Forme quadratiche e classi di ideali

Nel Capitolo V delle *Disquisitiones Arithmeticae* (1801) Carl Friedrich Gauss esamina a fondo le ***forme quadratiche binarie*** a coefficienti interi, ossia le espressioni della forma

$$f(x,y) = ax^2 + bxy + cy^2 \qquad \text{con } a,b,c \in \mathbb{Z}, \text{ e } a \neq 0.$$

La forma $f(x,y)$ è detta **primitiva** se $\mathrm{MCD}(a,b,c) = 1$.
Due **forme** sono da lui considerate **equivalenti** se è possibile trasformare l'una nell'altra tramite un cambio lineare invertibile di indeterminate a coefficienti interi, la cui matrice associata abbia determinante uno. In questo modo è definita una relazione di equivalenza, che si può restringere all'insieme delle forme primitive.
Il ***discriminante*** della forma f, il numero $D = b^2 - 4ac$, è invariante per equivalenza. Se $D < 0$, la forma è definita positiva o definita negativa (secondo che sia $a > 0$ oppure $a < 0$). Se invece $D > 0$ la forma assume sia valori positivi, sia valori negativi. Il caso $D = 0$ è di scarso interesse, in quanto corrisponde a forme ottenute elevando al quadrato una forma lineare omogenea. Gauss affronta il problema di determinare, per ogni valore di D, il numero (sempre finito) di classi di equivalenza di forme primitive, selezionando in ognuna di esse un rappresentante canonico.

Precisamente, nel caso in cui $D < 0$, Gauss prova che un sistema completo di rappresentanti per le forme primitive e definite positive si ottiene selezionando tutte e sole le forme siffatte che sono **ridotte**, ossia verificano la seguente condizione:

$$|b| \leq a \leq c, \text{ e } b \geq 0 \text{ se una delle relazioni è un'uguaglianza.}$$

L'argomento è di interesse ai fini dello studio della rappresentabilità di un dato numero intero positivo come $f(x,y)$, per opportuni interi x,y, un tema già affrontato da Pierre de Fermat. Si può provare che forme equivalenti assumono lo stesso insieme di valori interi. Non vale, però, il viceversa.

I successivi sviluppi teorici, dovuti a vari matematici, tra cui Richard Dedekind e David Hilbert, hanno stabilito, per ogni D, una corrispondenza biunivoca tra i rappresentanti canonici delle forme (primitive, definite positive) di discriminante D e un sistema completo di rappresentanti delle classi di ideali dell'anello A degli interi del campo quadratico $K = \mathbb{Q}\left(\sqrt{D}\right)$, precisamente

$$ax^2 + bxy + cy^2 \mapsto \left(a, \frac{-b + \sqrt{D}}{2}\right)$$

In altri termini, il numero calcolato da Gauss coincide con il numero delle classi di ideali del dominio di Dedekind A.

Esempio 1 (Rappresentabilità di numeri interi)

Sia $D = -8$. Allora vi è un'unica classe di forme quadratiche primitive definite positive, rappresentata da $f(x,y) = x^2 + 2y^2$. Il campo quadratico è $K = \mathbb{Q}\left(i\sqrt{2}\right)$, il cui anello degli interi è $A = \mathbb{Z}\left[i\sqrt{2}\right]$. Il suo numero delle classi di ideali è 1, ossia A è un UFD.
Sia ora m un intero per il quale esistono interi x,y tali che $m = x^2 + 2y^2$ (*). Possiamo supporre che m,x,y siano coprimi (vedi Nota). Sia ora **p un fattore primo di m in $\mathbb{Z}$**. Allora, in A, vale la seguente relazione di divisibilità:

$$p \mid \left(x - i\sqrt{2}y\right)\left(x + i\sqrt{2}y\right),$$

ove, tuttavia, p non divide alcuno dei due fattori (non dividendo almeno uno degli interi x e y). Ne consegue che **p non è primo in A**, e quindi è ivi riducibile. Siano $\alpha, \beta \in A$ non invertibili tali che $p = \alpha\beta$. Allora, passando alle norme, $p^2 = \alpha\beta\overline{\alpha}\,\overline{\beta} = (\alpha\overline{\alpha})(\beta\overline{\beta})$, ove i fattori dell'ultimo prodotto sono interi maggiori di 1. Pertanto sono entrambi uguali a p. Ma, allora, posto $\alpha = a + i\sqrt{2}b,$ si ha $p = a^2 + 2b^2$, dunque **p ammette una rappresentazione (*).** Viceversa, **se un numero intero p ammette una tale rappresentazione, allora p non è primo in A. Inoltre, se ogni fattore primo p del numero intero m verifica questa condizione, allora m ammette una rappresentazione (*).**

D'altra parte, sappiamo che p non è primo in A **se e solo se** -2 **è un residuo quadratico modulo p**, ossia **se e solo se $p = 2$ oppure p è dispari e** $\left(\frac{-2}{p}\right) = 1$. Proviamo, per p dispari, che ciò avviene se e solo se **$p \equiv 1$ oppure $p \equiv 3 \pmod 8$**.

Si ha:

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right).$$

Il primo fattore è noto, determiniamo il secondo. In base al criterio di Eulero, $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod p$. Sia $s = \frac{p-1}{2}$. Notiamo preliminarmente che, per ogni intero i,

$$2(s-i) = p - 1 - 2i \equiv -(2i+1) \pmod p .$$

Quindi consideriamo $s! = \prod_{i=1}^{s} i(-1)^i(-1)^i = (-1)^{\frac{s(s+1)}{2}} \prod_{i \text{ pari}} i \cdot \prod_{i \text{ dispari}} (-i)$

$$\equiv (-1)^{\frac{s(s+1)}{2}} \prod_{i \text{ pari}} i \cdot \prod_{i \text{ dispari}} 2\left(s - \frac{i-1}{2}\right) \pmod p$$

Se s è pari,

- i fattori della prima produttoria sono $2k$ con $k = 1, \ldots \frac{s}{2}$,
- i fattori della seconda produttoria sono $2k$ con $k = \frac{s}{2} + 1, \ldots, s$.

Se s è dispari,

- i fattori della prima produttoria sono $2k$ con $k = 1, \ldots \frac{s-1}{2}$,
- i fattori della seconda produttoria sono $2k$ con $k = \frac{s+1}{2}, \ldots, s$.

In ogni caso si ottiene:

$$s! \equiv (-1)^{\frac{s(s+1)}{2}} 2^s s! \pmod p,$$

da cui, potendo cancellare $s!$, non divisibile per p,

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

Ne consegue che

$\left(\frac{2}{p}\right) = 1$ se e solo se $p \equiv 1$ oppure $p \equiv 7 \pmod 8$.

D'altra parte,

$\left(\frac{-1}{p}\right) = 1$ se e solo se $p \equiv 1 \pmod 4$.

Pertanto $\left(\frac{-2}{p}\right) = 1$ se e solo se $p \equiv 1$ oppure $p \equiv 3 \pmod 8$.

In conclusione, m ammette una rappresentazione (*) se e solo se ogni suo fattore primo dispari p verifica la precedente condizione.

Rimuovendo l'ipotesi di coprimalità, si avrà: m **ammette una rappresentazione (*) se e solo se i suoi fattori primi dispari** p **non verificanti la precedente condizione hanno molteplicità pari** (vedi Nota).

Esempio 2 (Determinazione di un gruppo delle classi di ideali)

Sia $D = -56$. Allora Il campo quadratico è $K = \mathbb{Q}\left(i\sqrt{14}\right)$, il cui anello degli interi è $A = \mathbb{Z}\left[i\sqrt{14}\right]$. Il suo numero delle classi di ideali è 4, e le classi di forme quadratiche sono rappresentate da

$x^2 + 14y^2$
$2x^2 + 7y^2$
$3x^2 - 2xy + 5y^2$
$3x^2 + 2xy + 5y^2$

corrispondenti ai seguenti ideali:

$A = (1)$
$P_1 = \left(2, i\sqrt{14}\right)$
$P_2 = \left(3, 1 + i\sqrt{14}\right)$
$P_3 = \left(3, 1 - i\sqrt{14}\right)$

le cui norme sono: $1,\ 2,\ 3,\ 3$.

Si ha $P_1^2 = (2)$. Infatti $P_1^2 \subset (2)$, ed entrambi gli ideali hanno norma 4. Dunque, nel gruppo delle classi degli ideali di A, $[P_1]^{-1} = [P_1]$.

Si noti che P_1 e P_3 sono coprimi, dunque lo sono anche P_1 e $P_3^2 = \left(9,\ 3 - 3i\sqrt{14},\ -13 - 2i\sqrt{14}\right)$. Ad entrambi appartiene $\alpha = 2 + i\sqrt{14}$. Pertanto $(\alpha) \subset P_1 \cap P_3^2 = P_1 P_3^2$. Quest'ultimo ideale ha norma 18, esattamente come (α). Quindi l'inclusione è, in realtà, un'uguaglianza. Ne consegue che

$[P_1][P_3]^2 = [(1)]$, da cui $[P_3]^2 = [P_1]^{-1} = [P_1]$. Dunque $[P_3]$ ha periodo 4. In conclusione, il gruppo delle classi di ideali di A è ciclico.

Nota

Supponiamo che esista una rappresentazione (*) in cui m, x, y non sono coprimi. Allora $d = \mathrm{MCD}(m, x^2, y^2) > 1$. Proviamo che ogni fattore primo dispari di d ha molteplicità pari. Sia p un suo fattore primo dispari. Allora, se, per qualche numero naturale t, $p^{2t+1}|d$, in particolare $p^{2t+1}|x^2$, e quindi $p^{2t+2}|x^2$. Analogamente si vede che $p^{2t+2}|y^2$. Ne consegue che $p^{2t+2}|m$, e quindi $p^{2t+2}|d$. Ciò prova che la massima potenza di p che divide d ha esponente pari. Pertanto, per qualche intero positivo e, $d = e^2$ oppure $d = 2e^2$. In entrambi i casi $e|x$, $e|y$. Nel primo caso, $\frac{m}{e^2} = \left(\frac{x}{e}\right)^2 + 2\left(\frac{y}{e}\right)^2$, ove $\frac{m}{e^2}$, $\frac{x}{e}$, $\frac{y}{e}$ sono coprimi. Nel secondo caso, $\frac{x}{e}$ e $\frac{y}{e}$ sono pari, e pertanto $4|\frac{m}{e^2}$. Quindi una rappresentazione del tipo voluto è $\frac{m}{4e^2} = \left(\frac{x}{2e}\right)^2 + 2\left(\frac{y}{2e}\right)^2$, ove $\frac{m}{4e^2}$, $\frac{x}{2e}$, $\frac{y}{2e}$ sono coprimi. Poiché i fattori primi "indesiderati" non possono più essere presenti in $\frac{m}{e^2}$ o $\frac{m}{4e^2}$, rispettivamente, essi fanno parte della fattorizzazione di e^2, e quindi compaiono in m con molteplicità pari.

Viceversa, se m contiene fattori primi indesiderati, ma tutti con molteplicità pari, allora dividendo m per il loro prodotto (che è un quadrato perfetto), si ottiene un prodotto di soli fattori primi "desiderati", e quindi un numero avente la rappresentazione voluta. Moltiplicando per il quadrato per cui si è diviso, se ne ricava una rappresentazione anche per m.

Osservazione aggiuntiva: il ruolo del fattore primo 2 è inessenziale. Se un numero pari m ammette una rappresentazione (*), allora anche la sua metà la ammette. Infatti in tal caso x è pari e si ha: $\frac{m}{2} = y^2 + 2\left(\frac{x}{2}\right)^2$. Ma anche il suo doppio la ammette, in quanto $2m = (2y)^2 + 2x^2$.

APPENDICE

A proposito del discriminante

Proposizione I possibili valori di D sono tutti e soli gli interi congrui a 0 oppure a 1 modulo 4.

Dim.: Chiaramente ogni discriminante verifica la proprietà indicata. Viceversa, se D è un numero avente tale proprietà, allora, se $D \equiv 0 \pmod 4$, è il discriminante della forma $x^2 - \frac{D}{4}y^2$, e, se $D \equiv 1 \pmod 4$, è il discriminante della forma $x^2 + xy + \frac{1-D}{4}y^2$.

Ricordiamo che dato un intero d, diverso da 0 e da 1, e privo di quadrati, l'anello degli interi del campo quadratico $K = \mathbb{Q}(\sqrt{d})$ è $\mathbb{Z}[\alpha]$, ove $\alpha = \sqrt{d}$ se $d \equiv 2, 3 \pmod 4$, mentre $\alpha = \frac{1+\sqrt{d}}{2}$ se $d \equiv 1 \pmod 4$. Si dice **discriminante (fondamentale)** di K il discriminante d_K del polinomio minimo di α su $\mathbb{Q}$, che è, nei due casi, rispettivamente,

- $f(x) = x^2 - d \qquad \longrightarrow d_K = 4d$
- $f(x) = x^2 - x + \frac{1-d}{4} \qquad \longrightarrow d_K = d.$

Si noti che, in ogni caso, $K = \mathbb{Q}\left(\sqrt{d_K}\right)$.

A proposito della rappresentabilità dei numeri mediante forme

Si dice che la forma $f(x,y)$ **rappresenta propriamente** un numero intero m se esistono interi x, y coprimi tali che $f(x,y) = m$.

Lemma 1 Forme equivalenti rappresentano propriamente gli stessi numeri interi.

(Senza dim.)

Lemma 2 La forma $f(x,y)$ rappresenta propriamente il numero intero m se e solo se è equivalente ad una forma del tipo $mx^2 + uxy + vy^2$.

Dim.: Siano z, w interi coprimi tali che $f(z,w) = m$. Dati i coefficienti s, t di Bézout di un'identità $sz + tw = 1$, si consideri la matrice $\alpha = \begin{pmatrix} z & w \\ -t & s \end{pmatrix}$, a coefficienti interi e di determinante uno. Allora $f((x,y)\alpha)$ è una forma equivalente a $f(x,y)$, ottenuta sostituendo a x l'espressione $zx - ty$, e a y l'espressione $wx + sy$. In questa forma il coefficiente di x^2 è $az^2 + bzw + cw^2 = m$.

Proposizione Sia D un discriminante, e sia m un intero coprimo con D. Allora m è rappresentato propriamente da una forma primitiva di discriminante D se e solo se D è un quadrato modulo $4m$.

Dim.: Se m è rappresentato propriamente dalla forma primitiva $f(x,y)$ di discriminante D, allora, per i Lemmi precedenti, è rappresentato propriamente anche da una forma equivalente del tipo $f'(x,y) = mx^2 + uxy + vy^2$, il cui discriminante è ancora D. Quindi $D = u^2 - 4mv$, e dunque D è un quadrato modulo $4m$. Viceversa, supponiamo che D sia di questo tipo. Allora la forma $f'(x,y)$ rappresenta propriamente m (per $x = 1,\ y = 0$) ed è primitiva: infatti ogni divisore comune di m, u, v divide D, che, per ipotesi, è coprimo con m.

Corollario Sia m un intero e sia p un numero primo dispari che non divide m. Allora p è rappresentato da una forma primitiva di discriminante $-4m$ se e solo se $\left(\frac{-m}{p}\right) = 1$.

Dim.: Si noti anzitutto che, per un numero primo, la rappresentabilità è necessariamente propria. In base alla precedente proposizione, p è dunque rappresentato da una forma primitiva di discriminante $-4m$ se e solo se $-4m$ è un quadrato modulo $4p$, ossia se e solo se $-m$ è un residuo quadratico modulo p.

Esempio La forma $f(x,y) = x^2 + y^2$ ha discriminante $D = -4$. Quindi un primo dispari p è decomponibile nella somma di due quadrati se e solo se $\left(\frac{-1}{p}\right) = 1$. Ciò avviene se e solo se $p \equiv 1 \pmod 4$.

A proposito delle forme ridotte

Si dimostra che, per un discriminante $D < 0$, le forme ridotte aventi tale discriminante sono tutte della forma $f(x,y) = ax^2 + bxy + \frac{m}{a}y^2$ con

- $\frac{-D}{4} \le m \le \frac{-D}{3}$

- $a|m$
- $a^2 \leq m$
- $D + 4m = b^2$

Quindi possono essere determinate attraverso una ricerca finita.

Esempio
Determiniamo tutte le forme primitive ridotte (definite positive) con discriminante $D = -56$. Dovrà allora essere $a > 0$. I possibili valori di m sono $14, 15, 16, 17, 18$. Il numero $D + 4m$ è un quadrato solo per alcuni di questi valori, precisamente:

- per $m = 14 \longrightarrow b = 0$
- per $m = 15 \longrightarrow b = 2$ oppure $b = -2$
- per $m = 18 \longrightarrow b = 4$ oppure $b = -4$

Tuttavia, nell'ultimo caso, dovendo essere $a \in \{1, 2, 3\}$, e quindi $|b| > a$, la forma risultante non è mai ridotta.

Nel primo caso, $a \in \{1, 2\}$. Si ottengono le forme $f_1(x, y) = x^2 + 14y^2$, $f_2(x, y) = 2x^2 + 7y^2$, entrambe primitive e ridotte.

Nel secondo caso, $a \in \{1, 3\}$. Per $a = 3$ si ottengono le forme $f_3(x, y) = 3x^2 + 2xy + 5y^2$, $f_4(x, y) = 3x^2 - 2xy + 5y^2$, entrambe primitive ridotte. Per $a = 1$ non si ottengono forme ridotte.

Dunque le classi di equivalenza delle forme primitive definite positive di discriminante -56 sono esattamente 4.