Equazione di Pell

Scopo di questa nota è provare, usando metodi elementari, che se d è un numero naturale libero da quadrati, l'equazione diofantea $x^2 - dy^2 = 1$ ha infinite soluzioni. Iniziamo con un lemma.

Lemma 1 *Sia $d \in \mathbb{N}$ libero da quadrati. Allora:*

1. *per ogni naturale $N \geq 1$ esistono $u, v \in \mathbb{N} \setminus \{0\}$ tali che $\left|u - v\sqrt{d}\right| < \frac{1}{N} \leq \frac{1}{v}$;*
2. *esistono infiniti $u, v \in \mathbb{N}$ tali che $\left|u^2 - dv^2\right| < 1 + 2\sqrt{d}$.*

Dim. Per ogni numero reale a, indichiamo con $\langle a \rangle$ la sua parte frazionaria. Fissiamo N e scriviamo $[0,1[$ come unione degli N intervalli $[i/N, (i+1)/N[$ per $i = 0, \ldots, N-1$. Per il lemma dei cassetti esistono $r > s$ interi in $[0, N]$, ed $i \in \{0, 1, \ldots, N-1\}$, tali che $\langle r\sqrt{d} \rangle$, $\langle s\sqrt{d} \rangle$ appartengo all'intervallo $[i/N, (i+1)/N[$. Allora $0 < r - s \leq N$ e $\left|\langle r\sqrt{d} \rangle - \langle s\sqrt{d} \rangle\right| < \frac{1}{N}$. Poniamo $n = \lfloor r\sqrt{d} \rfloor$, $m = \lfloor s\sqrt{d} \rfloor$ ed osserviamo che $n > m$. Abbiamo quindi

$$\left|\langle s\sqrt{d} \rangle - \langle r\sqrt{d} \rangle\right| = \left|(s\sqrt{d} - m) - (r\sqrt{d} - n)\right| = \left|(n - m) - \sqrt{d}(r - s)\right|.$$

Posto $u = n - m$, $v = r - s$, otteniamo $u, v \in \mathbb{N}$ e $\left|u - v\sqrt{d}\right| < \frac{1}{N}$. Dato che $v = r - s \leq N$ si ha $\frac{1}{N} \leq \frac{1}{v}$, come richiesto.
Per il secondo punto scriviamo $u + v\sqrt{d} = u - v\sqrt{d} + 2v\sqrt{d}$ e, partendo da $\left|u - v\sqrt{d}\right| < \frac{1}{v}$, otteniamo

$$\left|u^2 - dv^2\right| = (u + v\sqrt{d})\left|u - v\sqrt{d}\right| \leq \frac{(u - v\sqrt{d})}{v} + 2\sqrt{d}$$

Vale la disuguaglianza $u - v\sqrt{d} \leq \left|u - v\sqrt{d}\right|$ e, essendo $v \geq 1$, anche

$$\frac{u - v\sqrt{d}}{v} \leq \frac{\left|u - v\sqrt{d}\right|}{v} \leq \left|u - v\sqrt{d}\right|.$$

Di conseguenza

$$\frac{u - v\sqrt{d}}{v} \leq \left|u - v\sqrt{d}\right| \leq \frac{1}{v} \leq 1$$

Si ottiene allora

$$\left|u^2 - dv^2\right| = (u + v\sqrt{d})\left|u - v\sqrt{d}\right| \leq \frac{(u - v\sqrt{d})}{v} + 2\sqrt{d} \leq 1 + 2\sqrt{d}$$

Per ogni $N \in \mathbb{N}$, sia (u_N, v_N) una coppia di naturali che soddisfano le proprietà 1 e 2. L'insieme $\{(u_N, v_N) \mid N \in \mathbb{N}\}$ è infinito. Infatti, se per assurdo questo insieme fosse finito, esisterebbero $u, v \in \mathbb{N}$, tali che $(u_N, v_N) = (u, v)$ per ogni $N \in I$, per un sottoinsieme infinito I di $\mathbb{N}$. Ma allora $\left|u - v\sqrt{d}\right| < \frac{1}{N}$ per ogni $N \in I$ e, dato che $\lim_{N \in I} \frac{1}{N} = 0$, si avrebbe $u = v\sqrt{d}$. Questo è impossibile perché u, v non sono 0 e $\sqrt{d}$ è irrazionale. □

Lemma 2 *Siano $d \in \mathbb{N}$ libero da quadrati e $k \in \mathbb{Z}$. Se $(x_1, y_1), (x_2, y_2) \in \mathbb{N}^2$ sono soluzioni distinte dell'equazione $x^2 - dy^2 = k$ e $x_1 \equiv x_2 \bmod k$, $y_1 \equiv y_2 \bmod k$, allora l'equazione diofantea $x^2 - dy^2 = 1$ ha soluzioni diverse da $(\pm 1, 0)$.*

Dim. Siano $a = x_1x_2 - dy_1y_2$, $b = x_1y_2 - x_2y_1$. Abbiamo $a = x_1x_2 - dy_1y_2 \equiv x_1x_1 - dy_1y_1 = (x_1)^2 - d(y_1)^2 = 0 \pmod k$ e $b = x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 = 0 \pmod k$. Allora $u = a/k$ e $v = b/k$ sono interi. Osserviamo inoltre che

$$k^2 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1 - y_1\sqrt{d})(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d})(x_2 + y_2\sqrt{d}) =$$
$$(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d})(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$$

Allora $(a/k)^2 - d(b/k)^2 = 1$ e la coppia (u, v) è una soluzione di $x^2 - dy^2 = 1$. Se $(u, v) = (\pm 1, 0)$, allora $b = 0$ e $a = \pm k$. Notiamo che almeno uno degli y_i è diverso da 0, altrimenti avremmo $x_i = \sqrt{k}$ e le due soluzioni $(x_1, y_1), (x_2, y_2)$ sarebbero uguali. Supponiamo $y_1 \neq 0$. Moltiplicando a per y_1, e ricordando che, se $b = 0$ allora $x_1y_2 = x_2y_1$, si ottiene

$$y_1a = x_1(y_1x_2) - dy_1{}^2y_2 = x_1(x_1y_2) - dy_1{}^2y_2 = y_2(x_1{}^2 - dy_1{}^2) = y_2k$$

Se $a = \pm k$ otteniamo $y_1 = \pm y_2$, da cui $y_1 = y_2$ dato che entrambi sono positivi. A questo punto, usando $b = 0$, si otterrebbe $x_1 = x_2$, una contraddizione. Pertanto $(u, v) \neq (\pm 1, 0)$. □

Teorema *Sia $d \in \mathbb{N}$ libero da quadrati. Allora l'equazione diofantea $x^2 - dy^2 = 1$ ha infinite soluzioni.*

Dim. Per il lemma 1 l'insieme $A = \{(u, v) \in \mathbb{Z}^2 \mid \left|u^2 - dv^2\right| \leq 1 + 2\sqrt{d}\}$ è infinito. Quindi esiste un intero $k \in [-(1 + 2\sqrt{d}), 1 + 2\sqrt{d}]$ tale che l'insieme $B = \{(u, v) \in A \mid u^2 - dv^2 = k\}$ è infinito. Consideriamo la funzione $\rho : B \longrightarrow \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ definita da $\rho(u, v) = (u + k\mathbb{Z}, v + k\mathbb{Z})$. Essendo B infinito la funzione ρ non è iniettiva. Esistono allora $(u_1, v_1), (u_2, v_2) \in B$, tali che $(u_1, v_1) \neq (u_2, v_2)$ ma $\rho(u_1, v_1) = \rho(u_2, v_2)$. Allora $u_1 \equiv u_2 \bmod k$, $v_1 \equiv v_2 \bmod k$, e, per il lemma 2, esiste una soluzione (u, v) per l'equazione diofantea $x^2 - dy^2 = 1$. Possiamo supporre $u, v > 0$. Scriviamo $u^2 - dv^2 = 1$ nella forma $(u + v\sqrt{d})(u - v\sqrt{d}) = 1$. Da questo otteniamo che, per ogni $n \in \mathbb{N}$, $(u + v\sqrt{d})^n(u - v\sqrt{d})^n = 1$. Poniamo $(u + v\sqrt{d})^n = u_n + v_n\sqrt{d}$. Di conseguenza $(u - v\sqrt{d})^n = u_n - v_n\sqrt{d}$ e $u_n^2 - v_n^2 = 1$. Ogni coppia del tipo (u_n, v_n) è quindi soluzione dell'equazione $x^2 - dy^2 = 1$. Avendo scelto $u, v > 0$, è facile verificare che, per ogni $n \geq 1$, si ha $u_n < u_{n+1}$ e $v_n < v_{n+1}$. Questo prova che l'equazione $x^2 - dy^2 = 1$ ha infinite soluzioni. □