Bollettino
Unione Matematica Italiana

Carlo Cellitti

Sopra una proprietà delle forme quadratiche binarie primitive di determinante $D \equiv 1 \pmod 4$.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **10** (1955), n.4, p. 527–530.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1955_3_10_4_527_0>

Bollettino dell'Unione Matematica Italiana, Zanichelli, 1955.

Sopra una proprietà delle forme quadratiche binarie primitive di determinante $D \equiv 1 \pmod 4$.

Nota di CARLO CELLITTI (a Ferentino)

Sunto. - *Mediante le sostituzioni lineari unimodulari a coefficienti interi, l'A. costruisce un sistema di rappresentanti di classi di forme quadratiche, binarie primitive di prima specie, e ne dimostra una interessante proprietà.*

1. Le relazioni tra i numeri delle classi di forme quadratiche binarie propriamente primitive e di forme quadratiche binarie impropriamente primitive di dato determinante, contenute nell'opera del GAUSS (1), e le ricerche che il DIRICHLET fa sullo stesso argomento (2) sono state il filo conduttore della dimostrazione del teorema che è oggetto della presente nota; ci siamo serviti delle sostituzioni lineari unimodulari a coefficienti interi.

A titolo di premessa, richiamiamo, intanto, brevemente, alcune classiche nozioni.

È ben noto che le sostituzioni lineari $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, a coefficienti interi, unimodulari ($\alpha\delta - \beta\gamma = 1$), costituiscono un gruppo Γ, e la loro legge di composizione

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + \beta\gamma' & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma' & \gamma\beta' + \delta\delta' \end{pmatrix}$$

unita al fatto che $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$, ci mostra la proposizione evidente secondo cui *le sostituzioni* S, *per le quali è* $\beta \equiv 0 \pmod p$, *costituiscono un gruppo* G_p. In particolare, per $p = 2$, *le sostituzioni* S *aventi* β *pari costituiscono un gruppo* G_2.

Si consideri la forma binaria quadratica

$$f \equiv (a,\ b,\ c) = ax^2 + 2bxy + cy^2$$

(1) C. F. GAUSS, *Disquisitiones arithmeticae*, Lipsiae 1801, art. 253-256; *Werke*, I, pp. 276-284, (Gottingen, 1870).

(2) G. LEJEUNE DIRICHLET, *Recherches sur diverses applications de l'Analyse infinitèsimale à la thèorie des nombres*, Journ. für d. r. u. a. Mathem. (von Crelle), Bd. 19, pp. 324-369; Bd. 21, pp. 1-12, 134-155, (1839-1840); *Werke*, I. Bd., pp. 411-496, (Berlin, 1889).

a determinante $D = b^2 - ac$ *non quadrato*, e denotiamo con τ e σ rispettivamente il m. c. d. (a, b, c) e il m. c. d. $(a, 2b, c)$. Ricordiamo che f si dice *primitiva* quando $\tau = 1$, primitiva di prima specie quando $\tau = \sigma = 1$, primitiva di seconda specie quando $\tau = 1$, $\sigma = 2$.

La forma $f' \equiv (a', b', c') = Sf = S(a, b, c)$, trasformata della f, mediante S, ha i coefficienti a', b', c' assegnati dalle classiche formule $(\alpha\delta - \beta\gamma = 1)$:

$$(1) \qquad \begin{cases} a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \\ b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ c' = a\beta^2 + 2b\beta\delta + c\delta^2 . \end{cases}$$

La f' si dice equivalente a f rispetto a Γ: questa relazione è evidentemente riflessiva, simmetrica e transitiva. Le forme f di assegnato determinante si distribuiscono in un numero finito di classi equivalenti.

2. *Consideriamo, ora, l'insieme delle forme* f *primitive con un assegnato determinante* $\mathrm{D} = \mathrm{b}^2 - \mathrm{ac} \equiv 1 \pmod 4$, *non quadrato perfetto.* Partiamo dalla seguente interessante osservazione:

Ogni forma $\mathrm{f} \equiv (\mathrm{a}, \mathrm{b}, \mathrm{c})$, *primitiva di prima specie, è equivalente a un'altra forma (eventualmente coincidente con la prima) necessariamente primitiva e di prima specie* $\mathrm{f}' \equiv (\mathrm{a}', \mathrm{b}', \mathrm{c}')$ *nella quale* $\mathrm{a}' \equiv 0 \pmod 4$ *e* b', c' *sono dispari.*

Dimostrazione. - 1) Sia b pari: essendo $b^2 - ac \equiv 1 \pmod 4$ è $ac \equiv 3 \pmod 4$, e, pertanto, uno e uno solo dei due numeri dispari a e c è $\equiv 3 \pmod 4$, e $a + c \equiv 0 \pmod 4$.

Allora, per le (1) è

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} (a, b, c) = (a', b', c') = (a + 2b + c, b + c, c)$$

e questa forma possiede evidentemente i requisiti dichiarati.

2) Sia b dispari: allora $b^2 \equiv 1 \pmod 4$ e $ac \equiv 0 \pmod 4$, ed essendo m. c. d. $(a, 2b, c) = 1$, dovrà essere $a \equiv 0 \pmod 4$ e c dispari, oppure a dispari e $c \equiv 0 \pmod 4$. Nel primo caso assumiamo $f' = f$, e nel secondo caso si osserva che

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} (a, b, c) = (c, -b, a)$$

e questa forma possiede i requisiti richiesti.

Si conclude che un sistema di rappresentanti di classi di forme primitive di prima specie può esser scelto dal tipo

$$\text{(H)} \qquad \begin{gathered}(4a_1,\ b_1,\ c_1),\ (4a_2,\ b_2.\ c_2)\ldots(4a_h,\ b_h,\ c_h)\\ (a_i,\ b_i,\ c_i \text{ interi};\ b_i \text{ e } c_i \text{ dispari};\ i=1,\ 2,\ldots,\ h).\end{gathered}$$

Osservazione sulla parità di a_i. Gli interi a_i risultano tutti pari o tutti dispari secondochè è $D \equiv 1$ oppure 5 (mod 8). Infatti è $D = b^2 - 4ac = (4l \pm 1)^2 - 4ac = 8l' + 1 - 4ac \equiv -4ac + 1$ (mod 8) da cui, essendo c dispari, segue l'asserto.

3. *Equivalenza rispetto a* G_2. Seguendo l'uso, diremo che la forma f' è equivalente a f rispetto a G_2 (e scriveremo $f' \sim f(G_2)$) quando esiste una sostituzione S appartenente a G_2 tale che $f' = Sf$: poichè G_2 è un gruppo, questa relazione risulta, evidentemente, riflessiva, simmetrica e transitiva, e ripartisce le forme f di determinante D in classi di forme equivalenti rispetto a G_2.

Siano $g \equiv (2a,\ b,\ 2c)$ e $g' \equiv (2a',\ b',\ 2c')$, con b e b' dispari, due forme primitive di seconda specie.

Se $g' \sim g(G_2)$ è

$$2c' = 2(a\beta^2 + b\beta\delta + c\delta^2) \equiv 2c\delta \equiv 2c \pmod 4$$

essendo β pari (e δ dispari, poichè $\alpha\delta - \beta\gamma = 1$). Ne segue;

Se due forme primitive di seconda specie sono equivalenti rispetto a G_2, *esse hanno i rispettivi ultimi coefficienti ambedue pari e divisibili per 4, oppure ambedue pari e non divisibili per 4.*

4. *Le forme primitive di seconda specie, altrimenti dette impropriamente primitive,* (2a, b, 2c), *con* $2c \equiv 2 \pmod 4$.

Accanto al sistema (H) (cfr. n. 2) di forme propriamente primitive, o primitive di prima specie, consideriamo il seguente di forme primitive dì seconda specie,

$$\text{(H')} \qquad (2a_1,\ b_1,\ 2c_1).\ (2a_2,\ b_2,\ 2c_2),\ldots,\ (2a_h,\ b_h,\ 2c_h)$$

dove $2c_i \equiv 2 \pmod 4$ ed $i = 1,\ 2,\ldots,\ h$. Sussiste il seguente

TEOREMA. - *Il sistema* (H') *è un sistema completo di rappresentanti di forme* (2a, b, 2c) *primitive di seconda specie, aventi il terzo coefficiente* 2c *pari e non divisibile per 4, non equivalenti rispetto al gruppo* G_2.

In altri termini, posto $g_i \equiv (2a_i, b_i, 2c_i)$, con $2c_i \equiv 2 \pmod 4$, ed $i = 1, 2, \ldots, h$; e detta $f \equiv (2a, b, 2c)$, con $2c \equiv 2 \pmod 4$, una qualunque forma primitiva di seconda specie, si dimostra che:

α) esiste un i tale che $f \sim g_i (G_2)$;

β) da $g_i \sim g_k (G_2)$ segue $i = k$.

Dimostrazione di α). La forma $(4a, b, c)$, primitiva di prima specie, ha $D = b^2 - 4ac$, come la f, ed è equivalente a una certa forma di (H), per esempio a $(4a_i, b_i, c_i)$. Allora si ha

$$4a_i = 4a\alpha^2 + 2b\alpha\gamma + c\gamma^2$$

ove, essendo c dispari, risulta $\gamma = 2\gamma'$ pari. La sostituzione $\begin{pmatrix} \alpha & 2\beta \\ \gamma' & \delta \end{pmatrix}$ è unimodulare e di G_2: applicata a $(2a, b, 2c)$ ci fornisce:

$$\begin{pmatrix} \alpha & 2\beta \\ \gamma' & \delta \end{pmatrix} (2a, b, 2c) = (a', b', c')$$

e le formule (1) ci dànno

$$a' = 2a\alpha^2 + 2b\alpha\gamma' + 2c\gamma' = 2a_i \qquad \left(\gamma' = \frac{\gamma}{2}\right)$$

$$b' = 2a\alpha \cdot 2\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma'\delta = b_i$$

$$c' = 2a \cdot 4\beta^2 + 2b \cdot 2\beta\delta + 2c\delta^2 = 2c_i$$

e quindi,

$$\begin{pmatrix} \alpha & 2\beta \\ \gamma' & \delta \end{pmatrix} (2a, b, 2c) = (2a_i, b_i, 2c_i).$$

Dimostrazione di β). Sia $g_i \sim g_k (G_2)$, e, precisamente, $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} g_k = g_i$, con β pari. Tenendo presenti le formule (1) si vede immediatamente che

$$\begin{pmatrix} \alpha & \frac{\beta}{2} \\ 2\gamma & \delta \end{pmatrix} (4a_k, b_k, c_k) = (4a_i, b_i, c_i)$$

ed essendo le sostituzioni di (H) a due a due non equivalenti, deve essere $i = k$.

Il teorema risulta, così dimostrato.

Le forme quadratiche primitive di seconda specie $(2a, b, 2c)$ con $2c \equiv 0 \pmod 4$ costituiscono delle classi rispetto a G_2 che non hanno rappresentanti in (H').