Capitolo 4

L'esponenziazione in 13 incognite

Given a polynomial P, we shall construct another polynomial $\overline{P}$ such that

$$P(\, a_1, \ldots, a_\mu,\, z_0, \ldots, z_\nu\,) \quad = \quad 0$$

for some $z_0, \ldots, z_\nu$ if and only if

$$\overline{P}(\, a_1, \ldots, a_\mu,\, b, c, d, e, f, g, h, i, j, k, l, m, n\,) \quad = \quad 0$$

for some $b, c, d, e, f, g, h, i, j, k, l, m, n$.

$$[\cdots]$$

Now a diophantine equation $F(\, a,\, u_1, \ldots, u_\nu\,) = 0$ has a solution for $u_1, \ldots, u_\nu$ if and only if

$$(u_0 + 1)\,\big(1 - F^2(\, u_0, \ldots, u_\nu\,)\big) - 1 \quad = \quad a$$

has a solution for $u_0, \ldots, u_\nu$ (see Putnam [9]). Thus, our theorem shows that *every diophantine set is the non-negative part of the range on* $\mathbb{N}$ *of a polynomial with 14 variables.* (Da [MR75, pagg. 521, 522])

N.B.: Le proposizioni che seguono e la loro applicazione—a partire dalla § 4.2—provengono da [MR75]; però impiego la stessa notazione utilizzata nell'appendice sull'equazione di Pell. In particolare, indico con $\langle\, \boldsymbol{y}_0(\mathfrak{a})\,,\, \boldsymbol{y}_1(\mathfrak{a})\,,\, \boldsymbol{y}_2(\mathfrak{a})\,, \ldots \rangle$ la successione infinita dei valori risolutivi per l'incognita y nell'equazione $(\mathfrak{a}^2 - 1)\, y + 1 = \square$, disposti in ordine crescente.

4.1 Teorema preparatorio

Richiamo qui da [MR75, pagg. 524–527], senza approfondirne la dimostrazione, il *Relation-combining Theorem*:

Teorema 9 (Combinazione di relazioni diofantee)**.** *C'è per ogni* $q \in \mathbb{N}$ *un polinomio* M_q *a coefficienti* interi *tale che, comunque presi* $A_1, \ldots, A_q, B, C, D$ *in* $\mathbb{Z}$ *con* $B \neq 0$*, le condizioni*

$$\bigwedge_{i=1}^{q} A_i = \square\,, \qquad B \mid C\,, \qquad D > 0$$

valgono tutte assieme se e solo se è risolubile l'equazione

$$M_q(\,A_1\,,\ldots,\,A_q\,,\,B\,,\,C\,,\,D\,,\,x\,) \;=\; 0$$

nell'incognita naturale x*.*

(Intendere $B \mid C$ come: $C = \pm h\,B$ per qualche $h \in \mathbb{N}$). ⊣

Esempio 109. *Nel caso* $q = 0$*, possiamo prendere*

$$M_0(\,B\,,\,C\,,\,D\,,\,x\,) \;=_{Def}\; B^2\,x + C^2 - B^2\,(2\,D-1)\,(C^2+1)\;.$$

⊣

Esempio 110. *Nel caso* $q = 1$*, possiamo prendere*

$$M_1(\,A\,,\,B\,,\,C\,,\,D\,,\,x\,) \;=_{Def}\; \left(B^2\,x + C^2 - B^2\,(2\,D-1)\,(C^2+1+A^2)\right)^2 - B^4\,(2D-1)^2\,A\,.$$

⊣

Esempio 111. *Nel caso* $q = 2$*, possiamo prendere*

$$\begin{aligned} M_2(\,A_1\,,\,A_2\,,\,B\,,\,C\,,\,D\,,\,x\,) \;=_{Def}\; & \left(\left[B^2\,x + C^2 - B^2\,(\,2\,D-1\,)\,\left(C^2 + \left(1 + A_1^2 + A_2^2\right)^2\right)\right]^2 + \right. \\ & \left. B^4\,(\,2\,D-1\,)^2\left(A_1 - A_2\,\left(1 + A_1^2 + A_2^2\right)^2\right)\right)^2 - \\ & 4\,B^4\,(\,2\,D-1\,)^2\,A_1\left[B^2\,x + C^2 - B^2\,(\,2\,D-1\,)\,\left(C^2 + \left(1 + A_1^2 + A_2^2\right)^2\right)\right]^2\,. \end{aligned}$$

⊣

Nei tre esempi che precedono, come pure oltre $q = 2$, l'idea è di porre

$$\begin{aligned} W \;&=_{\text{Def}}\; 1 \;+\; \textstyle\sum_{i=1}^{q} A_i^2\,, \\ M_q \;&=_{\text{Def}}\; \textstyle\prod_{\sigma \in \{-1,1\}^{\{1,\ldots,q\}}} \\ &\left(B^2\,x + C^2 - B^2\,(\,2\,D-1\,)\,\left(C^2 + W^q + \textstyle\sum_{j=1}^{q} \sigma(j)\sqrt{A_j}\,W^{j-1}\right)\right)\;; \end{aligned}$$

allora, grazie alla produttoria, risulta non necessario estrarre radici quadrate ed M_q può venir riscritto come un polinomio a coefficienti in $\mathbb{Z}$.

Esercizio 112. *Posto*

$$J_q(A_1, \ldots, A_q, X) \quad =_{Def} \quad \prod_{\sigma \in \{0,1\}^{\{1,\ldots,q\}}} \left(X + \sum_{j=1}^{q} (-1)^{\sigma(j)} \sqrt{A_j}\, W^{j-1} \right) ,$$

ove

$$W \quad =_{Def} \quad 1 \; + \; \sum_{i=1}^{q} A_i^2$$

(la produttoria, è chiaro, si riferisce a tutte le possibili scelte sui segni negli addendi $X \pm \sqrt{A_1} \pm \sqrt{A_2}\, W \pm \cdots \pm \sqrt{A_q}\, W^{q-1}$), *mostrare che* J_q *è esprimibile come polinomio a coefficienti in* $\mathbb{Z}$*, per ogni* q*.*

4.2 Utilizzo nella specifica diofantea di $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$

Poniamo

$$\mathsf{pell}(a, u) \quad =_{\mathrm{Def}} \quad (a^2 - 1)\, u^2 + 1 \ ,$$

dimodoché l'equazione di Pell di forma particolare di cui ci siamo occupati altrove si possa condensare cosí:

$$x^2 \quad = \quad \mathsf{pell}(\mathfrak{a}, y) \ .$$

In [MR75, pag. 532] viene proposto un sistema di equazioni diofantee che è sostanzialmente quello in Fig. 4.1, nei parametri $m, \mathfrak{a}, \mathfrak{n}, y$ <u>su $\mathbb{N}$</u> e nelle incognite (facilmente eliminabili) X, E, U, G, H, I <u>su $\mathbb{Z}$</u>, oltre che in due incognite i, j <u>su $\mathbb{N}$</u>, qui designate anonimamente con '$': *in virtú del Teor. 9, questo sistema non conta 5 variabili anonime ma solo* 3.

$$\begin{array}{|lrcl|}
\hline
1) & X & = & \mathsf{pell}\big(\mathfrak{a},\ y\big) \\
2) & E & = & 2\, X\, y^2\, (m+1)\, (\$ + 1) \\
3) & U & = & \mathsf{pell}\big(\mathfrak{a},\ E\big) \\
4) & G & = & U\, (U - \mathfrak{a}) + \mathfrak{a} \\
5) & H & = & \mathfrak{n} + 2\, y\, \$ \\
6) & I & = & \mathsf{pell}\big(G,\ H\big) \\
\hline
0) & \left\{ \begin{array}{rcl} X\, U\, I & = & \square \\ U & \mid & H - y \\ \mathfrak{n} & \leqslant & y \end{array} \right. & \\
\hline
\end{array}$$

Figura 4.1: Specifica diofantea della relazione $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a}) \wedge m = m$.

Teorema 10. *Fra le quaterne* $m, \mathfrak{a}, \mathfrak{n}, y$ *su* $\mathbb{N}$ *tali che*

$$\mathfrak{a} > 1 \,, \qquad \mathfrak{n} > 0 \,, \qquad y > 0 \ ,$$

quelle per cui il sistema di Fig. 4.1 è risolubile sono le stesse per cui vale $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$*. (Inoltre la 2) e la 3) ci forniscono la coprimalità* $m + 1 \perp U$*).* ⊣

Dimostrazione. Da $V = \mathsf{pell}\big(a,\, u\big)$, i.e. $V = (a+1)\,(a-1)\,u^2 + 1$ discende in generale, per ogni $a \geqslant 1$, che $V \geqslant 1$ e che se $a > 1$ ed $u > 0$ allora $V > a + 1$. Pertanto dalle $\mathfrak{a} > 1$, $\mathfrak{n} > 0$ ed $y > 0$ e dalle 1)–6) discende che

$$X > 0\,,\;\; E > 0\,,\;\; U > \mathfrak{a}\,,\;\; G > \mathfrak{a},\;\; H > 0\,,\;\; I > 0\,.$$

Grazie alla 0), otterremo che X, U ed I sono quadrati perfetti semplicemente verificando che sono numeri coprimi. In effetti abbiamo che

$$E \equiv 0\,,\;\; U \equiv 1\,,\;\; G \equiv 1\,,\;\; I \equiv 1 \pmod{X}$$

per la 2), la 3), la 4) (da cui $G = U^2 + \mathfrak{a}\,(1-U)$), e la 6) rispettivamente. Inoltre

$$G \equiv \mathfrak{a}\,,\;\; H \equiv y\,,\;\; I \equiv X \pmod{U},$$

le prime due per la 4) e la 0), la terza come conseguenza delle altre due, della 6) e della 1). Dalle $U \equiv 1 \pmod{X}$ ed $I \equiv 1 \pmod{X}$ conseguono $U \perp X$ ed $I \perp X$; dalle $I \equiv X \pmod{U}$ ed $U \perp X$ consegue $I \perp U$: il primo obiettivo è cosí raggiunto.

Essendo a questo punto stabilito che $X = \square$, $U = \square$ ed $I = \square$, le 1), 3), 6) implicano l'esistenza di p, q, r (ovviamente positivi) tali che

$$\begin{aligned} y &= \boldsymbol{y}_p(\mathfrak{a})\,, \qquad X &= \boldsymbol{x}_p^2(\mathfrak{a})\,, \\ E &= \boldsymbol{y}_q(\mathfrak{a})\,, \qquad U &= \boldsymbol{x}_q^2(\mathfrak{a})\,, \\ H &= \boldsymbol{y}_r(G)\,, \qquad I &= \boldsymbol{x}_r^2(G)\,. \end{aligned}$$

Ci basterà dimostrare che $p = \mathfrak{n}$ onde poter concludere che $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$—in effetti, G è stata scelta in modo che $\boldsymbol{y}_r(G)$ potesse far da tramite fra r e $\mathfrak{n}$ da un lato e fra r e p dall'altro, sí che ne discenda $p = \mathfrak{n}$.

Abbiamo in primo luogo $G \equiv 1 \pmod{2\,y}$ per le 2), 3), 4) e dunque

$$H \;=\; \boldsymbol{y}_r(G) \;\equiv\; r \pmod{2\,y}\;,$$

grazie alla regola di congruenza secondo cui $g \equiv h \pmod{m}$ implica che $\boldsymbol{y}_n(g) \equiv \boldsymbol{y}_n(h) \pmod{m}$ per $g > 0$, $h > 0$, $m > 0$ ed $n \geqslant 0$. Perciò, alla luce della 5),

$$r \;\equiv\; \mathfrak{n} \pmod{2\,y}\;.$$

In secondo luogo $G \equiv \mathfrak{a} \pmod{U}$, per la 4), cosicché—grazie alla stessa regola di congruenza di poco fa—

$$H \;=\; \boldsymbol{y}_r(G) \;\equiv\; \boldsymbol{y}_r(\mathfrak{a}) \pmod{U}\;;$$

inoltre

$$H \;\equiv\; y \pmod{U}$$

per la 0). Quindi

$$\boldsymbol{y}_r(\mathfrak{a}) \;\equiv\; \boldsymbol{y}_p(\mathfrak{a}) \pmod{\boldsymbol{x}_q(\mathfrak{a})}\;,$$

dato che $y = \boldsymbol{y}_p(\mathfrak{a})$ ed $U = \boldsymbol{x}_q^2(\mathfrak{a})$. Osserviamo poi che $y^2 \mid \boldsymbol{y}_q(\mathfrak{a})$ per la 2) e che, pertanto, $y \mid q$: ciò in virtú della regola (chiamata *first step-down lemma*)

secondo cui $\boldsymbol{y}_k^2(\mathfrak{a}) \mid \boldsymbol{y}_\ell(\mathfrak{a})$ implica $\boldsymbol{y}_k(\mathfrak{a}) \mid \ell$, per ogni k e ogni ℓ. Un'altra regola (chiamata *second step-down lemma*) ci dice che per ogni $n > 0$, ogni j ed ogni i, se $\boldsymbol{y}_j(\mathfrak{a}) \equiv \boldsymbol{y}_i(\mathfrak{a})$ (**mod** $\boldsymbol{x}_n(\mathfrak{a})$) allora $j \equiv i$ (**mod** $2\,n$) oppure $j \equiv -i$ (**mod** $2\,n$); cosí, dato che $q > 0$, otteniamo che $r \equiv p$ (**mod** $2\,q$) oppure $r \equiv -p$ (**mod** $2\,q$) e dunque che

$$r \;\equiv\; p \pmod{2\,y} \qquad \text{oppure} \qquad r \;\equiv\; -p \pmod{2\,y}\ .$$

Mettendo insieme, abbiamo che

$$\mathfrak{n} \;\equiv\; p \pmod{2\,y} \qquad \text{oppure} \qquad \mathfrak{n} \;\equiv\; -p \pmod{2\,y}\ .$$

Inoltre $\mathfrak{n} \leqslant y$ per la 0) e $p \leqslant \boldsymbol{y}_p(\mathfrak{a}) = y$; pertanto $\mathfrak{n} = p$, donde la conclusione attesa $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$.

La verifica dell'implicazione inversa, che quando $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$ allora sono determinabili per le incognite X, E, U, G, H, I, i, j valori in $\mathbb{N}$ tali da soddisfare il sistema 0)–6) viene lasciata al lettore come Esercizio 114. ⊣

Esercizio 113. *Dimostrare che in ogni soluzione delle prime sei equazioni della Fig. 4.1 nei parametri $m \geqslant 0$, $\mathfrak{a} > 1$, $\mathfrak{n} > 0$ ed $y > 0$ si ha che $X > \mathfrak{a} + 1$, $E > 7$, $U > 64\,(\mathfrak{a}+1)$, $G > 4032\,\mathfrak{a}^2 + 8256\,\mathfrak{a} + 4224$, $H > \mathfrak{n}$ ed $I > \mathfrak{n}^2\,(4032\,\mathfrak{a}^2 + 8256\,\mathfrak{a} + 4224)^2$.*

Esercizio 114. *Mostrare che il sistema in Fig. 4.1 ha infinite soluzioni per ogni m in $\mathbb{N}$, quando $\mathfrak{a} > 1$, $\mathfrak{n} > 0$ ed $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$.*

Corollario 11. *C'è un polinomio Z tale che se $\mathfrak{a} > 1$, $\mathfrak{n} > 0$ ed $y > 0$, allora $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$ vale se e solo se vi sono i, j, k tali che $Z(\mathfrak{a}, \mathfrak{n}, y, i, j, k) = 0$.* ⊣

Dimostrazione. Richiamando il Teor. 9 (v. anche Esempio 110) e il fatto che $U > 0$, si ottenga Z come

$$M_1(X\,U\,I,\ U,\ H - y,\ y - \mathfrak{n} + 1,\ k)\,,$$

ponendo $m = 0$ ed eliminando X, U, H, I in base alle equazioni della Fig. 4.1. ⊣

4.3 Specifica diofantea polinomiale di $b^{\mathfrak{n}} = c$

Consideriamo ora il sistema di Fig. 4.2, che risulta da quello di Fig. 4.1 per sostituzione di 0 ad m e per eliminazione delle incognite X, E, G, I. Si tratta di un sistema, riscrivibile come singola equazione diofantea polinomiale

$$R(\mathfrak{a}, \mathfrak{n}, y, U, H, z_1, z_2, z_3) \;=\; 0\ ,$$

nei tre parametri $\mathfrak{a}, \mathfrak{n}, y$ e in 5 incognite, di cui 3 anonime.[1]

Per quanto visto sopra, l'equazione parametrica

$$R(\mathfrak{a}, \mathfrak{n}, y, \dots) \;=\; 0$$

[1] Decidessimo di eliminare U ed H, due anonime cesserebbero di essere tali.

$$
\begin{array}{rcl}
U & = & \mathsf{pell}\Big(\mathfrak{a},\ 2\,(\$+1)\,y^2\,\mathsf{pell}\big(\mathfrak{a},\ y\big)\Big) \\
H & = & \mathfrak{n}+2\,y\,\$ \\
\Box & = & U\ \mathsf{pell}\big(\mathfrak{a},\ y\big)\ \mathsf{pell}\big(U\,(U-\mathfrak{a})+\mathfrak{a},\ H\big) \\
U & \mid & H-y \\
\mathfrak{n} & \leqslant & y
\end{array}
$$

Figura 4.2: Specifica diofantea ridotta della relazione $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$.

ha soluzione su $\mathbb{N}$, per una terna $\mathfrak{a}, \mathfrak{n}, y$ tale che $\mathfrak{a} > 1$, $\mathfrak{n} > 0$ ed $y > 0$, se e solo se $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$. Pertanto l'equazione

$$(y+\mathfrak{n})\,\Big(\big(1-R(\mathfrak{a},\mathfrak{n},y,\dots)\big)\,y\,\mathfrak{n}-1-\$\Big) \quad = \quad 0$$

ha soluzione su $\mathbb{N}$, per una terna $\mathfrak{a}, \mathfrak{n}, y$ tale che $\mathfrak{a} > 1$, se e solo se $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$. (Alle incognite di poco fa se n'è aggiunta una nuova, anonima).

Indicata questa equazione come $D_0(\mathfrak{n}, y, \mathfrak{a}, U, H, z_1, z_2, z_3, z_4)$, estendiamo poi $D_0(\mathfrak{n}, k, t, \dots)$ in una nuova specifica diofantea polinomiale

$$D(b, \mathfrak{n}, c)$$

'declassando' k e t a variabili e aggiungendo queste nuove condizioni:

Equazione:			Senso:
h^2	$=$	$\mathsf{pell}(t,\ k)$	$h = \boldsymbol{x}_{\mathfrak{n}}(t)$
$(h-k\,(t-b)-c)^2$	$=$	$(2tb-b^2-1)^2\,\$^2$	$c \equiv h-k\,(t-b)\ (\mathbf{mod}\ 2tb-b^2-1)$
$c+\$$	$=$	$2tb-b^2-1$	$c \leqslant 2tb-b^2-1$
$b+\$ \quad = \quad q$	$=$	$\mathfrak{n}+\$$	$q \geqslant b \wedge q \geqslant \mathfrak{n}$
$t^2-q^3\,(q+2)\,(\$+1)^2$	$=$	1	$t = \boldsymbol{x}_\ell(q+1) \wedge q \mid \boldsymbol{y}_\ell(q+1)$

Ora le incognite sono h, k, t, q, U, H, piú 9 anonime. È facile eliminare la q cambiando una delle variabili anonime in 'variabile-canale'; anche U, H sono eliminabili (v. Esercizio 117). È dimostrabile che:

Teorema 12. *Il sistema $D(b, \mathfrak{n}, c)$ in 12 incognite ha soluzione, per $b > 0$, se e solo se $b^{\mathfrak{n}} = c$.* ⊣

Di qui discende poi l'importante

Corollario 13 (Teorema di Matiyasevich)**.** *Il predicato $b^{\mathfrak{n}} = c$ è diofanteo.* ⊣

Una specifica dell'esponenziazione si ottiene semplicemente assemblando

$$\Big(\big(b-z_0-1\big)^2+Q(b,\mathfrak{n},c,z_1,\dots,z_{12})\Big)\Big(\big(c-1\big)^2+b+\mathfrak{n}\Big)\Big(c+b+\big(\mathfrak{n}-z_0-1\big)^2\Big) \quad = \quad 0$$

a partire dal polinomio

$$Q(b, \mathfrak{n}, c, z_1, \ldots, z_{12})$$

che risulta dalla somma dei quadrati delle equazioni di D, per tener conto della definizione

$$0^0 \;=\; 1 \qquad \text{e} \qquad 0^{\mathfrak{n}} \;=\; 0 \quad \text{per} \quad \mathfrak{n} \;\neq\; 0\,.$$

Esercizio 115. *Dimostrare che—come piú su asserito—l'equazione*

$$(y+\mathfrak{n})\,\Big(\big(1-R(\mathfrak{a},\mathfrak{n},y,\ldots)\big)\,y\,\mathfrak{n}-1-\$\Big) \;=\; 0$$

ha soluzione su $\mathbb{N}$*, per una terna* $\mathfrak{a},\mathfrak{n},y$ *tale che* $\mathfrak{a}>1$*, se e solo se* $y=\boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$*.*

Esercizio 116. *Che gradi hanno* R*,* D_0*,* D*,* Q *e la specifica polinomiale dell'esponenziazione fornita qui sopra?*

Esercizio 117. *Si sarebbe potuto, nel passare dal sistema di Fig. 4.1 a quello di Fig. 4.2, eliminare le incognite* U *ed* H*, cosí come sono state eliminate le incognite* X, E, G, I*? Quante incognite e quante tra di esse anonime sarebbero rimaste?*

4.4 Risoluzione degli esercizi

Soluzione Es. 112. Poniamo

$$I_q(A_1,\ldots,A_q,X,Y) \quad =_{\text{Def}} \quad \textstyle\prod_{\sigma\in\{0,1\}^{\{1,\ldots,q\}}}\Big(X+\sum_{j=1}^{q}(-1)^{\sigma(j)}\sqrt{A_j}\,Y^{j-1}\Big)\;;$$

cosí, tenuto conto che $J_q(A_1,\ldots,A_q,X)=I_q(A_1,\ldots,A_q,X,1+\sum_{i=1}^{q}A_i^q)$, ci basta mostrare che $I_q\in\mathbb{Z}[A_1,\ldots,A_q,X,Y]$. Avendo convenuto all'inizio della § 4.1 che identificatori quali A_i, X ed Y (qui variabili) si riferissero ad interi, ci basta individuare una riscrittura algebrica di I_q in cui non occorra il simbolo $\sqrt{\ }$. In effetti abbiamo, induttivamente, che

$$\begin{aligned} I_0(X,Y) &= X\,,\\ I_{q+1}(A_1,\ldots,A_{q+1},X,Y) &= \big(I_q(A_1,\ldots,A_q,X,Y)+\sqrt{A_{q+1}}\,Y^q\big)\cdot\\ &\quad\ \big(I_q(A_1,\ldots,A_q,X,Y)-\sqrt{A_{q+1}}\,Y^q\big)\\ &= I_q^2(A_1,\ldots,A_{q+1},X,Y)-A_{q+1}\,Y^{2\,q}\,. \end{aligned}$$

⊣

Soluzione Es. 113. Dato che $\mathfrak{a}>1$, $y>0$ ed $\mathfrak{n}>0$, le specifiche di H e di X ci danno che $H>\mathfrak{n}$ e che $X=(\mathfrak{a}+1)\,(\mathfrak{a}-1)\,y^2+1>\mathfrak{a}+1$, cosicché $X\geqslant 4$ ed $E>7$; dunque, tenendo di nuovo conto della $\mathfrak{a}>1$, dalla $U=\mathsf{pell}\big(\mathfrak{a},\,E\big)=(\mathfrak{a}+1)\,(\mathfrak{a}-1)\,E^2+1$ ricaviamo $U>64\,(\mathfrak{a}+1)$, donde $G\geqslant(64\cdot 63)\,\mathfrak{a}^2+(65\cdot(63+64)+1)\,\mathfrak{a}+65^2$; infine dalla $I=\mathsf{pell}\big(G,\,H\big)=(G+1)\,(G-1)\,H^2+1$ segue che $I>\mathfrak{n}^2(G-1)^2$. ⊣

Soluzione Es. 114. Cominciamo col porre $X=\boldsymbol{x}_{\mathfrak{n}}^2(\mathfrak{a})$ e col richiamare che vi sono un'infinità di $q>0$ tali che $2\,\big(\boldsymbol{x}_{\mathfrak{n}}(\mathfrak{a})\,\boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})\big)^2\,(m+1)\mid\boldsymbol{y}_q(\mathfrak{a})$.[2] A ogni q

[2] Vedi appendice sulle equazioni di Pell.

corrisponde un diverso i tale che $2\left(\boldsymbol{x}_{\mathfrak{n}}(\mathfrak{a})\,\boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})\right)^2(m+1)(i+1)=\boldsymbol{y}_q(\mathfrak{a})$ ed un $U=\boldsymbol{x}_q^2(\mathfrak{a})$. Fissati cosí i, E ed U, procederemo ora a determinare j, H, G ed I.

Posto $G=U\,(U-\mathfrak{a})+\mathfrak{a}$, osserviamo che da $\mathfrak{n}>0$ ed $\mathfrak{a}>1$ conseguono $\boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})\neq 0$, $\boldsymbol{y}_q(\mathfrak{a})>1$, $q>1$, $\boldsymbol{x}_q(\mathfrak{a})>\mathfrak{a}$, $U>\mathfrak{a}$, $G>\mathfrak{a}$. Inoltre $G=U^2-\mathfrak{a}\,(U-1)=1+2\,(\mathfrak{a}^2-1)\,\boldsymbol{y}_q^2(\mathfrak{a})+(\mathfrak{a}^2-1)^2\,\boldsymbol{y}_q^4(\mathfrak{a})+\mathfrak{a}\,(1-\mathfrak{a}^2)\,\boldsymbol{y}_q^2(\mathfrak{a})$; pertanto $G\equiv 1\ (\mathbf{mod}\ 2\,y)$, visto che $2\,y=2\,\boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$ divide $\boldsymbol{y}_q(\mathfrak{a})$. Grazie alla regola di congruenza, otteniamo che $\boldsymbol{y}_{\mathfrak{n}}(G)\equiv\mathfrak{n}\ (\mathbf{mod}\ 2\,y)$; inoltre $\boldsymbol{y}_{\mathfrak{n}}(G)\geqslant\boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})\geqslant\mathfrak{n}$.

Posto $H=\boldsymbol{y}_{\mathfrak{n}}(G)$—cosí che $H\geqslant y$—, individuiamo un j tale da soddisfare la $H=\mathfrak{n}+2\,y\,j$ e poniamo infine $I=\boldsymbol{x}_{\mathfrak{n}}^2(G)$.

Concludiamo osservando che il prodotto dei tre quadrati perfetti X, U, I è a sua volta un quadrato. Inoltre, da $G\equiv\mathfrak{a}\ (\mathbf{mod}\ U)$ discende $H=\boldsymbol{y}_{\mathfrak{n}}(G)\equiv\boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})=y\ (\mathbf{mod}\ U)$ grazie alla regola di congruenza. La $y\geqslant\mathfrak{n}$ segue da $y=\boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$. ⊣

Soluzione Es. 117. Nulla osta all'eliminazione, in quanto le incognite si riferiscono ad interi e non (almeno *a priori*) a numeri naturali. Tuttavia, quando eliminiamo U ed H cessano di essere anonime le due variabili che occasionalmente abbiamo chiamato i e j: questo perché U compare ripetuta nelle tre equazioni finali del sistema di Fig. 4.1 ed anche H vi compare ripetuta a valle dell'eliminazione di I. Alla fine otteniamo

$$\begin{array}{rcl}
\left((\mathfrak{a}^2-1)\,y^2+1\right)\left((\mathfrak{a}^2-1)\left(2\,(i+1)\left((\mathfrak{a}^2-1)\,y^2+1\right)(m+1)\,y^2\right)^2+1\right) & & \\
\left(\left(\left(\mathfrak{a}-\left((\mathfrak{a}^2-1)\left(2\,(i+1)\left((\mathfrak{a}^2-1)\,y^2+1\right)(m+1)\,y^2\right)^2+1\right)\mathfrak{a}+\right.\right.\right. & & \\
\left.\left.\left.\left((\mathfrak{a}^2-1)\left(2\,(i+1)\left((\mathfrak{a}^2-1)\,y^2+1\right)(m+1)\,y^2\right)^2+1\right)^2\right)^2-1\right) & & \\
\left.(\mathfrak{n}+2\,j\,y)^2+1\right) & = & \square\,, \\
(\mathfrak{a}^2-1)\left(2\,(i+1)\left((\mathfrak{a}^2-1)\,y^2+1\right)(m+1)\,y^2\right)^2+1 & \mid & (\mathfrak{n}+2\,j\,y)-y\,, \\
\mathfrak{n} & \leqslant & y
\end{array}$$

in cui rimangono le incognite i, j, piú altre 3 anonime (riducibili a una tramite il Teor. 9), nascoste nei costrutti $\square, \mid, \leqslant$. ⊣

B. Davis's reduction of $b^n = c$ to the relation $r = \boldsymbol{y}_n(a)$

The following crucial link between exponentiation and the sequence $\langle \boldsymbol{y}_i(a) \rangle_{i\in\mathbb{N}}$ was pointed out in [5] and explained at length, again, in [6]:

$$b \geqslant 1 \implies \Big[\; b^n = c \iff (\exists\, t\,,\, a\,,\, \ell\,,\, r\,,\, h)\Big(\begin{aligned} r = \boldsymbol{y}_n(a) \quad & \& \\ \ell^2 - (a^2-1)\, r^2 = 1 \quad & \& \\ t > b \quad \& \quad t > n \quad & \& \\ (t^2-1)\,(t-1)^2\,(h+1)^2 + 1 = a^2 \quad & \& \\ c < 2ab - b^2 - 1 \quad & \& \\ c \equiv \ell - (a-b)\, r \;(\mod 2ab - b^2 - 1) \quad & \Big)\Big]. \end{aligned}$$

Specifically, when $b \geqslant 1$ and $b^n = c$, the constraints here appearing in the scope of $\exists$ can be satisfied in infinitely many ways: for, corresponding to any $t > n \max b$, it suffices to put $a = \boldsymbol{x}_{t-1}(t)$ in order to be able to determine the values of $\ell\,, r\,,$ and h uniquely (see Lemma B.1 below).

In light of the above biimplication, if we now provided a Diophantine representation of the relation $r = \boldsymbol{y}_n(a)$, we would readily get that the relation $b^n = c$ is also Diophantine.

Let us recall here the proof of the above-stated relationship between exponentiation and the Pell equation. We begin with the proposition:

Lemma B.1. *If $b \geqslant 1$ and $b^n = c$, then to each number of the form $a = \boldsymbol{x}_{(s+1)(t-1)}(t)$ with $t > b \max n$ there correspond uniquely values ℓ, r, h such that the following conditions are met: $r = \boldsymbol{y}_n(a)$, $\ell = \boldsymbol{x}_n(a)$, $c < 2ab - b^2 - 1$, $c \equiv \ell - (a-b)r \pmod{2ab - b^2 - 1}$, and $a^2 - (t^2-1)(t-1)^2(h+1)^2 = 1$.*

Proof. Observe that, since $t > b \geqslant 1$, the Pell equation $x^2 - (t^2-1)y^2 = 1$ has the usual infinite sequence $\langle\langle \boldsymbol{x}_i(t), \boldsymbol{y}_i(t)\rangle\rangle_{i\in\mathbb{N}}$ of solutions; therefore, it makes sense to put $a := \boldsymbol{x}_{(s+1)(t-1)}(t)$. In its turn $a > 1$ holds, because $\boldsymbol{x}_{(s+1)(t-1)}(t) \geqslant \boldsymbol{x}_1(t) > 1$; hence it makes sense to put $r := \boldsymbol{y}_n(a)$ and $\ell := \boldsymbol{x}_n(a)$.

Plainly, $a \geqslant \boldsymbol{x}_{t-1}(t) \geqslant t^{t-1} > b^n$; hence it is easy to see that the inequality $b^n < 2ab - b^2 - 1$ is satisfied[18] when $n > 0$. The same inequality holds when $n = 0$, as it follows from $a \geqslant t^{t-1} \geqslant t > b \geqslant 1$.

The last two conditions in the claim simply state well-known congruences that are satisfied (as recalled in Fig. 2) by the solutions of any Pell equation of the special form being considered here. In particular,

$$c \equiv \ell - (a-b)r \pmod{2ab - b^2 - 1}$$

states that

$$b^n \equiv \boldsymbol{x}_n(a) - (a-b)\boldsymbol{y}_n(a) \pmod{2ab - b^2 - 1}. \qquad (\circ)$$

As for $a^2 - (t^2-1)(t-1)^2(h+1)^2 = 1$, it merely expresses that $\boldsymbol{y}_{(s+1)(t-1)}(t)$ is a non-null multiple of $t-1$—; recall, in fact, that $a = \boldsymbol{x}_{(s+1)(t-1)}(t)$ and $t - 1 > 0$, and that the congruence $\boldsymbol{y}_i(t) \equiv i \pmod{t-1}$ holds in general, for every i. ⊣

We next come to the converse of Lemma B.1:

Lemma B.2. *Suppose that $b \geqslant 1$ and that the conditions*

$$\begin{aligned}
&c \leqslant 2ab - b^2 - 1,\\
&c \equiv \ell - (a-b)r \pmod{2ab - b^2 - 1}\\
&\ell^2 - (a^2-1)r^2 = 1\\
&a^2 - (t^2-1)(t-1)^2(h+1)^2 = 1\\
&t > b \max n,
\end{aligned}$$

[18] Here, as we will again do in the proof of Lemma B.2, we are making use of the following fact (which gets easily proven even for a real number b): *If $n > 0$, $b \geqslant 1$, and $a > b^n$ (with $a, n \in \mathbb{N}$), then $2ab - b^2 - 1 > b^n$.*

are satisfied by a, ℓ, r, t, and h, where n is the value ensuring that $r = \boldsymbol{y}_n(a)$. Then $b^n = c$ holds.

Proof. Since $t > b \geqslant 1$, the Pell equation $x^2 - (t^2-1)\,y^2 = 1$ has the usual infinite sequence $\langle\langle \boldsymbol{x}_i(t)\,,\,\boldsymbol{y}_i(t)\rangle\rangle_{i\in\mathbb{N}}$ of solutions; thus, since $a^2-(t^2-1)\,y^2=1$ holds for some $y>0$, we have $a=\boldsymbol{x}_j(t)$ for some j, where $j>0$—since $a\geqslant t$—and $\ell=\boldsymbol{x}_n(a)$, $r=\boldsymbol{y}_n(a)$ holds for a suitable n. Consequently $2ab-b^2-1\geqslant 2$; moreover, by the well-known congruence $(\circ)$ recalled above, we have

$$c \equiv b^n \ (\mod 2ab-b^2-1\ ),$$

whence the sought equality will follow if we manage to prove that the side b^n of this congruence is smaller than $2ab-b^2-1$ (for, $c\leqslant 2ab-b^2-1$ is an explicit assumption and $b^n\geqslant 1$). Since this is obvious when $n=0$, we will assume $n>0$.

To see that $b^n < 2ab-b^2-1$, we argue as follows. Clearly $\boldsymbol{y}_j(t) = (t-1)\,(h+1)$ holds, whence $(t-1)\,(h+1)\equiv j\ (\mod t-1)$, i.e. $t-1 \mid j$, follows. Since $j\neq 0$, we get $j\geqslant t-1$, and therefore $a=\boldsymbol{x}_j(t)\geqslant t^j\geqslant t^{t-1}>b^n$. The sought inequality follows, which completes the proof. ⊣

Corollary B.3. *Put* $Q(w,h) \ :=\ (w+2)^3\,(w+4)\,(h+1)^2+1$ *. Then,*

$$\begin{aligned} b^n = c \iff (\exists a\,,\,\ell\,,\,r\,,\,j\,,\,h)\Big[\ & (c-1)^2+b+n=0 \ \vee\ (n\geqslant 1\ \&\ c+b=0) \quad \vee \\ & \Big(b\geqslant 1\ \&\ r=\boldsymbol{y}_n(a) \quad \& \\ & \ell^2=(a^2-1)\,r^2+1\ \&\ Q(b+j-2,h)=a^2\ \& \\ & 2ab-b^2-1\ \geqslant\ c \quad \&\quad b+j\geqslant n \quad \& \\ & c\equiv \ell-(a-b)\,r\ (\mod 2ab-b^2-1\ )\Big)\Big]. \end{aligned}$$

Proof. Suppose first that there are a,ℓ,r,j,h satisfying the conditions in the scope of '$\exists$', and that $b\geqslant 1$. By putting $t := b+j+1$, we obviously get $t > b\max n$ and $a^2-(t^2-1)\,(t-1)^2\,(h+1)^2=1$, so that $b^n=c$ holds by Lemma B.2.

Conversely, suppose that $b^n=c$ holds, where $b\geqslant 1$. Put $t := b+n+1$, $j := n$, and $a := \boldsymbol{x}_{t-1}(t)$. Then, by Lemma B.1, unique values ℓ, r, h exist satisfying all conditions that appear in the third disjunct of the scope of '$\exists$' in the claim. ⊣