONALE DEI LINCEI

ANNO CCCXVII.

1920

SERIE QUINTA

RENDICONTI

Classe di scienze fisiche, matematiche e naturali.

VOLUME XXIX.

2° Semestre.

ROMA

TIPOGRAFIA DELLA R. ACCADEMIA NAZIONALE DEI LINCEI

PROPRIETÀ DEL DOTT. PIO BEFANI

1920

RENDICONTI

DELLE SEDUTE

DELLA REALE ACCADEMIA NAZIONALE DEI LINCEI

Classe di scienze fisiche, matematiche e naturali.

MEMORIE E NOTE
DI SOCI O PRESENTATE DA SOCI

pervenute all'Accademia durante le ferie del 1920.

(Ogni Memoria o Nota porta a pie' di pagina la data d'arrivo).

Matematica. — *Osservazioni circa il carattere quadratico dei numeri in un corpo quadratico.* Nota del Socio L. BIANCHI (1).

1. Se in un corpo algebrico $K(\theta)$ consideriamo un qualunque *ideale primo* P, e con ω indichiamo un intero del corpo, non divisibile per P, il simbolo $\left[\frac{\omega}{P}\right]$ denoterà l'unità positiva o negativa, secondo che la congruenza

$$x^2 \equiv \omega \pmod{P} \tag{1}$$

è solubile, ovvero insolubile, con un intero x del corpo $K(\theta)$. All'ideale primo P è coordinato un ordinario numero primo p (il più piccolo numero razionale intero contenuto in P).

Quando $p = 2$, allora è sempre $\left[\frac{\omega}{P}\right] = +1$, ossia ω è residuo quadratico (mod P), e la congruenza (1) ha una sola radice. Se p è dispari, come ora supponiamo, può essere $\left[\frac{\omega}{P}\right] = +1$, ovvero $\left[\frac{\omega}{P}\right] = -1$, e nel primo caso la (1) ha due radici. In ogni caso vale pel simbolo $\left[\frac{\omega}{P}\right]$,

(1) Pervenuta all'Accademia il 21 settembre 1920.

che diciamo di Dirichlet, il criterio generalizzato di Eulero

$$\left[\frac{\omega}{\mathrm{P}}\right] = \pm 1, \text{ secondo che } \omega^{\frac{1}{2}\Phi(\mathrm{P})} \equiv \pm 1 \pmod{\mathrm{P}},$$

dove con $\Phi(\mathrm{P})$ si è indicato la funzione aritmetica generalizzata di Gauss

$$\Phi(\mathrm{P}) = \mathrm{NP} - 1$$

e con NP s'intende la norma dell'ideale P

$$\mathrm{NP} = p^f,$$

l'esponente f essendo il grado dell'ideale P.

Nelle sue celebri ricerche sulle forme binarie quadratiche nel *campo di Gauss* $[1, i]$, Dirichlet ha ridotto, per questo corpo quadratico, il calcolo del simbolo $\left[\frac{\omega}{\mathrm{P}}\right]$ a quello di un ordinario simbolo di Legendre $\left(\frac{a}{p}\right)$. Non constandomi che sia stata osservata la riduzione del tutto analoga pel caso di un corpo quadratico qualunque, dimostro in questa breve Nota le due formole relative.

2. Indicando con m un numero razionale intero, positivo o negativo, ma privo di fattori quadrati, il corpo quadratico $\mathrm{K}(\sqrt{m})$ ha il numero *fondamentale* D dato da

$$\mathrm{D} = 4m \text{ , se } m \not\equiv 1 \pmod 4$$
$$\mathrm{D} = m \text{ , per } m \equiv 1 \pmod 4.$$

Una *base* per gli interi del corpo è data da

$$[1, \theta],$$

avendo posto

$$\theta = \sqrt{m} \text{ , per } m \not\equiv 1 \pmod 4$$
$$\theta = \frac{-1+\sqrt{m}}{2} \text{ , per } m \equiv 1 \pmod 4.$$

Gli ideali primi P del corpo $\mathrm{K}(\sqrt{m})$, a numero primo coordinato p dispari, sono da distinguersi in tre specie, a seconda che si presenta uno dei tre casi possibili seguenti

$$a) \left(\frac{m}{p}\right) = -1 , \qquad b) \left(\frac{m}{p}\right) = +1 ,$$

$$c) \ m \text{ divisibile per } p \text{ o } \left(\frac{m}{p}\right) = 0.$$

L'accennata formola di riduzione assume due diversi aspetti, secondo che

ci troviamo nel caso *a*), ovvero in uno degli altri due *b*) o *c*). Pel caso *a*) dimostreremo che si ha la formola di riduzione

$$\text{(A)} \qquad \left[\frac{\omega}{\mathrm{P}}\right] = \left(\frac{\mathrm{N}\omega}{p}\right),$$

dove $\mathrm{N}\omega$ denota la norma del numero ω.

In questo primo caso *a*) l'ideale principale (p) coincide coll'ideale primo P (di 2° grado) ed è $\mathrm{NP} = p^2$. La congruenza (1) equivale perfettamente all'altra

$$x^2 \equiv \omega \pmod{p},$$

dalla quale prendendo le norme dei due numeri congrui x^2, ω, risulta

$$(\mathrm{N}x)^2 \equiv \mathrm{N}\omega \pmod{p};$$

la risolubilità della (1) porta quindi la risolubilità dell'altra nel *campo razionale*

$$\text{(2)} \qquad \xi^2 \equiv \mathrm{N}\omega \pmod{p}.$$

Vediamo dunque che, se nella (A) il valore del simbolo a sinistra è $+1$, tale è anche quello del simbolo a destra. Basterà quindi provare che inversamente se $\left(\frac{\mathrm{N}\omega}{p}\right) = +1$ è anche $\left[\frac{\omega}{\mathrm{P}}\right] = +1$, cioè che, supposta solubile la (2) (nel campo razionale), è pure solubile la (1) nel campo $\mathrm{K}(\sqrt{m})$.

Cominciamo per ciò dal supporre $m \not\equiv 1 \pmod 4$, indi $\theta = \sqrt{m}$, e posto

$$\omega = a + b\sqrt{m},$$

con a, b interi razionali, avremo

$$\mathrm{N}\omega = a^2 - mb^2.$$

Per ipotesi esiste un intero razionale s che soddisfa alla congruenza (2)

$$s^2 \equiv a^2 - mb^2 \pmod{p};$$

dobbiamo provare l'esistenza di due numeri razionali interi t, u, tali che sussista la congruenza

$$(t + u\sqrt{m})^2 \equiv a + b\sqrt{m} \pmod{p}.$$

Questa si scinde, nel campo razionale, nelle due

$$\text{(4)} \qquad \begin{cases} t^2 + mu^2 \equiv a \\ 2tu \equiv b \end{cases} \pmod{p}$$

e se dapprima consideriamo il caso $b \equiv 0 \pmod{p}$, sarà certamente $\left(\frac{N\omega}{p}\right) = \left(\frac{a^2}{p}\right) = +1$ e dovremo provare che anche $\left[\frac{\omega}{P}\right] = +1$, ossia che le (4) ammettono soluzioni. E infatti, siccome $a \not\equiv 0 \pmod{p}$, perchè ω non è divisibile per P, avremo

$$\left(\frac{a}{p}\right) = +1 \quad , \quad \text{ovvero} \quad \left(\frac{a}{p}\right) = -1.$$

Nel primo caso basta prendere $u = 0$ e per t una radice della congruenza $t^2 \equiv a \pmod{p}$; nel secondo caso si assuma $t = 0$ e si prenda u come radice della congruenza

$$mu^2 \equiv a \pmod{p},$$

la quale è solubile, perchè m è non residuo come $a \pmod{p}$.

Sia ora $b \not\equiv 0 \pmod{p}$, e si osservi che da

$$(Nx)^2 = (t^2 - mu^2)^2 \equiv s^2 \pmod{p}$$

segue

$$t^2 - mu^2 \equiv \pm s \pmod{p},$$

che, combinata per addizione e sottrazione colla prima delle (4), dà

$$(5) \qquad \begin{matrix} 2t^2 \equiv a \pm s \\ 2mu^2 \equiv a \mp s \end{matrix} \pmod{p}.$$

Ma per la prima delle (3)

$$2(a - s) \cdot 2(a + s) \equiv 4mb^2 \pmod{p},$$

onde, essendo $b \not\equiv 0 \pmod{p}$, $\left(\frac{m}{p}\right) = -1$, segue

$$\left(\frac{2(a-s)}{p}\right) \cdot \left(\frac{2(a+s)}{p}\right) = -1.$$

Poniamo p. e. che sia

$$\left(\frac{2(a+s)}{p}\right) = +1 \quad , \quad \left(\frac{2(a-s)}{p}\right) = -1,$$

e scegliendo nelle (5) i segni superiori, queste risulteranno solubili. Inoltre, dalla loro moltiplicazione, risulta

$$4mt^2u^2 \equiv a^2 - s^2 \equiv mb^2 \pmod{p},$$

ossia

$$4t^2u^2 \equiv b^2$$

$$2tu \equiv \pm b \pmod{p},$$

e disponendo dei segni di t, u possiamo così soddisfare anche la seconda delle (4). Nel caso $m \not\equiv 1 \pmod 4$ la formola (A) è così dimostrata.

3. Per provare che sussiste la medesima formola (A) anche nel caso $m \equiv 1 \pmod 4$, ove è da prendersi

$$\theta = \frac{-1+\sqrt{m}}{2},$$

osserviamo che l'equazione quadratica per θ si scrive ora

$$\theta^2 + \theta - \frac{m-1}{4} = 0, \tag{6}$$

e se $a + b\theta$ è un intero qualunque del corpo (a, b interi razionali), per la sua norma si ha

$$N(a+b\theta) = a^2 - \frac{m-1}{4} b^2 - ab.$$

Dobbiamo ora provare che, se è solubile in s la congruenza

$$s^2 \equiv a^2 - \frac{m-1}{4} b^2 - ab, \tag{7}$$

è solubile anche l'altra in t, u

$$(t+u\theta)^2 \equiv a + b\theta \pmod p.$$

Questa, sviluppata con riguardo alla (6), si sdoppia, nel campo razionale, nelle due

$$\begin{cases} t^2 + \dfrac{m-1}{4} u^2 \equiv a \\ 2tu - u^2 \equiv b \end{cases} \pmod p. \tag{8}$$

Come al numero precedente, consideriamo dapprima il caso $b \equiv 0 \pmod p$, indi $a \not\equiv 0 \pmod p$.

Se $\left(\frac{a}{p}\right) = +1$ prendiamo $u = 0$ e t come radice di $t^2 \equiv a \pmod p$; se invece $\left(\frac{a}{p}\right) = -1$, facciamo $u = 2t$ e, per soddisfare anche alla prima delle (8), prendiamo t dalla congruenza

$$mt^2 \equiv a \pmod p,$$

che è solubile perchè a ed m sono insieme non residui (mod p).

Considerando ora il caso generale $a \not\equiv 0 \pmod p$, alle (8) associamo l'altra

$$N(t+u\theta) \equiv \pm s,$$

ossia

$$(8^*) \qquad t^2 - \frac{m-1}{4} u^2 - tu \equiv \pm s \pmod{p}.$$

Le (8), (8*), risolute rapporto a t^2, u^2, tu. dànno il sistema equivalente:

$$(9) \qquad \begin{cases} mt^2 \equiv \dfrac{m+1}{2} a + \dfrac{m-1}{4} (b + 2s) \\ mu^2 \equiv 2a - (b \pm 2s) \qquad\qquad (\text{mod } p) \\ mtu \equiv a + \dfrac{m-1}{2} b \mp s. \end{cases}$$

Ma dalla (7), scritta sotto la forma

$$(2a - b)^2 - 4s^2 = (2a - b - 2s)(2a - b + 2s) \equiv mb^2 \pmod{p},$$

avendosi $b \not\equiv 0 \pmod{p}$, $\left(\dfrac{m}{p}\right) = -1$, vediamo che il prodotto

$$(2a - b - 2s)(2a - b + 2s)$$

è un non residuo (mod p), cioè

$$\left(\frac{2a - b - 2s}{p}\right) = \pm 1 \quad , \quad \left(\frac{2a - b + 2s}{p}\right) = \mp 1.$$

E allora nelle (9) prendiamo quella determinazione di segni che rende, nella media delle (9), il secondo membro non residuo (mod p); così questa sarà risolubile e si potrà scegliere fra due valori opposti per u. Dopo ciò, la terza delle (9), essendo $u \not\equiv 0 \pmod{p}$, individuerà un valore di t, che soddisferà insieme la prima delle (9). Quest'ultima cosa risulta evidente servendosi dell'identità

$$\left\{a + \frac{m-1}{2} b \mp s\right\}^2 \equiv \left\{\frac{m+1}{2} a + \frac{m-1}{4} (b \pm 2s)\right\} \cdot \left\{2a - (b \pm 2s)\right\},$$

la quale, a meno del fattore m, non è altro che la (7).

Concludiamo adunque: *Per quegli ideali primi* **P** *del corpo quadratico, che sono al tempo stesso ideali principali, vale la formola di riduzione* (A) *del simbolo di Dirichlet al simbolo di Legendre.*

4. Veniamo al secondo caso b), ove $\left(\dfrac{m}{p}\right) = +1$. Qui l'ideale principale (p) si decompone nel prodotto PP′ di due ideali primi coniugati e *diversi*, che possiamo definire mediante le loro basi come segue.

Si consideri dapprima il caso $m \not\equiv 1 \pmod 4$, e indichi α una radice della congruenza

$$\alpha^2 \equiv m \pmod p; \tag{10}$$

potremo prendere

$$\mathrm{P} = [p, \alpha + \sqrt{m}], \tag{11}$$

indi pel coniugato

$$\mathrm{P}' = [p, -\alpha + \sqrt{m}]. \tag{11'}$$

Se si suppone solubile la congruenza

$$x^2 \equiv a + b\sqrt{m} \pmod{\mathrm{P}}, \tag{12}$$

cioè

$$\left[\frac{a + b\sqrt{m}}{\mathrm{P}}\right] = +1,$$

siccome $\mathrm{NP} = p$, e i numeri razionali

$$0, 1, 2, , \ldots p - 1$$

formano già un sistema completo di numeri incongrui (mod p), il valore della incognita x nella (12) può assumersi razionale intero. Ma ogni numero dell'ideale P, colla base (11), ha la forma

$$rp + s(\alpha + \sqrt{m}) \qquad (r, s \text{ razionali interi})$$

e la (12), ovvero

$$x^2 = a + b\sqrt{m} + rp + s(\alpha + \sqrt{m}),$$

si sdoppia nelle due nel campo razionale

$$\begin{cases} x^2 = a + s\alpha + rp \\ s = -b \end{cases}$$

che equivalgono alla congruenza

$$x^2 \equiv a - \alpha b \pmod p.$$

Così, se $\left[\frac{a + b\sqrt{m}}{\mathrm{P}}\right] = +1$ è anche $\left(\frac{a - \alpha b}{p}\right) = +1$, ma anche viceversa da questa seconda eguaglianza segue la prima. Nel caso attuale $m \not\equiv 1 \pmod 4$ la formola di riduzione domandata si scrive dunque

$$\left[\frac{a + b\theta}{\mathrm{P}}\right] = \left(\frac{a - \alpha b}{p}\right). \tag{B}$$

È facile vedere che questa medesima formola sussiste anche nel caso $m \equiv 1 \pmod 4$, purchè s'intenda allora per α una radice della congruenza

$$\alpha^2 - \alpha - \frac{m-1}{4} \equiv 0 \pmod p,$$

ossia

$$(10^*) \qquad (2\alpha - 1)^2 \equiv m \pmod p,$$

chè allora per base dell'ideale P possiamo prendere

$$P = [p\ ,\ \alpha + \theta],$$

e pel coniugato P'

$$P' \equiv [p\ ,\ \alpha' + \theta], \qquad \alpha' = 1 - \alpha,$$

e basta procedere come sopra.

Resta solo da considerare il terzo caso *c*) in cui $m \equiv 0 \pmod p$, e l'ideale principale (p) è il quadrato di un ideale primo P, coincidente col coniugato P', e colla base

$$[p\ ,\ \sqrt{m}], \qquad \text{se} \quad m \not\equiv 1 \pmod 4$$

$$\left[p\ ,\ \frac{p+1}{2} + \theta\right], \quad \text{se} \quad m \equiv 1 \pmod 4.$$

Ma si osserva subito che la medesima formola (B) è applicabile anche in questo caso, ove si ponga $\alpha = 0$ quando $m \not\equiv 1 \pmod 4$, ed $\alpha = \frac{p+1}{2}$ (o $\alpha \equiv \frac{1}{2}$) quando $m \equiv 1 \pmod 4$.

Non lascieremo di osservare che dalla formola (B) risulta un facile confronto fra i due caratteri quadratici che uno stesso numero ω del corpo offre rispetto a due ideali primi coniugati (diversi) P, P', colla formola

$$\left[\frac{\omega}{P}\right]\left[\frac{\omega}{P'}\right] = \left(\frac{N\omega}{p}\right),$$

in parole: *Ogni numero ω del corpo quadratico ha, rispetto a due ideali primi coniugati diversi del corpo, caratteri quadratici concordanti o discordanti secondo che la sua norma è residuo o non residuo del numero primo p coordinato ai due ideali.*