Lezione 25

Prerequisiti: Lezione 24.

Risolubilità di equazioni diofantee.

In questa lezione applichiamo il numero delle classi di ideali alla risoluzione di *equazioni diofantee*, ossia equazioni polinomiali a coefficienti interi in più incognite, di cui si cercano le soluzioni intere.

Esempio 25.1 Proviamo che l'unica soluzione (intera) dell'equazione diofantea $x^3 - y^2 = 1$ è (1,0).

Esaminiamo dapprima la parità delle soluzioni (x,y). Se supponiamo che x sia pari, allora $x^3 \equiv 0$ (mod 8), quindi $y^2 \equiv 7$ (mod 8). Ma ciò è impossibile. Infatti i possibili resti modulo 8 di un quadrato perfetto sono: 0, 1, 4. Quindi x è dispari, e di conseguenza y è pari.
Quindi riscriviamo l'equazione nella forma $y^2 + 1 = x^3$, e fattorizziamo il primo membro su $\mathbf{Z}[i]$:

$$(y+i)(y-i) = x^3. \tag{1}$$

Sfruttiamo ora il fatto ben noto che $\mathbf{Z}[i]$ è un UFD, in quanto è un dominio euclideo, (vedi Algebra 2, Proposizione 16.4). Gli interi gaussiani $y+i$ e $y-i$ sono coprimi. Supponiamo per assurdo che essi ammettano un comune fattore primo p. Allora p divide $y+i-(y-i) = 2i = (1+i)^2$. Ma $1+i$ è irriducibile in $\mathbf{Z}[i]$, perché tale è la sua norma, che è pari a 2. Quindi, per la proprietà di fattorizzazione unica, necessariamente $1+i$ coincide (a meno di un fattore invertibile) con p. Allora $1+i$ divide $(y+i)(y-i) = x^3$, quindi divide x. Sia $a \in \mathbf{Z}[i]$ tale che $x = (1+i)a$. Allora, moltiplicando entrambi i membri per il complesso coniugato, si ha

$$x\overline{x} = (1-i)(1+i)a\overline{a}, \quad \text{cioè} \quad x^2 = 2a\overline{a}, \quad \text{quindi 2 divide } x^2 \text{ in } \mathbf{Z}.$$

Avevamo però stabilito che x è necessariamente dispari.

Dalla (1) segue allora, per la proprietà di fattorizzazione unica, che $y+i, y-i$ sono del tipo uc^3, dove $u, c \in \mathbf{Z}[i]$, e u è invertibile. Ma allora, in base all'Esempio 23.16 a), $u \in \{1, -1, i, -i\}$, e quindi u è a sua volta un cubo in $\mathbf{Z}[i]$. Sia allora $y+i = (a+ib)^3$, con $a, b \in \mathbf{Z}$. Allora

$$y+i = (a^3 - 3ab^2) + (3a^2b - b^3)i, \text{ da cui } y = a(a^2 - 3b^2) \text{ e } 1 = b(3a^2 - b^2). \tag{2}$$

L'ultima uguaglianza implica che $b=1$ oppure $b=-1$. Se $b=1$, allora $1 = 3a^2 - 1$, da cui $3a^2 = 2$, impossibile. Se $b=-1$, allora $-1 = 3a^2 - 1$, da cui $a=0$. Dalla (2) segue allora che $y=0$, e quindi $x=1$. Pertanto l'unica soluzione è (1,0), come volevasi.

Esempio 25.2 Proviamo che l'equazione diofantea $x^3 - y^2 = 5$ non ha soluzione.

Il procedimento dimostrativo ricalcherà quello dell'esempio precedente, con le varianti necessarie: è chiaro che l'anello $\mathbf{Z}[i]$ dovrà essere sostituito da $\mathbf{Z}[i\sqrt{5}]$: questo non è UFD. A ciò sopperiremo utilizzando:

- la proprietà della fattorizzazione per gli ideali in un dominio di Dedekind;
- il fatto che $|Cl(\mathbf{Z}[i\sqrt{5}])| = 2$.

Il primo passo è identico a sopra: si esclude che x possa essere pari, poiché nessun intero y verifica $y^2 \equiv 3 \pmod 4$. Pertanto x è dispari e y è pari. Inoltre è facile vedere che x e y sono coprimi. Quindi si considera la decomposizione di ideali

$$(y + i\sqrt{5})(y - i\sqrt{5}) = (x)^3 \qquad (3)$$

Proviamo che gli ideali $(y + i\sqrt{5}), (y - i\sqrt{5})$ non hanno fattori comuni non banali. Supponiamo per assurdo che essi ammettano un comune fattore primo P. Allora P divide $(x)^3$ (e quindi divide (x)), Inoltre, in virtù dell'Esercizio 22.20, l'ideale primo P divide (cioè contiene) anche l'ideale somma $(y + i\sqrt{5}) + (y - i\sqrt{5}) = (y + i\sqrt{5}, y - i\sqrt{5}) = (2y, y + i\sqrt{5}) \supset (2y)$, e quindi contiene (cioè divide) $(2y) = (2)(y)$. Essendo x dispari, si ha che (x) e (2) sono coprimi, per cui P non divide (2). Ma allora P divide (y). Quindi, in base all'Esercizio 22.20, P divide $(x) + (y) = \mathbf{Z}[i\sqrt{5}]$, assurdo. Dalla (3) segue allora, per la proprietà di fattorizzazione unica degli ideali, che $(y + i\sqrt{5}) = I^3, (y - i\sqrt{5}) = J^3$ per opportuni ideali interi I,J di $\mathbf{Z}[i\sqrt{5}]$. Allora in $Cl(\mathbf{Z}[i\sqrt{5}])$ si ha $[I]^3 = [J]^3 = [(1)]$. Poiché, in base all'Esercizio 24.7, $Cl(\mathbf{Z}[i\sqrt{5}])$ ha ordine due, segue che $[I] = [J] = [(1)]$, cioè I e J sono ideali principali. In particolare $(y + i\sqrt{5}) = (a + ib\sqrt{5})^3 = \left((a + ib\sqrt{5})^3\right)$ per opportuni $a, b \in \mathbf{Z}$. Pertanto $y + i\sqrt{5}$ e $(a + ib\sqrt{5})^3$ differiscono per un fattore invertibile, ossia, in base all'Esempio 23.16 b), coincidono a meno del segno. Quindi possiamo supporre che sia $y + i\sqrt{5} = (a + ib\sqrt{5})^3$, cioè

$$y + i\sqrt{5} = (a^3 - 15ab^2) + (3a^2b - 5b^3)i\sqrt{5}, \text{ da cui } y = a(a^2 - 15b^2) \text{ e } 1 = b(3a^2 - 5b^2). \qquad (4)$$

L'ultima uguaglianza implica che $b = \pm 1$, e quindi si ha che $3a^2 - 5 = \pm 1$, impossibile. Ciò prova che l'equazione diofantea proposta non ha soluzione.