5 La (così detta) equazione di Pell: $X^2 - dY^2 = 1$

Attorno al 1657, Fermat pose il seguente problema:

Dato comunque un intero positivo che non è un quadrato, mostrare che esistono infiniti numeri interi tali che se il quadrato di ognuno di essi è moltiplicato per il numero assegnato e se 1 *viene aggiunto al risultato, allora ciò che si ottiene è ancora il quadrato di un numero intero.*

In simboli, ciò si può tradurre semplicemente nella seguente maniera: *dato un intero positivo d, che non sia un quadrato, mostrare che esistono infinite soluzioni intere per l'equazione diofantea*:

$$X^2 - dY^2 = 1 \ . \tag{5.1}$$

Osservazione 5.1. (a) Come osservato da Brouncker e Wallis attorno al 1660, si vede agevolmente che l'equazione (5.1) possiede infinite soluzioni razionali. Infatti, ponendo $X = 1 + (m/n)Y$, con $m, n \in \mathbb{Z}$, $n \geq 0$, si ha infatti la seguente equazione quadratica in una indeterminata:

$$1 + \left(\frac{m}{n}\right)^2 Y^2 + 2\frac{m}{n}Y - dY^2 = 1 \ .$$

Pertanto una soluzione di tale equazione è data da $y = 0$ (e quindi $x = 1$); l'altra soluzione (al variare di m ed n) è data da:

$$y = 2mn/(n^2d - m^2)$$

e quindi: $x = (n^2d + m^2)/(n^2d - m^2)$.

(b) A causa dell'estrema parsimonia di informazioni sulla propria attività matematica, non sembrano essere chiaramente note le motivazioni che avrebbero portato Fermat allo studio di un tale problema. Probabilmente, Fermat fu stimolato dalla lettura della *Arithmetica Infinitorum* di J. Wallis suo contemporaneo. È evidente però che tale questione non sia stata posta "a caso". Ad esempio, l'equazione (5.1) è di importanza fondamentale per il problema generale della risoluzione di una qualunque equazione diofantea quadratica in due variabili. Infatti, si può dimostrare che tutte le equazioni diofantee di secondo grado in due variabili possono essere "ricondotte" allo studio di una equazione del tipo (5.1), (cfr. anche l'Esercizio 5.8).

Si noti, inoltre, che riferimenti a casi specifici dell'equazione di Pell si incontrano sovente nella matematica classica: ad esempio, il cosiddetto "problema del bestiame" di Archimede (III sec. a.C.). Questo è un problema con otto incognite (relative a tipi differenti di capi di bestiame) che soddisfano sette relazioni lineari e due condizioni che assicurano che alcuni numeri sono quadrati perfetti. Tramite tecniche di eliminazione di indeterminate, questo problema veniva ricondotto alla risoluzione di un'equazione diofantea del tipo $X^2 - 4729494 \cdot Y^2 = 1$.

(c) J. Wallis, come osservato in (a), fu tra i primi a dare un metodo per determinare delle soluzioni al problema di Fermat sopra enunciato, per valori assegnati di d, senza però dimostrare, in generale, che tale metodo potesse permettere di determinare tutte le soluzioni. Questa "parte rimanente" del problema è certamente di particolare difficoltà, in quanto lo stesso Euler, pur provandoci, non pervenne ad una conclusione definitiva.

Lagrange nel 1766 dette la prima dimostrazione completa del Teorema di Fermat enunciato all'inizio del presente paragrafo. Questo problema è, oggi, comunemente noto come "problema della risoluzione dell'equazione di Pell" (dal nome di un matematico inglese contemporaneo del Wallis). Ciò è dovuto molto probabilmente al fatto che Euler, nel 1730, (quando cioè aveva appena 23 anni) aveva avuto l'errata impressione, leggendo l'opera del Wallis, che questi attribuisse a Pell l'idea del metodo di risoluzione dell'equazione diofantea $X^2 - dY^2 = 1$. Il nome di "equazione di Pell" è poi restato ad indicare l'equazione (5.1), benché Pell non si sia mai occupato effettivamente di tale equazione. (Per maggiori informazioni storiche e bibliografiche sull'argomento, cfr. I.E. Dickson [4, vol. II, Ch. XII] ed anche il volume di E. Whitford [17] dedicato a tale argomento.)

Prima di passare a descrivere le tecniche che ci porteranno alla risoluzione dell'equazione (5.1), vogliamo giustificare la presenza dell'ipotesi fatta su d, e cioè che d non sia un quadrato (di un intero). Infatti, se $d = a^2$, con $a \in \mathbb{Z}$, $a \neq 0$, allora:

$$1 = X^2 - dY^2 = (X - aY)(X + aY)$$

ovvero: $X - aY = \pm 1$ e $X + aY = \pm 1$; ciò equivale a dire che l'equazione diofantea (5.1) ammette solamente le soluzioni banali $x = \pm 1$ e $y = 0$. Più generalmente, possiamo supporre che d sia un intero privo di fattori quadratici. Infatti, se fosse $d = a^2 d'$ con $a, d' \in \mathbb{Z}$ e d' privo di fattori quadratici, allora si avrebbe che (x_0, y_0) è una soluzione di $X^2 - dY^2 = 1$ se, e soltanto se, (x_0, ay_0) è una soluzione di $X^2 - d'Y^2 = 1$.

Infine, ovviamente, si suppone $d > 0$, poiché, se fosse $d < 0$, allora si avrebbe $x^2 - dy^2 \geq 0$ presi comunque $x, y \in \mathbb{Z}$, e dunque $x^2 - dy^2 = 1$, se, e soltanto se, $x = \pm 1$ e $y = 0$ ed anche, nel caso in cui $d = -1$, $x = 0$ e

$y = \pm 1$. Quindi, per $d < 0$, l'equazione di Pell avrebbe soltanto soluzioni banali.

Procediamo, ora, alla dimostrazione dell'esistenza di infinite soluzioni dell'equazione diofantea di Pell $X^2 - dY^2 = 1$, quando d è *un intero positivo che non possiede fattori quadratici (interi).*

Lemma 5.2. *Presi, comunque, $x_1, y_1, x_2, y_2, d \in \mathbb{Z}$, vale la seguente identità:*

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 \mp dy_1y_2)^2 - d(x_1y_2 \mp y_1x_2)^2 \ ,$$

(dove la scelta dei segni a secondo membro deve essere concorde).

Dimostrazione. La verifica è diretta.

□

Corollario 5.3. *Se (x_1, y_1), (x_2, y_2) sono due soluzioni dell'equazione di Pell, allora anche le seguenti coppie:*

$$(x_3 := x_1x_2 - dy_1y_2,\ y_3 := x_1y_2 - y_1x_2)\ ,\ (x_4 := x_1x_2 + dy_1y_2,\ y_4 := x_1y_2 + y_1x_2)$$

sono soluzioni dell'equazione di Pell.

□

Lemma 5.4. *Sia $\alpha \in \mathbb{R}$ e sia N un intero positivo. Allora, esistono due interi p e q tali che $1 \leq q \leq N$ e*

$$|\alpha - p/q| \leq 1/qN \ .$$

Dimostrazione. La prova di questo lemma, che ci fornisce una "approssimazione razionale" conveniente per un qualunque numero reale (non razionale), è basata sul cosiddetto Principio di Dirichlet (cfr. il Paragrafo 3 di questo Capitolo). Sia $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Si considerino i seguenti $N+1$ numeri reali

$$k\alpha - [k\alpha] \ , \quad 0 \leq k \leq N \, ,$$

compresi tra 0 e 1. Si divida l'intervallo reale $[0, 1]$ in N sub–intervallini uguali di ampiezza esattamente $\frac{1}{N}$ e cioè:

$$\left[\frac{h}{N}, \frac{h+1}{N}\right] , \quad 0 \leq h \leq N-1 \, .$$

Allora, per il Principio di Dirichlet, almeno due tra i numeri reali $k\alpha - [k\alpha]$ appartengono allo stesso intervallino, cioè esistono $n, m \in \mathbb{Z}$ con $0 \leq n < m \leq N$ tali che, se $q := m - n$ e $p := [m\alpha] - [n\alpha]$,

$$|q\alpha - p| \leq \frac{1}{N} \; .$$

$\square$

Corollario 5.5. *Sia* $\alpha \in \mathbb{R}$. *Esistono infinite coppie di interi* (p, q) *con* $q \geq 1$ *tali che:*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2} \; .$$

Dimostrazione. Possiamo supporre che α sia irrazionale (cioè, $\alpha \in \mathbb{R} \setminus \mathbb{Q}$), altrimenti l'affermazione è banalmente soddisfatta. Ponendo $N := N_1 := 1$, per il Lemma 5.4 possiamo affermare che esistono $p_1, q_1 \in \mathbb{Z}$ (con $q_1 = 1$) tali che:

$$\left|\alpha - \frac{p_1}{q_1}\right| \leq \frac{1}{q_1 N_1} = \frac{1}{q_1^2} \; .$$

Poiché α è irrazionale, si ha che $|q_1\alpha - p_1| \neq 0$; pertanto si può trovare $1 \lneqq N_2$ tale che

$$\frac{1}{N_2} < |q_1\alpha - p_1| \; .$$

Per il Lemma 5.4, applicato al caso $N := N_2$, possiamo affermare che esistono q_2, $1 \leq q_2 \leq N_2$, e $p_2 \in \mathbb{Z}$ tali che:

$$\left|\alpha - \frac{p_2}{q_2}\right| \leq \frac{1}{q_2 N_2} \leq \frac{1}{q_2^2} \; .$$

Dunque, abbiamo:

$$|q_2\alpha - p_2| \leq 1/N_2 < |q_1\alpha - p_1| \, ,$$

quindi $(p_2, q_2) \neq (p_1, q_1)$. Il procedimento precedente si può iterare essendo $|q_2\alpha - p_2| \neq 0$.

$\square$

Lemma 5.6. *Sia $B := 2\sqrt{d} + 1$, con d intero positivo privo di fattori quadratici. Allora, esistono infinite coppie di interi (x, y) tali che:*

$$|x^2 - dy^2| \leq B \ .$$

Dimostrazione. Per il Corollario 5.5, esistono infinite coppie di interi x, y con $y \geq 1$ tali che:

$$\left| \sqrt{d} - \frac{x}{y} \right| \leq \frac{1}{y^2} \ ,$$

da cui si ricava che:

$$|\sqrt{d}y - x| \leq \frac{1}{y} \ ,$$

ed anche che:

$$\left| \frac{x}{y} \right| \leq \sqrt{d} + \frac{1}{y^2} \leq \sqrt{d} + 1 \ .$$

Pertanto:

$$\begin{aligned} |x^2 - dy^2| &= |\sqrt{d}y + x| \cdot |\sqrt{d}y - x| \leq \left| \frac{\sqrt{d}y + x}{y} \right| = \left| \sqrt{d} + \frac{x}{y} \right| \leq \\ &\leq \sqrt{d} + \left| \frac{x}{y} \right| \leq \sqrt{d} + \sqrt{d} + 1 = B \ . \end{aligned}$$

□

Teorema 5.7. *Sia d un intero positivo privo di fattori quadratici. Allora, l'equazione di Pell:*

$$X^2 - dY^2 = 1 \tag{5.1}$$

ha infinite soluzioni distinte.

Dimostrazione. Per il Lemma 5.6, ci sono infinite coppie di interi (x, y) tali che $|x^2 - dy^2| \leq B = 2\sqrt{d} + 1$. Poiché $x^2 - dy^2$ è un intero e poiché ci sono solo un numero finito di interi k tali che $0 \leq |k| \leq B$, allora esiste un intero k_0, $-B \leq k_0 \leq B$, in corrispondenza del quale esistono infinite coppie di interi (x, y) tali che $x^2 - dy^2 = k_0$. Si noti che $k_0 \neq 0$ (altrimenti d sarebbe un quadrato perfetto).
Esaminiamo l'insieme delle soluzioni (x, y) dell'equazione diofantea $X^2 - dY^2 = k_0$ e consideriamole modulo $|k_0|$. Evidentemente ci sono solo k_0^2 coppie (a, b) tali che $x \equiv a \pmod{|k_0|}$, $y \equiv b \pmod{|k_0|}$ e $0 \leq a, b < |k_0|$, al variare di (x, y).

Poiché l'equazione $X^2 - dY^2 = k_0$ ammette infinite soluzioni, debbono esistere allora due interi a, b, con $0 \leq a,\, b < |k_0|$, in modo tale che le soluzioni (x, y) di $X^2 - dY^2 = k_0$ soddisfacenti simultaneamente anche il sistema di congruenze:

$$\begin{cases} X \equiv a \pmod{|k_0|} \\ Y \equiv b \pmod{|k_0|} \end{cases}$$

siano infinite. Presa comunque una coppia di tali soluzioni, siano esse (x_1, y_1) e (x_2, y_2) con $(x_1, y_1) \neq (x_2, y_2)$, allora:

$$\begin{aligned} &x_1^2 - dy_1^2 = k_0 = x_2^2 - dy_2^2\,, \\ &x_1 \equiv a \equiv x_2 \pmod{|k_0|}\,, \\ &y_1 \equiv b \equiv y_2 \pmod{|k_0|}\,, \end{aligned}$$

Usando, ora, l'identità del Lemma 5.2, si ha:

$$k_0^2 = (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - y_1x_2)^2 \ .$$

Inoltre,

$$\begin{aligned} &x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 = k_0 \equiv 0 \pmod{|k_0|}\,, \\ &x_1y_2 - y_1x_2 \equiv x_1y_1 - y_1x_1 = 0 \pmod{|k_0|}\,. \end{aligned}$$

Perciò:

$$1 = \left(\frac{x_1x_2 - dy_1y_2}{k_0}\right)^2 - d\left(\frac{x_1y_2 - y_1x_2}{k_0}\right)^2$$

e quindi la coppia:

$$\left(x_3 := \frac{x_1x_2 - dy_1y_2}{k_0}\ ,\ y_3 := \frac{x_1y_2 - y_1x_2}{k_0}\right)$$

è una soluzione dell'equazione di Pell. Ora, se fissiamo (x_1, y_1) (si noti che $k_0 \neq 0$, e che x_1 e y_1 non sono entrambi nulli) e facciamo variare (x_2, y_2), dal momento che x_2 o y_2 possono assumere infiniti valori distinti, abbiamo trovato infinite soluzioni distinte (descritte dalla coppia (x_3, y_3)) per l'equazione di Pell.

$\square$

Lemma 5.8. *Siano $x_1, y_1, x_2, y_2, d \in \mathbb{Z}$. Allora, valgono le seguenti identità:*

$$\begin{aligned} (x_1 + \sqrt{d}y_1)(x_2 + \sqrt{d}y_2) &= (x_1x_2 + dy_1y_2) + \sqrt{d}(x_1y_2 + y_1x_2)\,, \\ (x_1 + \sqrt{d}y_1)(x_2 - \sqrt{d}y_2) &= (x_1x_2 + dy_1y_2) - \sqrt{d}(x_1y_2 + y_1x_2)\,. \end{aligned}$$

Dimostrazione. La verifica è banale.

□

Corollario 5.9. *Siano* $x_1, y_1, d, n \in \mathbb{Z}$, $n \geq 1$. *Allora:*

$$(x_1 + \sqrt{d}y_1)^n = x_n + \sqrt{d}y_n \,,$$
$$(x_1 - \sqrt{d}y_1)^n = x_n - \sqrt{d}y_n \,,$$

con $x_n := x_1 x_{n-1} + dy_1 y_{n-1}$ *e* $y_n := x_1 y_{n-1} + y_1 x_{n-1}$, *per* $n \geq 2$.

Dimostrazione. Basta ragionare per induzione su n, ed applicare il Lemma 5.8.

□

Lemma 5.10. *Sia* $n \geq 1$ *e sia* (x_1, y_1) *una soluzione dell'equazione di Pell. Allora, se definiamo (come nel Corollario 5.9.)* x_n *e* y_n *tramite la relazione*

$$(x_1 + \sqrt{d}y_1)^n = x_n + \sqrt{d}y_n$$

allora anche (x_n, y_n) *è una soluzione dell'equazione di Pell.*

Dimostrazione.

$$\begin{aligned} x_n^2 - dy_n^2 &= (x_n + \sqrt{d}y_n)(x_n - \sqrt{d}y_n) = (x_1 + \sqrt{d}y_1)^n (x_1 - \sqrt{d}y_1)^n = \\ &= ((x_1 + \sqrt{d}y_1)(x_1 - \sqrt{d}y_1))^n = (x_1^2 - dy_1^2)^n = 1 \,. \end{aligned}$$

□

Osservazione 5.11. Sia (x_1, y_1) una soluzione dell'equazione di Pell. Essendo

$$(x_1 + \sqrt{d}y_1)^n (x_1 - \sqrt{d}y_1)^n = (x_1^2 - dy_1^2)^n = 1 \,,$$

allora, per ogni $n \geq 1$, si ha che l'inverso di $(x_1 + \sqrt{d}y_1)^n$ è dato da:

$$(x_1 + \sqrt{d}y_1)^{-n} = (x_1 - \sqrt{d}y_1)^n = x_n - \sqrt{d}y_n \,.$$

Si noti, anche, che per per ogni $n \geq 1$,

$$x_n + \sqrt{d}y_n = (x_n - \sqrt{d}y_n)^{-1} \,.$$

Osserviamo che se (x, y) è una soluzione dell'equazione di Pell, allora anche $(\pm x, \pm y)$ è una soluzione, per ogni possibile scelta di segno; quindi, basta determinare tutte le soluzioni di (5.1) per le quali $x \geq 0$ ed $y \geq 0$. È evidente poi che le soluzioni per le quali x o y è zero sono solo $(\pm 1, 0)$; quindi, in definitiva, basta determinare tutte le soluzioni per le quali $x > 0$ e $y > 0$. Tali soluzioni sono chiamate *soluzioni positive dell'equazione di Pell.*

Proposizione 5.12. *Sia (x, y) una soluzione dell'equazione di Pell. Allora, (x, y) è una soluzione positiva se, e soltanto se, $x + \sqrt{d}y > 1$.*

Dimostrazione. È chiaro che, se $x \geq 1$ e $y \geq 1$, allora $x + \sqrt{d}y \geq 1 + \sqrt{d} \geq 2 > 1$.

Viceversa, supponiamo che $x+\sqrt{d}y > 1$; quindi $(x, y) \neq (\pm 1, 0)$. Esaminiamo le varie possibilità:

Caso 1: Se $x < 0$ e $y < 0$, allora anche $x + \sqrt{d}y < 0$, donde un assurdo.

Caso 2: Se $x > 0$ e $y < 0$, allora $x - \sqrt{d}y \geq 1 + \sqrt{d} \gneqq 1$, quindi $1 = x^2 - dy^2 = (x + \sqrt{d}y)(x - \sqrt{d}y)$ è assurdo.

Caso 3: Se $x < 0$ e $y > 0$, allora $-x + y\sqrt{d} > 1$, quindi $-1 = -x^2 + dy^2 = (-x + \sqrt{d}y)(x + \sqrt{d}y)$ è assurdo.

Caso 4: Il caso $x > 0$ e $y > 0$ è pertanto l'unico caso possibile affinché risulti $x + \sqrt{d}y > 1$.

$\square$

Definizione 5.13. La soluzione positiva (x_1, y_1) della equazione (5.1) per la quale $x_1 + \sqrt{d}y_1$ è minimo è detta *soluzione fondamentale dell'equazione di Pell.*

Si noti che la definizione sopra data è ben posta. Sia infatti (x_0, y_0) una soluzione positiva dell'equazione di Pell, che sappiamo esistere (Teorema 5.7). Per la Proposizione 5.12, $M := x_0+\sqrt{d}y_0 > 1$. Se (x, y) è una qualunque altra soluzione positiva tale che $x + \sqrt{d}y \leq M$, allora $x \leq M$ e $y \leq M$. Pertanto, ci sono soltanto un numero finito di scelte intere (positive) per x e y. Quindi, è possibile trovare soltanto un numero finito di numeri reali del tipo $1 < x + \sqrt{d}y \leq M$.

Teorema 5.14. *Sia $d > 0$, d privo di fattori quadratici. Sia (x_1, y_1) la soluzione fondamentale dell'equazione di Pell:*

$$X^2 - dY^2 = 1 \tag{5.1}$$

e sia (x_n, y_n)*,* $n \geq 1$*, tale che* $(x_1 + \sqrt{d}y_1)^n = x_n + \sqrt{d}y_n$ *(Corollario 5.9). Allora, tutte e sole le soluzioni dell'equazione di Pell sono date da:*

$$(\pm 1, 0) \quad \text{e} \quad (\pm x_n, \pm y_n)\,, \qquad n \geq 1\,,$$

dove tutte le possibilità di scelta per i segni sono ammesse. Inoltre, tutte queste soluzioni sono distinte tra loro.

Dimostrazione. Già sappiamo che $(\pm x_n, \pm y_n)$ e $(\pm 1, 0)$ sono soluzioni dell'equazione di Pell. Inoltre, $x_1 > 0$ e $y_1 > 0$ implica che $x_n > 0$ e $y_n > 0$; pertanto ogni soluzione del tipo $(\pm x_n, \pm y_n)$ è distinta dalle soluzioni $(\pm 1, 0)$. Per mostrare che le soluzioni $(\pm x_n, \pm y_n)$ sono tutte distinte, basta provare che $(x_n, y_n) \neq (x_m, y_m)$ per $n \neq m$. Supponiamo, per assurdo, che $(x_n, y_n) = (x_m, y_m)$ con $n \lneqq m$; allora dalla uguaglianza:

$$(x_1 + \sqrt{d}y_1)^n = x_n + \sqrt{d}y_n = x_m + \sqrt{d}y_m = (x_1 + \sqrt{d}y_1)^m$$

segue che $(x_1 + \sqrt{d}y_1)^{m-n} = 1$ con $m - n > 0$. Ciò è assurdo, poiché, essendo (x_{m-n}, y_{m-n}) una soluzione positiva dell'equazione di Pell, per la Proposizione 5.12 si ha che $(x_1 + \sqrt{d}y_1)^{m-n} \gneqq 1$.

Mostriamo, ora, che ogni altra soluzione (u, v) dell'equazione di Pell deve coincidere con una delle soluzioni sopra descritte. Possiamo limitarci ovviamente a supporre che $u \gneqq 0$ e $v \gneqq 0$. Per come si è scelta la soluzione fondamentale si ha che:

$$x_1 + \sqrt{d}y_1 \leq u + \sqrt{d}v\ .$$

Affermiamo che esiste un intero $n > 0$ tale che

$$(x_1 + \sqrt{d}y_1)^n \leq u + \sqrt{d}v \lneqq (x_1 + \sqrt{d}y_1)^{n+1}\ .$$

Infatti, essendo $x_1 + \sqrt{d}y_1 > 1$, il numero reale $(x_1 + \sqrt{d}y_1)^k$ cresce al crescere di k; basta quindi considerare il più grande intero positivo n tale che $(x_1 + \sqrt{d}y_1)^n \leq u + \sqrt{d}v$. Moltiplicando la disuguaglianza precedente per $(x_1 - \sqrt{d}y_1)^n$ e tenendo conto che $x_1 - \sqrt{d}y_1 > 0$, in quanto $x_1 + \sqrt{d}y_1 > 1$ e $(x_1 + \sqrt{d}y_1)(x_1 - \sqrt{d}y_1) = 1$, si ottiene:

$$1 \leq (u + \sqrt{d}v)(x_1 - \sqrt{d}y_1)^n < x_1 + \sqrt{d}y_1\ .$$

Se poniamo $u_1 := ux_n - dvy_n$ e $v_1 := vx_n - y_nu$, allora

$$1 \leq u_1 + \sqrt{d}v_1 < x_1 + \sqrt{d}y_1\ .$$

D'altra parte, si verifica subito che

$$u_1^2 - dv_1^2 = (u^2 - dv^2)(x_n^2 - dy_n^2) = 1 \cdot 1 = 1 \ ,$$

cioè, che (u_1, v_1) è una soluzione dell'equazione di Pell. Quindi, essendo (x_1, y_1) la soluzione fondamentale, si ha che $u_1 + \sqrt{d}v_1 = 1$. Quindi,

$$(u + \sqrt{d}v)(x_1 - \sqrt{d}y_1)^n = 1 \, ,$$

da cui si ricava che:

$$u + \sqrt{d}v = x_n + \sqrt{d}y_n \ .$$

Pertanto, $u = x_n$ e $v = y_n$.

□

Osservazione 5.15. Si può dimostrare agevolmente che le soluzioni della equazione di Pell formano un gruppo rispetto alla "composizione" definita utilizzando le identità del Lemma 5.8 (cfr. anche Lemma 5.2, Corollario 5.9 ed Osservazione 5.10).
Inoltre, se $\mathbf{Sol}(d) := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x^2 - dy^2 = 1\}$ è l'insieme di tutte le soluzioni dell'equazione di Pell, allora l'applicazione canonica:

$$\varphi : \mathbf{Sol}(d) \longrightarrow \mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} \ , \quad (x, y) \mapsto x + y\sqrt{d}$$

definisce un isomorfismo canonico tra $\mathbf{Sol}(d)$ ed il gruppo moltiplicativo $\mathrm{Im}(\varphi)$ (sottogruppo del gruppo moltiplicativo degli elementi non nulli di $\mathbb{Z}[\sqrt{d}]$) il quale è un gruppo moltiplicativo ciclico infinito generato da $\varepsilon_1 := x_1 + \sqrt{d}y_1$, dove (x_1, y_1) è la soluzione fondamentale dell'equazione di Pell (cfr. anche l'Esercizio 5.2).

5.17. Algoritmo elementare per determinare la soluzione fondamentale dell'equazione di Pell

Il Teorema precedente permette di trovare tutte le soluzioni dell'equazione di Pell non appena ne sia nota una non banale. Infatti, da una soluzione non banale è possibile, con un numero finito di passi, determinare la soluzione fondamentale. Un metodo (algoritmico elementare) per trovare effettivamente la soluzione fondamentale dell'equazione di Pell è il seguente:

Fissato d (intero positivo che non possiede fattori quadratici), si consideri la successione di interi positivi:

$$\{1 + dk^2 : k \geq 1\} \, .$$

Sia y_1 il più piccolo intero positivo tale che $1 + dy_1^2$ sia il quadrato di un intero positivo x_1. Allora (x_1, y_1) è la soluzione fondamentale dell'equazione di Pell.

Infatti, se (x, y) è una soluzione positiva dell'equazione di Pell, allora (per la scelta di y_1) $y \geq y_1$ e, quindi, $x = \sqrt{1 + dy^2} \geq \sqrt{1 + dy_1^2} = x_1$, da cui si ricava che $x + \sqrt{d}y \geq x_1 + \sqrt{d}y_1$.

Osservazione 5.16. Si noti che, in alcuni casi, cioè per valori particolari di d, è facile determinare la soluzione fondamentale (x_1, y_1) dall'equazione di Pell.

(i) Se $d = a^2 - 1$, con a intero ed $a > 1$, allora:

$$(x_1, y_1) = (a, 1) \ .$$

Infatti, $1 + k^2(a^2 - 1) = k^2a^2$ che è un quadrato per $k = 1$. Dunque $y_1 = 1$ e $x_1 = a$.

(ii) Se $d = a(a + 1)$, con a intero positivo, allora:

$$(x_1, y_1) = (2a + 1, 2) \ .$$

Infatti, è evidente che $(2a+1, 2)$ è una soluzione positiva dell'equazione di Pell. Inoltre, se esistesse una soluzione del tipo $(x, 1)$, cioè con $y = 1$, allora si avrebbe $x^2 = dy^2 + 1 = d + 1 = a^2 + a + 1 > a^2$, cioè $x > a$, ovvero $x \geq a+1$ e, quindi, $x^2 \geq a^2+2a+1 > a^2+a+1 = x^2$, donde un assurdo. Quindi, ogni altra soluzione positiva (x, y) deve avere $y \geq 2$ e, quindi, $x \geq 2a + 1$.

Segnaliamo anche che è possibile dimostrare, anche se ciò è meno semplice, che:

(iii) Se $d = a^2 + 1$, con a intero positivo, allora:

$$(x_1, y_1) = (2a^2 + 1, 2a) \ .$$

(iv) Se $d = a^2 + 2$, con a intero positivo, allora:

$$(x_1, y_1) = (a^2 + 1, a) \ .$$

Terminiamo il paragrafo mostrando come le soluzioni dell'equazione diofantea di Pell forniscono un metodo di approssimazione dei numeri reali che sono radici quadrate di interi positivi. Tale metodo fornisce un semplice esempio di uno strumento particolarmente importante per lo studio delle equazioni diofantee, quale è quello della *teoria delle approssimazioni diofantee.* Questa è una branca tecnica e specializzata della teoria dei numeri che ha avuto inizio verso la metà del XVIII secolo con il tentativo di risoluzione numerica delle equazioni diofantee, osservando la rapidità di convergenza di valori approssimati delle radici.

Proposizione 5.17. (L. Euler, 1759) *Se (x, y) è una soluzione positiva della equazione di Pell* (5.1)*, allora il numero razionale x/y approssima il numero reale $\sqrt{d}$ con un'accuratezza superiore all'inverso del quadrato del denominatore, cioè:*

$$x/y - \sqrt{d} < 1/y^2 \ .$$

Dimostrazione. $1 = x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$ da cui:

$$(x - y\sqrt{d})/y = 1/[y(x + y\sqrt{d})] < 1/y^2\sqrt{d} < 1/y^2 \ .$$

□

Segnaliamo infine che, facendo uso della teoria delle "frazioni continue", si può dare un metodo effettivo, sistematico e generale per la risoluzione dell'equazione diofantea di Pell. Tale metodo, risalente a Wallis e Brouncker, consiste essenzialmente nel produrre approssimazioni razionali vieppiú precise di $\sqrt{d}$. Per maggiori dettagli rinviamo al volume di Allenby e Redfern [1, Section 11.6] oppure a quello di Hardy e Wright [6, p. 129–153 e p. 210]; cfr. anche Davenport [3, Ch. 4, Par. 11], Olds [10].

Osservazione 5.18. L'equazione lineare e l'equazione quadratica di Pell godono di una particolare proprietà tra le equazioni diofantee in due indeterminate: esse sono essenzialmente le uniche equazioni diofantee in due indeterminate che ammettono infinite soluzioni intere o quasi–intere (cioè, razionali con denominatore fissato). Questo fatto è una delle conseguenze della introduzione di metodi della geometria algebrica in aritmetica.

Precisamente, a partire dall'inizio del 1900 con i lavori di H. Poincaré la teoria delle equazioni diofantee si è sviluppata in modo più sistematico ed organico interpretando "geometricamente" problematiche di origine aritmetica. Le equazioni polinomiali in due indeterminate a coefficienti in $\mathbb{Z}(\subset \mathbb{Q})$, da un punto di vista geometrico, definiscono delle curve algebriche nel piano. Pertanto, le equazioni diofantee di tale tipo possono essere classificate utilizzando un invariante geometrico: il "genere" g delle curve algebriche associate.

Le curve di genere $g = 0$ possono essere ricondotte (tramite trasformazioni birazionali) a rette o a coniche (cfr. anche l'Esercizio 5.8). Le equazioni di tali curve hanno, in generale, infinite soluzioni intere e, quindi, le curve hanno infiniti punti a coordinate razionali.

Le curve di genere $g = 1$ sono le "curve ellittiche", che possono essere ricondotte ad un'equazione cubica standard. Mordell nel 1922 ha dimostrato che un'equazione diofantea la cui curva associata ha genere 1 ha soltanto un numero finito di soluzioni in $\mathbb{Z}$, ma può avere infinite soluzioni razionali, "generate" però da un numero finito tra esse.

Mordell ha poi congetturato che ogni curva algebrica di genere $g > 1$ può avere soltanto un numero finito di punti razionali. Tale congettura è stata dimostrata da G. Faltings nel 1983, con un lavoro che gli è valso la Medaglia Fields.

5 Esercizi e complementi

5.1. Mostrare che la soluzione fondamentale dell'equazione di Pell è data da:

$$\begin{array}{ll} (3,2), & \text{se } d=2\,; \\ (2,1), & \text{se } d=3\,; \\ (9,4), & \text{se } d=5\,; \\ (5,2), & \text{se } d=6\,; \\ (8,3), & \text{se } d=7\,; \\ (3,1), & \text{se } d=8\,; \\ (19,6), & \text{se } d=10\,; \\ (10,3), & \text{se } d=11\,; \\ (7,2), & \text{se } d=12\,. \end{array}$$

Per $d = 13$, la soluzione fondamentale è data da $(649, 180)$ e per $d = 61$, poi, la soluzione fondamentale è data da $(1766319049, 226153980)$ e risulta ovviamente non "agevole" il suo calcolo, procedendo con il metodo elementare precedentemente descritto.

[*Suggerimento*. Utilizzare il semplice algoritmo descritto in 5.15]

5.2. Sia d un intero positivo che non è un quadrato. Supponiamo che l'equazione diofantea:

$$X^2 - dY^2 = -1 \tag{5.2.1}$$

ammetta almeno una soluzione. (Si osservi che in generale un'equazione del tipo (5.2.1) non è risolubile: ad esempio $X^2 - 3Y^2 = -1$ non è risolubile perché non è risolubile la congruenza $x^2 \equiv -1 \pmod 3$). Allora:

(a) Esiste sempre una soluzione positiva (u_1, v_1) di (5.2.1) per la quale $\gamma_1 := u_1 + v_1\sqrt{d} > 1$ è minimo. Tale soluzione è detta *soluzione fondamentale.*

(b) Siano (w_1, z_1) e (w_2, z_2) due soluzioni di (5.2.1). Siano $\alpha_1 := w_1 + z_1\sqrt{d}$ e $\alpha_2 := w_2 + z_2\sqrt{d}$. Verificare che $\alpha_1\alpha_2 = (w_1w_2 + dz_1z_2) + (w_1z_2 + w_2z_1)\sqrt{d}$ e che $(w_3 := w_1w_2 + dz_1z_2,\ z_3 := w_1z_2 + w_2z_1)$ è una soluzione dell'equazione di Pell (5.1).

(c) Se $\varepsilon_1 = \gamma_1^2 = u_2 + v_2\sqrt{d}$, allora (u_2, v_2) è la soluzione fondamentale della equazione di Pell (5.1), cioè tutte le soluzioni non banali di (5.1) sono date da $(\pm u_{2n}, \pm v_{2n})$ per $n \geq 1$, dove $\gamma_{2n} := \varepsilon_1^n =: u_{2n} + v_{2n}\sqrt{d}$, e per ogni scelta possibile del segno.

(d) Tutte e sole le soluzioni di (5.2.1) sono date da $(\pm u_{2n+1}, \pm v_{2n+1})$ con $n \geq 0$ e per ogni possibile scelta del segno.

[*Suggerimento*. Sia (u, v) una soluzione di (5.2.1) e sia $\gamma := u + \sqrt{d}v$.

(a) Come nel caso dell'equazione di Pell, $u > 0$ e $v > 0$ equivale a $\gamma > 1$. Il ragionamento che segue la Definizione 5.13. si può applicare pure in questo caso, per cui è possibile trovare una soluzione positiva (u_1, v_1) di (5.2.1), in modo tale che $\gamma_1 := u_1 + \sqrt{d}v_1 > 1$ sia minimo.

(b) È conseguenza del Lemma 5.2.

(c) Per definizione della soluzione fondamentale ε_1 dell'equazione di Pell (5.1) (Definizione 5.13) e per il fatto che γ_1^2 è anch'essa soluzione di (5.1), si ha:

$$1 < \varepsilon_1 \leq \gamma_1^2 \ .$$

Se poniamo $\overline{\gamma}_1 := u_1 - \sqrt{d}v_1$, allora $\gamma_1\overline{\gamma}_1 = -1$, dunque:

$$-\overline{\gamma}_1 < -\overline{\gamma}_1\varepsilon_1 \leq \gamma_1 \ .$$

È subito visto che, se scriviamo $-\overline{\gamma}_1\varepsilon_1 = a+\sqrt{d}b$ (rispettivamente, $\gamma_1\varepsilon_1 = a'+\sqrt{d}b'$), allora (a, b) (rispettivamente, (a', b')) è una soluzione di (5.2.1). Dunque

$$-\overline{\gamma}_1 < -\overline{\gamma}_1\varepsilon_1 < 1 \quad \text{oppure} \quad 1 < -\overline{\gamma}_1\varepsilon_1 \leq \gamma_1 \ .$$

La prima eventualità è esclusa perché essa è equivalente a

$$1 < \gamma_1\varepsilon_1 < \gamma_1 \, ,$$

che è esclusa per la proprietà di minimalità di γ_1 tra le soluzioni positive di (5.2.1). Pertanto, $1 < -\overline{\gamma}_1\varepsilon_1 \leq \gamma_1$ e quindi $-\overline{\gamma}_1\varepsilon_1 = \gamma_1$ (sempre per la minimalità di γ_1), cioè $\varepsilon_1 = \gamma_1^2$.

(d) Se (a, b) è una soluzione positiva di (5.2.1) e se $\delta := a + \sqrt{d}b$, allora si può trovare un intero positivo $n \geq 1$ tale che

$$1 \leq \delta\gamma_1^{-n} < \gamma_1 = \varepsilon_1^2 \, ,$$

dunque

$$\varepsilon_1^{-1} \leq \delta\varepsilon_1^{-1}\gamma_1^{-n} < \varepsilon_1 \ .$$

Dove scrivendo $\delta\varepsilon_1^{-1}\gamma_1^{-n} = x + \sqrt{d}y$ si ha che (x, y) è una soluzione dell'equazione di Pell (5.1).

D'altro lato $1 < \varepsilon_1 < \gamma_1 = \varepsilon_1^2$, quindi $1 > \varepsilon_1^{-1} > \gamma_1^{-1}$, pertanto:

$$\gamma_1^{-1} \leq \delta\varepsilon_1^{-1}\gamma_1^{-n} < \gamma_1$$

da cui si ricava che $\delta\varepsilon_1^{-1}\gamma_1^{-n} = 1$ cioè $\delta = \varepsilon_1^{2n+1}$.]

5.3. Mostrare che l'equazione (5.2.1) *non* è risolubile se $d = p$ è un numero primo, con $p \equiv 3 \pmod 4$.

[*Suggerimento*. Se (5.2.1) è risolubile, allora la congruenza $X^2 \equiv -1 \pmod p$ è risolubile].

5.4. Sia d un intero positivo che non è un quadrato. Si consideri l'equazione diofantea:

$$X^2 - dY^2 = 4 \; . \tag{5.4.1}$$

(a) Mostrare che (5.4.1) è sempre risolubile, provando che se (x', y') è una soluzione dell'equazione di Pell (5.1), allora $(2x', 2y')$ è una soluzione di (5.4.1).

(b) Mostrare che *non* ogni soluzione di (5.4.1) è del tipo descritto in (a) (ad esempio: $(3, 1)$ per $d = 5$).

(c) Mostrare che esiste sempre una soluzione positiva minima di (5.4.1) (ξ_1, η_1) (cioè tale che $\zeta_1 := \xi_1 + \sqrt{d}\eta_1$ è minimo positivo), detta *soluzione fondamentale* di (5.4.1).

(d) Provare che tutte e sole le soluzioni non banali (a, b) di (5.4.1) sono tali che, se $\alpha := a + b\sqrt{d}$, allora

$$(\star_n) \qquad \frac{\alpha}{2} = \pm \left(\frac{\zeta_1}{2}\right)^n \qquad \text{per qualche } n \geq 1 \; .$$

Viceversa se α verifica $(\star_n)$ per un qualche n, allora (a, b) è una soluzione di (5.4.1).

[*Suggerimento*. (a) si verifica in modo diretto.

(b) $3^2 - 5 \cdot 1^2 = 4$, però $3 + \sqrt{5} \neq 2x' + 2y'\sqrt{5}$ presi comunque $x', y' \in \mathbb{Z}$.

(c) Si noti che se (x, y) è una soluzione di (5.4.1), allora x e y sono entrambi pari oppure entrambi dispari. Pertanto, possiamo scrivere $x + y\sqrt{d} \equiv a(1 + \sqrt{d}) \pmod 2$, con $a = 0$ oppure $a = 1$. Diremo che (x, y) è una *soluzione dispari* se $a = 1$. Si noti che, se esiste una soluzione dispari di (5.4.1), allora necessariamente d deve essere dispari. In ogni caso, se $\alpha := x + y\sqrt{d}$ e $\beta := x' + y'\sqrt{d} \equiv b(1 + \sqrt{d}) \pmod 2$ sono due soluzioni di (5.4.1), allora $\alpha\beta \equiv ab(d + 1 + 2\sqrt{d}) \equiv 0 \pmod 2$, perché se $ab = 1$ allora d è dispari e quindi $d + 1$ è pari. In ogni caso, per ogni coppia di soluzioni (x, y), (x', y') di (5.4.1), si ha:

$$\frac{\alpha\beta}{2} = 2 \cdot \frac{\alpha}{2} \cdot \frac{\beta}{2} = u + v\sqrt{d} \quad \text{con } u, v \in \mathbb{Z} \quad \text{e} \quad u^2 - v^2 d = 4 \; .$$

Da questa osservazione discende la prima parte di (c).]

La seconda affermazione di (c) e (d) si dimostrano con un ragionamento analogo a quello del Teorema 5.14.

5.5. Sia d un intero positivo che non è un quadrato. Si consideri l'equazione diofantea:

$$X^2 - dY^2 = -4 \; . \tag{5.5.1}$$

(a) Mostrare che (5.5.1) non è sempre risolubile.

Se (5.5.1) è risolubile, allora mostrare che:

(b) Esiste una soluzione positiva minima (μ_1, ν_1) di (5.5.1) (cioè, tale che $\lambda_1 := \mu_1 + \sqrt{d}\nu_1$ è minimo positivo) detta *soluzione fondamentale*.

(c) Se $\zeta_1 := \xi_1 + \sqrt{d}\eta_1$, dove (ξ_1, η_1) è la soluzione fondamentale di (5.4.1), allora mostrare che:

$$\frac{\zeta_1}{2} = \left(\frac{\lambda_1}{2}\right)^2 .$$

(d) Siano $a, b \in \mathbb{Z}$ e sia $\alpha := a + \sqrt{d}b$. Mostrare che:

$$\frac{\alpha}{2} = \pm\frac{\lambda_1}{2}\left(\frac{\zeta_1}{2}\right)^n , \quad \text{con } n \in \mathbb{Z},$$

se e soltanto se (a, b) è una soluzione di (5.5.1).

[*Suggerimento*. Le dimostrazioni delle affermazioni sopra enunciate sono simili a quelle dell'Esercizio 5.2.]

5.6. Sia d un intero positivo che non è un quadrato. Si consideri l'equazione diofantea:

$$X^2 - dY^2 = n , \quad \text{con } n > 0 . \tag{5.6.1}$$

(a) Mostrare che (5.6.1) non è sempre risolubile.

(b) Mostrare che se (5.6.1) è risolubile, allora essa ammette infinite soluzioni. Più precisamente, mostrare se (a, b) è una soluzione di (5.6.1) e se $(\pm x_k, \pm y_k)$ è una soluzione dell'equazione di Pell (5.1), allora $(\pm a x_k \pm dby_k, \pm a y_k \pm bx_k)$, con una appropriata evidente scelta dei segni, è ancora una soluzione di (5.6.1). L'insieme costituito da tali soluzioni con $k \geq 1$ e da (a, b) è detto *classe di soluzioni* individuata da (a, b).

(c) Mostrare che l'equazione $X^2 - 2Y^2 = 49$ ammette come soluzioni $(7, 0)$ e $(9, 4)$ e che tali soluzioni individuano classi di soluzioni disgiunte.

Osservazione. Si può dimostrare che se (5.6.1) è risolubile allora, nella classe individuata da una qualunque soluzione, esiste una soluzione (a, b) tale che

$$\sqrt{n} < a \leq \sqrt{\Delta n} \quad \text{dove } \Delta := \frac{1}{2}\left(1 + \frac{x_1 + \sqrt{d}y_1}{(x_1 - 1) + y_1\sqrt{d}} x_1\right)$$

essendo (x_1, y_1) la soluzione fondamentale dell'equazione di Pell (5.1). Pertanto, da ciò si ricava facilmente che (5.6.1) ammette soltanto un numero finito di classi distinte di soluzioni. Per maggiori dettagli cfr. ad esempio LeVeque [8, Theorem 8.9].

[*Suggerimento*. (a) Ad esempio, se $d = 3$ ed $n = 2$ l'equazione diofantea $X^2 - 3Y^2 = 2$ non è risolubile, altrimenti sarebbe risolubile la congruenza $X^2 \equiv 2 \pmod 3$.

(b) Discende facilmente dal Lemma 5.2.

(c) Si noti che la soluzione fondamentale dell'equazione di Pell $X^2 - 2Y^2 = 1$ è data da $(3, 2)$. Allora, basta osservare che, se $\varepsilon_1 := 3 + 2\sqrt{2}$, si ha:

$$7 = (7 + 0\sqrt{2}) \neq (9 + 4\sqrt{2})\varepsilon_1^k , \quad \text{per ogni } k \geq 1. \text{]}$$

5.7. Nella stessa situazione dell'Esercizio 5.6, si consideri l'equazione diofantea:

$$X^2 - dY^2 = -n \ . \tag{5.7.1}$$

Mostrare che, *mutatis–mutandis*, valgono ancora gli enunciati (a), (b), (c) ed un enunciato "analogo" a quello dell'Osservazione dell'Esercizio 5.6. Più precisamente, nell'enunciato dell'"analogo" di quello dell'Osservazione precedente, si deve porre la disuguaglianza:

$$\sqrt{n} < a < \sqrt{\Delta' n} \ , \quad \text{dove } \Delta' := \frac{(x_1 + y_1\sqrt{d})x_1}{2(x_1 + 1 + y_1\sqrt{d})} \ .$$

[*Suggerimento*. Per (a) si vedano anche gli Esercizi 5.2 e 5.5 e per (b) l'Esercizio 5.6 (b). (c) Si noti che se (x, y) è una soluzione (5.7.1) e (u, v) è una soluzione di (5.2.1) allora, per il Lemma 5.2, $(xy \mp dyv, xv \mp yu)$ sono ancora soluzioni di (5.7.1). Si concluda ragionando in modo analogo a quello dell'Esercizio 5.6 (c), osservando che la soluzione fondamentale dell'equazione diofantea $X^2 - 2Y^2 = -1$ è determinata $\gamma_1 := 1 + \sqrt{2}$, cioè è data da $(1, 1)$ (e quindi, come è noto, $\gamma_1^2 = \varepsilon_1 = 3 + 2\sqrt{2}$ determina la soluzione fondamentale dell'Equazione di Pell $X^2 - 2Y^2 = 1$).]

5.8. Sia

$$aX^2 + bXY + cY^2 + dX + eY + f = 0 \tag{5.8.1}$$

la generale equazione diofantea quadratica in due indeterminate (a coefficienti in $\mathbb{Z}$). Mostrare che il calcolo delle soluzioni di tale equazione può essere ricondotto al calcolo delle soluzioni di una equazione di Pell, nelle indeterminate U e V, del tipo:

$$U^2 - sV^2 = t \,,$$

dove $s := 4(b^2 - 4ac)$, $t := (2bd - 4ac)^2 - 4(b^2 - 4ac)(d^2 - af)$.

[*Suggerimento*. Si osservi che un'equazione quadratica:

$$AX^2 + BX + C = 0$$

con $A, B, C \in \mathbb{Q}$, $A \neq 0$ ha soluzioni in $\mathbb{Q}$ se, e soltanto se, $B^2 - 4AC = D^2$, per un qualche $D \in \mathbb{Q}$. Si noti, poi, che se $A, B, C \in \mathbb{Z}$, allora tale equazione ha soluzioni intere se, e soltanto se, $2A \mid (-B \pm D)$.

Si consideri ora la generale equazione quadratica a coefficienti in $\mathbb{Z}$ in due indeterminate (5.8.1). Ponendo $Y = y_0$ per un qualche $y_0 \in \mathbb{Z}$, l'equazione (5.8.1) nella sola indeterminata X, ha soluzioni razionali se, e soltanto se,

$$(by_0 + d)^2 - 4a(cy_0^2 + ey_0 + f) = (b^2 - 4c)y_0^2 + (2bd - 4ae)y_0 + d^2 - 4af = v^2$$

per un qualche $v \in \mathbb{Q}$, (si noti che dopo la sostituzione si ha: $A := a$, $B := by_0 + d$, $C := cy_0^2 + ey_0 + f$).

Lasciamo al Lettore il compito di esprimere esplicitamente, in questo caso, quando tali soluzioni sono intere.
Poniamo $p := b^2 - 4ac$ e supponiamo $p \neq 0$ (per evitare casi banali), $q := 2bd - 4ae$ e $r := d^2 - 4af$. Allora, l'equazione nell'indeterminata Y a coefficienti interi:

$$pY^2 + qY + (r - v^2) = 0$$

ha soluzioni razionali se, e soltanto se,

$$q^2 - 4p(r - v^2) = u^2 \,, \quad \text{per un qualche } u \in \mathbb{Q} \,.$$

Anche in questo caso, lasciamo al Lettore il compito di esprimere quando tali soluzioni sono intere.
Dunque, ci siamo ricondotti a considerare l'equazione di Pell in due indeterminate U e V del tipo:

$$U^2 - 4pV^2 = q^2 - 4pr \,.$$

Quindi, in definitiva, il saper risolvere tale equazione diofantea di Pell permette di saper risolvere l'equazione diofantea generale quadratica in due incognite (5.8.1).]

References

[1] R.B.J.T. Allenby, E.J. Redfern, *Introduction to Number Theory with Computing*, Arnold, 1989.

[2] E.T. Bell, "The Last Theorem", *MAA*, 1990.

[3] H. Davenport, *Aritmetica Superiore. Una introduzione alla Teoria dei Numeri*, Zanichelli, 1994.

[4] I.E. Dickson, *History of the theory of numbers*, (3 voll. 1920–1923) Ristampa Chelsea, New York 1974.

[5] H.M. Edwards, *Fermat's Last Theorem*, Springer, 1996 (new updated edition).

[6] G.H. Hardy, E.M. Wright, *An introduction to the theory of numbers*, Oxford 1954.

[7] E. Landau, *Elementary Number Theory*, Chelsea, New York 1958 (traduzione inglese di Vorlesungen über Zahlentheorie, vol. I, 1927).

[8] W.J. LeVeque, *Fundamentals of Numbers Theory*, Addison–Wesley, 1977.

[9] L.J. Mordell, *Diophantine equations*, Academic Press, 1969.

[10] C.D. Olds, *Continued fractions*, Random House, 1963.

[11] P. Ribenboim, *Fermat's Last Theorem for amateurs*, Springer, 1999

[12] H.E. Rose, *A course in number theory*, Oxford Science Pu., 1988.

[13] W. Sierpiński, *Elementary Theory of Numbers*, North–Holland 1988.

[14] S. Singh, *L'Ultimo Teorema di Fermat*, Rizzoli, 1997.

[15] A. van der Porten, *Notes on Fermat's Last Theorem*, Wiley, 1996.

[16] A. Weil, *Number Theory. An Approach through history*, Birkhäuser, 1984.

[17] E. Whitford, *The Pell's Equation*, New York 1912.