

Breve nota sugli anelli $\mathbb{Z}[\sqrt{A}]$ e l'equazione di Pell-Fermat.

Versione del 29 Febbraio 2008

Importanti esempi di **domini di integrità** si costruiscono generalizzando il caso degli interi di Gauss:

Sia $A \neq 0 \in \mathbb{Z}$. Allora l'insieme:

$$\mathbb{Z}[\sqrt{A}] = \{a + \sqrt{A}b \text{ con } a, b \in \mathbb{Z}\}$$

è un sottoanello commutativo di $\mathbb{C}$ senza divisori dello zero (dove $0 = 0 + \sqrt{A}0$, e $1 = 1 + \sqrt{A}0$).

Ovviamente se $A \geq 0$ ed è il quadrato di un numero naturale, l'anello $\mathbb{Z}[\sqrt{A}]$ è isomorfo a $\mathbb{Z}$; se invece $A = -1$ l'anello è $\mathbb{Z}[i]$. Quest'ultimo anello è detto *anello degli interi di Gauss*. Supporremo pertanto che **A non sia un quadrato**.

I divisori dello zero $a + \sqrt{A}b \neq 0$ sono elementi tali che esiste $(x + \sqrt{A}y) \neq 0$ in modo che:

$$(x + \sqrt{A}y)(a + \sqrt{A}b) = 0.$$

Osserviamo ora che se $a + \sqrt{A}b = 0$, necessariamente $a = b = 0$. Infatti se $A < 0$ il risultato si ottiene separando la parte reale e la parte immaginaria, mentre se $A > 0$ il risultato si ottiene osservando che se A non è un quadrato, se $a + \sqrt{A}b = 0$ con a e b ambedue $\neq 0$, si otterrebbe $\sqrt{A} = -\frac{a}{b}$, ma questo è assurdo perchè $\sqrt{A}$ è un numero irrazionale¹. Dobbiamo quindi studiare il sistema:

$$\begin{cases} ax + Aby = 0 \\ bx + ay = 0 \end{cases}$$

¹Infatti se $A > 0$ non è un quadrato deve necessariamente contenere almeno un fattore primo p elevato a una potenza dispari, ovvero deve essere $A = p^{2\alpha+1}B$ e B non contiene p come fattore primo. Se $\sqrt{A}$ fosse razionale, sarebbe $\sqrt{A} = \frac{a}{b}$ con a e b primi fra loro. Cioè $a^2 = p^{2\alpha+1}Bb^2$, e quindi $a^2 \bmod p = 0$ e allora, essendo $\mathbb{Z}_p$ un campo, $a \bmod p = 0$. Cioè si avrebbe $a = kp$ e quindi $(kp)^2 = p^{2\alpha+1}Bb^2$, otteniamo allora:

$$k^2 = p^{2\alpha-1}Bb^2$$

Ancora si ottiene $k^2 \bmod p = 0$ e allora, essendo $\mathbb{Z}_p$ un campo, $k \bmod p = 0$. Cioè si avrebbe $k = hp$ e quindi $(hp)^2 = p^{2\alpha-1}Bb^2$, quindi:

$$h^2 = p^{2\alpha-3}Bb^2$$

Procediamo così fino a quando l'esponente di p a destra dell'uguale si riduce a 1 (non può ridursi a zero perchè ad ogni passo sottraiamo 2 ad un numero dispari). Abbiamo quindi, dopo un numero finito di passi:

$$l^2 p^2 = p B b^2$$

e quindi anche $b^2 \bmod p = 0$, cioè $b \bmod p = 0$, ma questo è assurdo perchè abbiamo supposto a e b primi fra loro. Il lettore con buona memoria noterà che abbiamo banalmente generalizzato la dimostrazione elementare e notissima del fatto che $\sqrt{2}$ è irrazionale.

Questo sistema lineare omogeneo nelle incognite x, y ha soluzioni diverse da zero se e solo se $a^2 - Ab^2 = 0$. Questo però non può mai verificarsi: se $A < 0$ dovrebbe essere $a = b = 0$ (escluso per ipotesi), se invece $A > 0$, $a^2 - Ab^2 = 0$ implicherebbe la razionalità di $\sqrt{A}$ contro l'ipotesi che A non sia un quadrato.

La ricerca delle unità in questi anelli coinvolge interessanti questioni di teoria elementare dei numeri. Mentre il caso $A < 0$ non presenta ulteriori difficoltà e verrà studiato in seguito, il caso $A > 0$ si basa su un'importante equazione diofantina di secondo grado, già nota come "equazione di Pell" oppure di Fermat, che la studiò approfonditamente, pur senza giungere a risultati completi (il risultato definitivo fu raggiunto da Lagrange). Siccome

L'equazione in questione è:

$$x^2 - Ay^2 = \pm 1$$

con x, y interi che possiamo supporre > 0 (trascuriamo infatti, nel caso $x^2 - Ay^2 = 1$, le soluzioni banali $x = \pm 1, y = 0$) e, inoltre, $A > 0$ non deve essere il quadrato di un naturale.

L'equazione ha a che vedere con la ricerca delle unità **non banali** di $\mathbb{Z}[A]$ perchè:

$$(x + \sqrt{A}y)(x - \sqrt{A}y) = x^2 - Ay^2$$

e quindi, se $x^2 - Ay^2 = 1$, allora $(x \pm \sqrt{A}y)$ è una unità perchè ha inverso $(x \mp \sqrt{A}y)$, mentre nel caso $x^2 - Ay^2 = -1$, $(\pm x + \sqrt{A}y)$ è una unità perchè ha inverso $(\mp x + \sqrt{A}y)$.

Se troviamo una unità non banale, ad esempio $(x + \sqrt{A}y)$ con $x^2 - Ay^2 = 1$, è chiaro che anche $(x + \sqrt{A}y)^n$ per ogni n intero è una unità e quindi questi anelli, se hanno una unità non banale, ne hanno infinite. Lagrange ha dimostrato che l'equazione $x^2 - Ay^2 = 1$ ha sempre soluzioni non banali, mentre il caso $x^2 - Ay^2 = -1$ non sempre è risolubile.

Vediamo subito un esempio: se $A = 7$, allora da $x^2 - 7y^2 = -1$ seguirebbe che $x^2 = -1 = 6 \pmod{7}$, e questo, esaminando la tavola di moltiplicazione di $\mathbb{Z}_7^*$ si rivela impossibile. Nel caso $x^2 - Ay^2 = 1$ si ricava invece $x^2 = 1 \pmod{7}$ e questo è possibile in infiniti modi, basta considerare i numeri della forma: $x = 1 + 7k$, oppure $x = 6 + 7k$. Naturalmente queste condizioni sono solo necessarie per l'esistenza di soluzioni, trovare a quali di questi numeri corrisponde effettivamente una soluzione è tutta un'altra storia! Nel caso del nostro esempio è facile trovare una soluzione particolare: $x = 8, y = 3$. Questa soluzione si chiama "fondamentale", perchè è la soluzione con $x, y > 0$ in cui x, y assumono il minimo valore possibile.

Analizziamo un po' più approfonditamente il caso $x^2 - Ay^2 = 1$.

Trovata la soluzione fondamentale (Lagrange ha dimostrato che esiste sempre, e ha trovato un procedimento molto laborioso per trovarla; la sua teoria, specialmente il procedimento costruttivo, è tutt'altro che banale perchè richiede la teoria delle frazioni continue ed è stato lo scoglio su cui si è arenato il grande Fermat), è facile trovare *infinite* soluzioni, poniamo:

$$\begin{aligned} (x_n + \sqrt{A}y_n) &= (x + \sqrt{A}y)^n \quad \text{da cui:} \\ (x_n - \sqrt{A}y_n) &= (x + \sqrt{A}y)^{-n} \end{aligned}$$

E' chiaro, per quanto detto sopra, che x_n, y_n è una soluzione se x, y lo è.

Se introduciamo le matrici:

$$M_n = \begin{pmatrix} x_n & Ay_n \\ y_n & x_n \end{pmatrix}$$

Abbiamo che tutte queste matrici sono invertibili perchè $\det M = 1$.

Si trova anche, per induzione, che:

$$M_n = \begin{pmatrix} x_1 & Ay_1 \\ y_1 & x_1 \end{pmatrix}^n$$

Inoltre:

$$\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 & Ay_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

Che si generalizza subito:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} x_n & Ay_n \\ y_n & x_n \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 & Ay_1 \\ y_1 & x_1 \end{pmatrix}^n \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

Possiamo ora dimostrare, con Fermat (anche se ovviamente, non con le sue notazioni) che, in questo modo, partendo dalla soluzione fondamentale troviamo *tutte* le soluzioni positive. La dimostrazione è molto brillante e si basa su un tipo di ragionamento molto caro a Fermat che lo inventò e lo utilizzò con successo in moltissimi teoremi. Il principio è (apparentemente) banale e consiste essenzialmente nel fatto che ogni insieme di numeri interi positivi ha un unico elemento minimo.

L'insieme delle soluzioni positive (x_n, y_n) può essere ordinato per ordine crescente delle x , esiste dunque un primo elemento (x_1, y_1) ; per tutti gli altri n si ha: $x_n > x_1 > 1$ e $y_n > y_1 > 0$, infatti:

$$(x_n + \sqrt{A}y_n) = (x_1 + \sqrt{A}y_1)^n \Rightarrow x_n = x_1^n + \dots$$

Si vede allora che ambedue le successioni $x_n, y_n \rightarrow \infty$.

E' chiaro allora che per ogni coppia di soluzioni positive (x, y) possiamo trovare un n tale che:

$$\begin{aligned} x_n &\leq x < x_{n+1} \\ y_n &\leq y < y_{n+1} \end{aligned}$$

Otteniamo allora:

$$x_n + \sqrt{A}y_n \leq x + y\sqrt{A} < x_{n+1} + \sqrt{A}y_{n+1}$$

A questo punto moltiplichiamo i tre membri per $x_n - \sqrt{A}y_n$, ottenendo:

$$1 \leq (x + y\sqrt{A})(x_n - \sqrt{A}y_n) < (x_{n+1} + \sqrt{A}y_{n+1})(x_n - \sqrt{A}y_n)$$

Osserviamo ora che $(x + y\sqrt{A})(x_n - \sqrt{A}y_n)$ è una soluzione perchè è una unità essendo il prodotto di due unità, mentre:

$$(x_{n+1} + \sqrt{A}y_{n+1})(x_n - \sqrt{A}y_n) = (x_1 + \sqrt{A}y_1)^{n+1} (x_1 + \sqrt{A}y_1)^{-n} = x_1 + \sqrt{A}y_1$$

Abbiamo quindi trovato una soluzione strettamente minore della soluzione fondamentale e questo è assurdo.

Deve quindi essere $x = x_n, y = y_n$: tutte le soluzioni si ottengono dalla formula $(x_n + \sqrt{A}y_n) = (x_1 + \sqrt{A}y_1)^n$.

Osserviamo ora che se l'equazione $x^2 - Ay^2 = -1$ è risolubile, e u, v è la sua soluzione fondamentale, allora

$$\begin{aligned}x &= u^2 + Av^2 \\ y &= 2uv\end{aligned}$$

è la soluzione fondamentale di $x^2 - Ay^2 = 1$. Cioè:

$$x + \sqrt{A}y = (u + \sqrt{A}v)^2$$

Consideriamo ad esempio $\mathbb{Z}[\sqrt{5}]$: la soluzione fondamentale di $x^2 - 5y^2 = -1$ esiste ed è ovviamente $u = 2, v = 1$. Allora $x = 9, y = 4$ è la soluzione fondamentale di $x^2 - 5y^2 = 1$. Il gruppo delle unità è allora generato dagli elementi $(9 + 4\sqrt{5})$ e $(2 + \sqrt{5})$. Essendo però $(9 + 4\sqrt{5}) = (2 + \sqrt{5})^2$ abbiamo che il gruppo delle unità è isomorfo a $\mathbb{Z}$. Infatti:

$$(9 + 4\sqrt{5})^n (2 + \sqrt{5})^m = (2 + \sqrt{5})^{2n+m}$$

Questo risultato è valido in generale: **il gruppo delle unità dell'anello $\mathbb{Z}[\sqrt{A}]$ con $A > 0$ intero non quadrato è sempre ciclico infinito.** Infatti se x, y è la soluzione fondamentale di $x^2 - Ay^2 = 1$ e $x^2 - Ay^2 = -1$ non è risolubile, allora $g = x + \sqrt{A}y$ è un generatore. Se invece $x^2 - Ay^2 = -1$ è risolubile e la sua soluzione fondamentale è u, v allora un generatore è $g = u + \sqrt{A}v$.

Per illustrare la difficoltà computazionale del problema ecco un esempio: $x^2 - 61y^2 = -1$ è risolubile, la sua soluzione fondamentale è $u = 29718, y = 3805$, allora $x = 29718^2 + 61 \times 3805^2 = 1766\,319\,049$ e $y = 2 \times 29718 \times 3805 = 226\,153\,980$ è la più piccola soluzione di $x^2 - 61y^2 = 1$.

Studiamo ora il caso $A < 0$. L'equazione in questione è ancora:

$$x^2 - Ay^2 = \pm 1$$

Il caso $x^2 - Ay^2 = -1$ è sempre escluso per ragioni di segno e resta solo il caso $x^2 - Ay^2 = 1$. Se $A < -1$ le soluzioni sono solo $x = \pm 1, y = 0$, mentre nel caso $A = -1$ appaiono anche le soluzioni $x = 0, y = \pm 1$. **il gruppo delle unità dell'anello $\mathbb{Z}[\sqrt{A}]$ con $A < 0$ intero è sempre ciclico finito:** se $A = -1$ il gruppo è $\{\pm 1, \pm i\}$, se $A < -1$ il gruppo è $\{\pm 1\}$.