$\mathfrak{E} \subseteq \mathfrak{D}$: *L'esponenziazione in poche incognite*

Eugenio G. Omodeo

$y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$

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

Trieste, 28.04–12/19.05.2022

$\mathfrak{E} \subseteq \mathfrak{D}$: *L'esponenziazione in poche incognite*

Eugenio G. Omodeo

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

$y \;=\; \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$

$$\begin{array}{rcl} U & \leftrightharpoons & \mathrm{pell}\Big(\mathfrak{a},\ 2\,(i+1)\,y^2\,\mathrm{pell}\big(\mathfrak{a},\ y\big)\Big) \\ H & \leftrightharpoons & \mathfrak{n} + 2\,y\,j \\ \hline \square & = & U\,\mathrm{pell}\big(\mathfrak{a},\ y\big)\,\mathrm{pell}\big(U\,(U-\mathfrak{a})+\mathfrak{a},\ H\big) \\ U & \mid & H - y \\ \mathfrak{n} & \leqslant & y \end{array}$$

$$\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c} \quad \Longleftrightarrow \quad \mathfrak{c} = \left\lfloor \frac{\boldsymbol{y}_{\mathfrak{n}+1}(\ 8\,\mathfrak{b}\,(\mathfrak{n}+1)\ \boldsymbol{y}_{\mathfrak{n}+1}(\mathfrak{b}+1)+2\ )}{\boldsymbol{y}_{\mathfrak{n}+1}(\ 8\quad(\mathfrak{n}+1)\ \boldsymbol{y}_{\mathfrak{n}+1}(\mathfrak{b}+1)\quad\ )} \right\rfloor$$

Trieste, 28.04–12/19.05.2022

Voce bibliografica

Yuri Matijasevič and Julia Robinson.
Reduction of an arbitrary diophantine equation to one in 13 unknowns.
Acta Arithmetica, XXVII:521–553, 1975.
Reprinted in [Rob96, p. 235ff.].

Julia Robinson.
The collected works of Julia Robinson, volume 6 of *Collected Works*.
American Mathematical Society, Providence, RI, 1996.
ISBN 0-8218-0575-4. With an introduction by Constance Reid. Edited and with a foreword by Solomon Feferman. xliv+338 pp.

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

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

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

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

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

[MR75, pagg. 521, 522]

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

$[\ldots]$

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. [MR75, pagg. 521, 522]

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

$[\ldots]$

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. [MR75, pagg. 521, 522]

(Qui $\overline{P}$ non indica una complementazione !)

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

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

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

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

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

$[\ldots]$

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. [MR75, pagg. 521, 522]

'Cheap trick' di Putnam:

$$\big(a+1\big)\cdot\Big(1-\overline{P}^{\,2}(\underbrace{a, b, c, d, e, f, g, h, i, j, k, l, m, n}_{14})\Big)-1=\alpha\,.$$

Celebre abbaglio in una recensione di [DPR61]

(Georg Kreisel, 1923–2015)

"*These results are superficially related to Hilbert's tenth Problem on (ordinary, i.e., non-exponential) Diophantine equations. The proof of the authors' results, though very elegant, does not use recondite facts in the theory of numbers nor in the theory of r.e. sets, and so it is likely that the present result is not closely connected with Hilbert's tenth Problem. Also it is not altogether plausible that all (ordinary) Diophantine problems are uniformly reducible to those in a fixed number of variables of fixed degree, which would be the case if all r.e. sets were Diophantine.*"

Poniamo

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

dimodoché l'equazione di Pell di forma particolare che utilizzeremo si possa condensare:

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

Poniamo

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

dimodoché l'equazione di Pell di forma particolare che utilizzeremo si possa condensare:

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

In [MR75, pag. 532] viene proposto un sistema di equazioni diofantee —sostanzialmente quello che ora vedremo— nei parametri $m, \mathfrak{a}, \mathfrak{n}, y$ su $\mathbb{N}$ e nelle incognite (facili da eliminare) X, E, U, G, H, I $\boxed{\text{su } \mathbb{Z}}$, oltre che in due incognite i, j $\boxed{\text{su } \mathbb{N}}$, qui designate anonimamente con '$\bullet$':

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

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

Qui è da intendersi:

$$P = Q \;\&\; R = S \quad \rightsquigarrow \quad P^2 + Q^2 + R^2 + S^2 = 2\,P\,Q + 2\,R\,S\,,$$

$$B \mid C \quad \leftrightarrow_{\mathsf{Def}} \quad C = \pm h\,B \quad \text{per qualche} \quad h \in \mathbb{N}\,,$$

$$\rightsquigarrow \quad C^2 - h^2\,B^2 \;=\; 0\,,$$

$$Q = \square \quad \leftrightarrow_{\mathsf{Def}} \quad Q = h^2 \quad \text{per qualche} \quad h \in \mathbb{N}\,.$$

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

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

Specifica semplificata della rel. $y = y_{\mathfrak{n}}(\mathfrak{a})$

(Imponiamo $m = 0$)

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

Specifica semplificata della rel. $y = y_{\mathfrak{n}}(\mathfrak{a})$

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

Una volta eliminate per sostituzione anche U ed H, quante incognite rimarranno?

Specifica semplificata della rel. $y = y_{\mathfrak{n}}(\mathfrak{a})$

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

Una volta eliminate per sostituzione anche U ed H, quante incognite rimarranno?

5 ?

Specifica semplificata della rel. $y = y_{\mathfrak{n}}(\mathfrak{a})$

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

Una volta eliminate per sostituzione anche U ed H, quante incognite rimarranno?

No, 3 ! (v. sotto)

Relation-combining Thm. [MR75, pagg. 524–527]

Teorema (Combinazione di relazioni diofantee)

C'è per ogni $q \in \mathbb{N}$ un polinomio M_q a coefficienti in $\mathbb{Z}$ tale che, comunque presi $A_1, \ldots, A_q, B, C, D$ in $\mathbb{Z}$ con $B \neq 0$, le condizioni

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

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 x su $\mathbb{N}$. (Teor. qui solo richiamato)

Esempio / Esercizio

Per $q = 0, 1$, possiamo prendere:

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

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

Relation-combining Thm. [MR75, pagg. 524–527]

Teorema (Combinazione di relazioni diofantee)

C'è per ogni $q \in \mathbb{N}$ un polinomio M_q a coefficienti in $\mathbb{Z}$ tale che, comunque presi $A_1, \ldots, A_q, B, C, D$ in $\mathbb{Z}$ con $B \neq 0$, le condizioni

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

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 x su $\mathbb{N}$. (Teor. qui solo richiamato)

Esempio / Esercizio

Per $q = 0, 1$, possiamo prendere:

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

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

Proof sketch: For $q = 0, 1, 2$, we may instantiate M_q as follows:

$$
\begin{aligned}
M_0 &\leftrightharpoons B^2\,x + C^2 - B^2\,(2\,D-1)\,(C^2+1)\,,\\
M_1 &\leftrightharpoons \left(B^2\,x + C^2 - B^2\,(2\,D-1)\,(C^2+1+A_1^2)\right)^2 - B^4\,(2\,D-1)^2\,A_1\,,\\
M_2 &\leftrightharpoons \Bigg(\left[B^2\,x + C^2 - B^2\,(2\,D-1)\left(C^2+\left(1+A_1^2+A_2^2\right)^2\right)\right]^2 +\\
&\qquad B^4\,(2\,D-1)^2\left(A_1 - A_2\left(1+A_1^2+A_2^2\right)^2\right)\Bigg)^2 -\\
&\qquad 4\,B^4\,(2\,D-1)^2\,A_1\left[B^2\,x + C^2 - B^2\,(2\,D-1)\left(C^2+\left(1+A_1^2+A_2^2\right)^2\right)\right]^2 .
\end{aligned}
$$

Here, and beyond $q = 2$, the idea is to set

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

thanks to the product, extracting square roots then becomes unnecessary and M_q turns out to be rewritable as a polynomial with coefficients in $\mathbb{Z}$. ⊣

Teorema (Correttezza)

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 primo dei due sistemi è risolubile sono le stesse per cui vale $y = y_{\mathfrak{n}}(\mathfrak{a})$.

(Inoltre la 2) e la 3) ci forniscono la coprimalità $m + 1 \perp U$).

Teorema (Correttezza)

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 primo dei due sistemi è risolubile sono le stesse per cui vale $y = y_{\mathfrak{n}}(\mathfrak{a})$.
(Inoltre la 2) e la 3) ci forniscono la coprimalità $m + 1 \perp U$).

La verifica che quando $y = y_{\mathfrak{n}}(\mathfrak{a})$ ecc. allora per ogni m sono determinabili (in infiniti modi) valori in $\mathbb{N}$ per le incognite X, E, U, G, H, I, i, j tali da soddisfare il sistema 0)–6) viene lasciata come esercizio.

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

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

$$V = \underbrace{(a+1)\,(a-1)\,u^2+1}_{\mathrm{pell}(a,\,u)}$$ implica, in gen., che

se $a > 1$ e $u \neq 0$ allora $V > a+1$.

$\therefore$ 1)–6) ci danno

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

$V = \underbrace{(a+1)\,(a-1)\,u^2+1}_{\mathsf{pell}(a,\,u)}$ implica, in gen., che

se $a > 1$ e $u \neq 0$ allora $V > a+1$.

$\therefore$ 1)–6) ci danno

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

Grazie alla 0), semplicemente verificando che

$$I \perp X \perp U \perp I\,,$$

otterremo:

$$X = \square\,,\quad U = \square\,,\quad I = \square\,.$$

Grazie alla 0), semplicemente verificando che

$$I \perp X \perp U \perp I,$$

otterremo:

$$X = \square, \quad U = \square, \quad I = \square.$$

In effetti le 2), 3), 4) e 6) ci danno

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

$\therefore$

$$I \perp X \perp U.$$

Grazie alla 0), semplicemente verificando che

$$I \perp X \perp U \perp I,$$

otterremo:

$$X = \square, \quad U = \square, \quad I = \square.$$

Inoltre 4) e 0) ci danno

$$G \equiv \mathfrak{a}, \quad H \equiv y \pmod{U}$$

$\therefore$ (anche per 6) e 1)) $I \equiv X \pmod{U}$ $\therefore$ (grazie a $X \perp U$)

$$I \perp U.$$

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

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

Ora sappiamo che per opportuni $\boxed{p, q, r > 0}$:

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

Ora sappiamo che per opportuni $\boxed{p, q, r > 0}$:

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

Ci basterà stabilire 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 ed $\mathfrak{n}$ da un lato e fra r e p dall'altro, sí che ne discenda $p = \mathfrak{n}$.

In 1º luogo $G \equiv 1 \pmod{2\,y}$ per le 2), 3), 4) $\therefore$

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

grazie alla regoletta di congruenza:

$$g \equiv h \pmod{m} \;\Rightarrow\; \boldsymbol{y}_n(g) \equiv \boldsymbol{y}_n(h) \pmod{m}$$

per $g > 0$, $h > 0$, $m > 0$ ed $n \geqslant 0$. Perciò, grazie alla 5),

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

In 1º luogo $G \equiv 1 \pmod{2y}$ per le 2), 3), 4) $\therefore$

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

grazie alla regoletta di congruenza:

$$g \equiv h \pmod{m} \implies \boldsymbol{y}_n(g) \equiv \boldsymbol{y}_n(h) \pmod{m}$$

per $g > 0$, $h > 0$, $m > 0$ ed $n \geqslant 0$. Perciò, grazie alla 5),

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

In 2º luogo $G \equiv \mathfrak{a} \pmod{U}$ per la 4) $\therefore$ (per la stessa regoletta)

$$\begin{array}{rcccll} H & = & \boldsymbol{y}_r(G) & \equiv & \boldsymbol{y}_r(\mathfrak{a}) \pmod{U} & \text{e (per la 0))} \\ \boldsymbol{y}_p(\mathfrak{a}) & = & y & \equiv & H \pmod{U} & \therefore \\ & & \boldsymbol{y}_p(\mathfrak{a}) & \equiv & \boldsymbol{y}_r(\mathfrak{a}) \pmod{\boldsymbol{x}_q^2(\mathfrak{a})} & \therefore \\ & & \boldsymbol{y}_r(\mathfrak{a}) & \equiv & \boldsymbol{y}_p(\mathfrak{a}) \pmod{\boldsymbol{x}_q(\mathfrak{a})} . & \end{array}$$

In 2º luogo $G \equiv \mathfrak{a} \pmod{U}$ per la 4) $\therefore$ (per la stessa regoletta)

$$\begin{aligned} H &= \boldsymbol{y}_r(G) \equiv \boldsymbol{y}_r(\mathfrak{a}) \pmod{U} && \text{e (per la 0))} \\ \boldsymbol{y}_p(\mathfrak{a}) &= y \equiv H \pmod{U} && \therefore \\ \boldsymbol{y}_p(\mathfrak{a}) &\equiv \boldsymbol{y}_r(\mathfrak{a}) \pmod{\boldsymbol{x}_q^2(\mathfrak{a})} && \therefore \\ \boldsymbol{y}_r(\mathfrak{a}) &\equiv \boldsymbol{y}_p(\mathfrak{a}) \pmod{\boldsymbol{x}_q(\mathfrak{a})} \,. \end{aligned}$$

Perciò, grazie ai due lemmi *'step-down'*, alla 2) ed a $q > 0$:

$$\begin{aligned} r &\equiv \pm p \pmod{2\,q} \,, \\ y^2 \mid E = \boldsymbol{y}_q(\mathfrak{a}) &\;\therefore\; y \mid q \,. \end{aligned}$$

Mettendo insieme, otteniamo

$$\mathfrak{n} \equiv \pm p \pmod{2\,y} \,,$$

$\therefore$ (dato che $\mathfrak{n} \leqslant y$ per la 0) e che $p \leqslant \boldsymbol{y}_p(\mathfrak{a}) = y$)

$$\mathfrak{n} = p \,. \qquad \dashv$$

Esercizio.

La definizione polinomiale

$$R(\mathfrak{a}, \mathfrak{n}, y, \bullet, \bullet, \bullet) \quad = \quad 0$$

della relazione $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$, costruita sopra, funziona solo per $\mathfrak{n} > 0$ e $y > 0$. Mostrare che allora

$$(y + \mathfrak{n}) \left(\left(1 - R(\mathfrak{a}, \mathfrak{n}, y, \bullet, \bullet, \bullet)\right) y\, \mathfrak{n} - 1 - \bullet \right) \quad = \quad 0$$

definisce $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$ in generale (fermo restando che $\mathfrak{a} > 1$). $\dashv$

Aggiungendo a quest'ultima

$$(y+\mathfrak{n})\left(\left(1-R(\mathfrak{a},\mathfrak{n},y,\bullet,\bullet,\bullet)\right)y\,\mathfrak{n}-1-\bullet\right) \;=\; 0$$

il 'raccordo'

$$\begin{aligned} x^2 &= \mathsf{pell}(\mathfrak{a},\, y) \\ \bullet^2\,(2\,\mathfrak{a}\,\mathfrak{b}-\mathfrak{b}^2-1)^2 &= \left(x-y\,(\mathfrak{a}-\mathfrak{b})-\mathfrak{c}\right)^2 \\ 2\,\mathfrak{a}\,\mathfrak{b}-\mathfrak{b}^2-1 &\geqslant \mathfrak{c} \\ \mathfrak{b}+h &\geqslant \mathfrak{n} \\ \mathfrak{a}^2 &= \mathsf{pell}\big(\mathfrak{b}+h+1\,,\,(\mathfrak{b}+h)\,(\bullet+1)\big) \end{aligned}$$

otterremo una definiz. di $\mathfrak{b}^{\mathfrak{n}}=\mathfrak{c}$ che funziona se so che $\mathfrak{b}>0$.

Siamo cosí giunti a un'eq. polinomiale

$$Q(\mathfrak{b}, \mathfrak{n}, \mathfrak{c}, z_1, \ldots, z_{12}) \quad = \quad 0$$

nelle 12 'incognite'

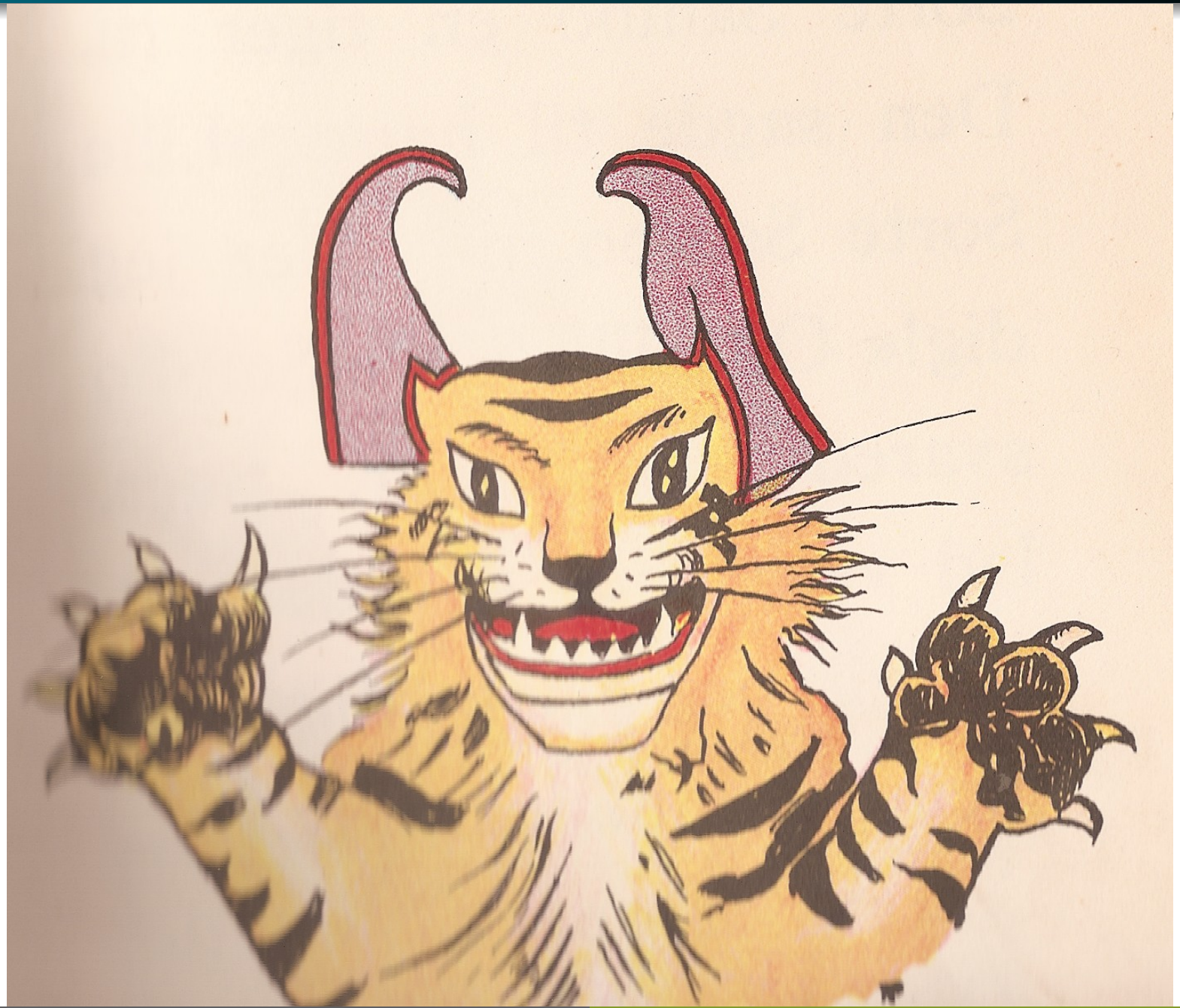
$$\mathfrak{a}, x, y, h, \geqslant, \geqslant, \bullet, \bullet, \bullet, \bullet, \bullet, \bullet,$$

donde una specifica completa,

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

dell'esponenziazione. $\boxed{13}$ incognite in tutto!

Vi ringrazio per l'attenzione !



Richiami essenziali sull'equazione di Pell

Circa le soluz. alle eq. di Pell della forma $X^2 = (a^2 - 1)\, Y^2 + 1$, con $a > 1$, richiamiamo:

Circa le soluz. alle eq. di Pell della forma $X^2 = (a^2-1)\,Y^2 + 1$, con $a > 1$, richiamiamo:

Le soluzioni intere non-negative, ordinate per valori crescenti, formano la successione

$$X = \boldsymbol{x}_n(a)\,, \quad Y = \boldsymbol{y}_n(a)$$

($n \in \mathbb{N}$), ove

$$\boldsymbol{x}_n(a) + \boldsymbol{y}_n(a)\sqrt{\mathfrak{d}} \;=\; \left(a+\sqrt{\mathfrak{d}}\right)^n, \quad \text{con} \quad \mathfrak{d} \;=\; a^2-1\,.$$

Vige la doppia ricorrenza:

$$\begin{array}{rcl|rcl}
\boldsymbol{x}_0(a) & = & 1\,, & \boldsymbol{y}_0(a) & = & 0\,; \\
\boldsymbol{x}_1(a) & = & a\,, & \boldsymbol{y}_1(a) & = & 1\,; \\
\hline
\boldsymbol{x}_{n+2}(a) & = & 2\,a\,\boldsymbol{x}_{n+1}(a) - \boldsymbol{x}_n(a)\,, & & & \\
\boldsymbol{y}_{n+2}(a) & = & 2\,a\,\boldsymbol{y}_{n+1}(a) - \boldsymbol{y}_n(a)\,. & & &
\end{array}$$

(Cambia forse qualcosa quando $a = 1$?)

Regoletta: Per $p, q, r > 0$ ed $\ell \geqslant 0$:

$$p \equiv q \pmod{r} \Rightarrow \begin{cases} \boldsymbol{x}_\ell(p) \equiv \boldsymbol{x}_\ell(q) \pmod{r}, \\ \boldsymbol{y}_\ell(p) \equiv \boldsymbol{y}_\ell(q) \pmod{r}. \end{cases}$$

I due lemmi 'step-down': Per $i, j \geqslant 0$ ed $n > 0$:

- $\boldsymbol{y}_i^2(a) \mid \boldsymbol{y}_j(a) \Rightarrow \boldsymbol{y}_i(a) \mid j$, se $a > 0$.
- $\boldsymbol{y}_i(a) \equiv \boldsymbol{y}_j(a) \pmod{\boldsymbol{x}_n(a)} \Rightarrow (i \equiv j \vee i \equiv -j) \pmod{2\,n}$.

Inoltre:

Lemma A. $y_n(a) \equiv n \pmod{a-1}$.

Lemma B. $x_n(a) - y_n(a)\,(a-\ell) \equiv \ell^n \pmod{2\,a\,\ell - \ell^2 - 1}$.

Lemma C. $x_n(a) \geqslant a^n$.

Lemma D. $y_{n+1}(a) > n$.

Lemma E. Se $c > 0$, $a > 1$, $a > b^c$ e $b \geqslant 1$ (con $a, b, c \in \mathbb{N}$):

$$2\,a\,b - b^2 - 1 > b^c \ .$$

Dimostrazione del Lemma E

Lemma E. Se $c > 0$, $a > 1$, $a > b^c$ e $b \geqslant 1$ (con $a, b, c \in \mathbb{N}$):

$$2\,a\,b - b^2 - 1 \;>\; b^c \;.$$

Dim. del Lemma E. Ovvio che $a > b \geqslant 1$. Inoltre, la funzione

$$g(y) \;=_{\mathsf{Def}}\; 2\,a\,y - y^2 - 1$$

di var. *reale* ha derivata positiva per $y < a$ $\therefore$ cresce su $[\,1,\, a\,[$ $\therefore$

$$g(y) \;\geqslant\; g(1) \;=\; 2\,a - 2 \;\geqslant\; a \;>\; b^c$$

per ogni $y \in [\,1,\, a\,[$. In particolare, $g(\,b\,) > b^c$. $\dashv$

Le equazioni di raccordo

Le equazioni che raccordano $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$ con l'esponenziazione sono:

(vii)	x^2	$=$	$\mathsf{pell}\big(\mathfrak{a}\,,\ y\big)$
(viii)	$\bullet^2\ (2\,\mathfrak{a}\,\mathfrak{b} - \mathfrak{b}^2 - 1)^2$	$=$	$\big(x - y\cdot(\mathfrak{a}-\mathfrak{b}) - \mathfrak{c}\big)^2$
(ix)	$2\,\mathfrak{a}\,\mathfrak{b} - \mathfrak{b}^2 - 1$	$\geqslant$	$\mathfrak{c}$
(x)	$\mathfrak{b} + h$	$\geqslant$	$\mathfrak{n}$
(xi)	$\mathfrak{a}^2$	$=$	$\mathsf{pell}\big(\mathfrak{b}+h+1\,,\ (\mathfrak{b}+h)\,(p+1)\big)$

La seconda di queste esprime:

$$\text{(viii)}\ \Big|\ \ \mathfrak{c} \ \equiv\ x - y\cdot(\mathfrak{a}-\mathfrak{b}) \quad \big(\textbf{mod}\ 2\,\mathfrak{a}\,\mathfrak{b} - \mathfrak{b}^2 - 1\big)\ \ ;$$

l'ultima: che $\mathfrak{a} = \boldsymbol{x}_n(\mathfrak{b}+h+1)\ \&\ \mathfrak{b}+h \mid \boldsymbol{y}_n(\mathfrak{b}+h+1)$, per un n.

Teorema. Il sistema

$$D(\overbrace{\mathfrak{b}, \mathfrak{n}, \mathfrak{c}}^{\text{param.}}, \overbrace{y, \mathfrak{a}, \vec{z}}^{\text{incogn.}})$$

che si ottiene aggiungendo le (vii)–(xi) alle 0)–6) ha soluzione, per $\mathfrak{b} > 0$, se e solo se $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$.

Nel dimostrare ciò, assumeremo già verificata la correttezza della specifica 0)–6), i.e.:

0)–6) ha soluzione, per $\mathfrak{a} > 1$ ed $\mathfrak{n}, y > 0$, se e solo se $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$.

Teorema. Il sistema

$$D(\overbrace{\mathfrak{b}, \mathfrak{n}, \mathfrak{c}}^{\text{param.}}, \overbrace{y, \mathfrak{a}, \vec{z}}^{\text{incogn.}})$$

che si ottiene aggiungendo le (vii)–(xi) alle 0)–6) ha soluzione, per $\mathfrak{b} > 0$, se e solo se $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$.

Nel dimostrare ciò, assumeremo già verificata la correttezza della specifica 0)–6), i.e.:

0)–6) ha soluzione, per $\mathfrak{a} > 1$ ed $\mathfrak{n}, y > 0$, se e solo se $y = \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})$.

Supponiamo dapprima soddisfatto il sistema $D(\mathfrak{b}, \mathfrak{n}, \mathfrak{c})$. Utilizzando (x), (xi), l'ipotesi $\mathfrak{b} \geqslant 1$, la correttezza della specifica 0)–6), la (vii), si ottengono:

$$\begin{aligned} \mathfrak{b} + h + 1 &\geqslant 2\,, \\ \mathfrak{a} &> 1\,, \\ y &= \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a}) \quad \text{ed} \quad x = \boldsymbol{x}_{\mathfrak{n}}(\mathfrak{a}) \end{aligned}$$

e quindi, grazie alla (viii),

$$\mathfrak{c} \equiv \boldsymbol{x}_{\mathfrak{n}}(\mathfrak{a}) - \boldsymbol{y}_{\mathfrak{n}}(\mathfrak{a})\,(\mathfrak{a} - \mathfrak{b}) \quad \left(\mathbf{mod}\ 2\,\mathfrak{a}\,\mathfrak{b} - \mathfrak{b}^2 - 1\right)\,,$$

dove $2\,\mathfrak{a}\,\mathfrak{b} - \mathfrak{b}^2 - 1 \geqslant 2$. Grazie al Lemma B,

$$\mathfrak{c} \equiv \mathfrak{b}^{\mathfrak{n}} \quad \left(\mathbf{mod}\ 2\,\mathfrak{a}\,\mathfrak{b} - \mathfrak{b}^2 - 1\right)\,.$$

☞

☞

Discenderà l'attesa ug. $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$ se stabiliamo che il membro sinistro è minore di $2\,\mathfrak{a}\,\mathfrak{b} - \mathfrak{b}^2 - 1$ (come espressam. richiesto, per il membro destro, dalla (ix)).
Nel caso $\mathfrak{n} = 0$, segue subito $\mathfrak{c} = 1 = \mathfrak{b}^{\mathfrak{n}}$ da (viii) e (ix); supponiamo dunque $\mathfrak{n} > 0$. Posto $q = \mathfrak{b} + h$, in base alla (x) abbiamo che

$$0 \;<\; \mathfrak{b} \;\leqslant\; q \qquad \text{e} \qquad 0 \;<\; \mathfrak{n} \;\leqslant\; q \;;$$

quindi, grazie alla (xi), c'è un n tale che

$$\mathfrak{a} \;=\; \boldsymbol{x}_n(q+1) \qquad \text{e} \qquad q\cdot(p+1) \;=\; \boldsymbol{y}_n(q+1)\;,$$

donde, per il Lemma A,

$$q\cdot(p+1) \;\equiv\; n \pmod{q} \qquad \therefore \qquad q \mid n\;.$$

☞

☞

Da $\boldsymbol{y}_n(q+1) \neq 0$ consegue $n \neq 0 \therefore n \geqslant q$, cosicché, grazie al Lemma C,

$$\mathfrak{a} \;=\; \boldsymbol{x}_n(q+1) \;\geqslant\; (q+1)^n \;\geqslant\; (q+1)^q \;>\; \mathfrak{b}^n$$

e di qui, grazie al Lemma E,

$$\mathfrak{b}^n < 2\,\mathfrak{a}\,\mathfrak{b} - \mathfrak{b}^2 - 1\,,$$

che è quanto cercavamo. ⊣

Supponendo ora, per converso, che $\mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}$ (con $\mathfrak{b} > 0$), vogliamo soddisfare le condizioni $D(\mathfrak{b}, \mathfrak{n}, \mathfrak{c})$. Fissato un q tale che $q \geqslant \mathfrak{b}$ e $q \geqslant \mathfrak{n}$ come richiesto dalla (x), poniamo $\mathfrak{a} = \boldsymbol{x}_q(q+1)$. Avendo, grazie al Lemma A,

$$\boldsymbol{y}_q(q+1) \quad \equiv \quad q \quad \equiv \quad 0 \pmod{q} \ ,$$

potremo scrivere (alla luce del Lemma D)

$$\boldsymbol{y}_q(q+1) \quad = \quad q \cdot (p+1) \ ,$$

cosí soddisfacendo la (xi)—che ci dà anche $\mathfrak{a} > 1$.
Grazie al Lemma C, abbiamo che

$$\mathfrak{a} \quad = \quad \boldsymbol{x}_q(q+1) \quad \geqslant \quad (q+1)^q \quad > \quad \mathfrak{b}^{\mathfrak{n}} \ ;$$

perciò, tenendo conto che $\mathfrak{b} \geqslant 1$, possiamo convalidare la (ix) o grazie al Lemma E oppure, se $\mathfrak{n} = 0$, osservando che la $1 < 2\,\mathfrak{a}\mathfrak{b} - \mathfrak{b}^2 - 1$ consegue dalle ulteriori disuguaglianze $(q+1)^q \geqslant q+1 > \mathfrak{b}$.

☞

Si ponga poi $x = \boldsymbol{x}_n(\mathfrak{a})$, $y = \boldsymbol{y}_n(\mathfrak{a})$, in modo che sia soddisfatta la (vii) e dunque, in base alla correttezza della specifica 0)–6), sia risolubile 0)–6). Il Lemma B ci dà la congruenza

$$\mathfrak{c} \equiv x - y\,(\mathfrak{a} - \mathfrak{b}) \quad \left(\mathbf{mod}\ 2\,\mathfrak{a}\,\mathfrak{b} - \mathfrak{b}^2 - 1\right),$$

onde possiamo trovare un $\bullet$ soddisfacente la (viii). ⊣