Journal of Logic & Analysis 1:4 (2009) 1–23
ISSN 1759-9008

Decomposition of terms in Lucas sequences

ABDELMADJID BOUDAOUD

Let P, Q be non-zero integers such that $D = P^2 - 4Q$ is different from zero. The sequences of integers defined by

$$\begin{cases} U_n = PU_{n-1} - QU_{n-2}; & U_0 = 0, \quad U_1 = 1; \\ V_n = PV_{n-1} - QV_{n-2}; & V_0 = 2, \quad V_1 = P. \end{cases}$$

are called the Lucas sequences associated to the pair (P, Q) [6,7]. In this paper we prove the following result: *If P, Q are such that D is strictly positive, then, for unlimited n, each of the integers U_n and V_n differs by a limited integer from a product of two unlimited integers.*

2000 Mathematics Subject Classification 11B39, 11A51, 26E35

Keywords: Lucas sequences, Fibonacci sequences, nonstandard analysis

1 Introduction

Let N be any large integer. Proceeding directly to the factorization of N is not an easy task, even unfeasible unless N belongs to a particular family of integers. Then to surmount this major difficulty we might choose to ask about the factorization of an integer in a small neighborhood of N instead of N. This is expressed through the following question: Is there a small integer s such that $N = s + \mu\vartheta$, where μ and ϑ are two large integers ?

The fact that the integer $N - s$ is a product of two large integers, gives an idea of its factorization. In the existing literature, the decomposition of integers is an immense problem which has been posed in several ways and treated by different methods (for example [1, 3, 8]).

This idea originated in [2], where we chose to work in the framework of nonstandard analysis [4, 5] to be able to give sense to the words "small", "large", ... and the question has the formulation: Is every unlimited integer the sum of a limited integer and a product of two unlimited integers ? To give a partial answer we provided some examples [2] and we devote the present work to another example concerning Lucas

Published: 16 April 2009 doi: 10.4115/jla.2009.1.4

sequences. In the final section we give the classical equivalence of the result obtained and a general remark.

We start with a brief overview of Lucas sequences associated to a pair of integers [6]. Let P, Q be non-zero integers. Consider the polynomial $p(x) = x^2 - Px + Q$; its discriminant is $D = P^2 - 4Q$ and the roots are

$$\alpha = \frac{P + \sqrt{D}}{2}, \qquad \beta = \frac{P - \sqrt{D}}{2}. \tag{1–1}$$

Suppose that P and Q are such that $D \neq 0$. The sequences of integers

$$\begin{cases} U_n(P,Q) = \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & \text{with} \quad U_0(P,Q) = 0 \ \text{ and } U_1(P,Q) = 1 \\ V_n(P,Q) = \alpha^n + \beta^n & \text{with} \quad V_0(P,Q) = 2 \ \text{ and } \ V_1(P,Q) = P \end{cases} \tag{1–2}$$

are called the *Lucas sequences* associated to the pair (P,Q). We will note by U_n (resp. V_n) the element $U_n(P,Q)$ (resp. $V_n(P,Q)$).

It can be proved that for $n \geq 2$

$$\begin{array}{ll} U_n = PU_{n-1} - QU_{n-2}; & U_0 = 0, \quad U_1 = 1, \\ V_n = PV_{n-1} - QV_{n-2}; & V_0 = 2, \quad V_1 = P\,. \end{array} \tag{1–3}$$

In the particular case $(P,Q) = (1,-1)$, the sequence $(U_n)_{n\geq 0}$ begins $0, 1, 1, 2, 3, 5, 8, 13$ ... and was first considered by Fibonacci. The companion sequence of the Fibonacci numbers, still with $(P,Q) = (1,-1)$, is the sequence of Lucas numbers $(V_n)_{n\geq 0}$ and it begins $2, 1, 3, 4, 7, 11, 18$ ... .

We give here some known results [6, 7]

$$V_{2n} = (V_n)^2 - 2Q^n. \tag{1–4}$$

Let p be a prime integer, then

$$\begin{cases} U_p = \left(\dfrac{D}{p}\right) mod\,(p) & \text{for } p \geq 3, \\ V_p = P\, mod\,(p) & \text{for } p \geq 2, \end{cases} \tag{1–5}$$

where $\left(\dfrac{D}{p}\right)$ represents the Legendre symbol which is, according to the relation between p and D, one of the values -1, 0, $+1$. In addition, if n, $k \geq 1$, then

$$U_n \mid U_{nk} \text{ for all } k, \qquad V_n \mid V_{nk} \text{ if } k \text{ is odd}. \tag{1–6}$$

Moreover

$$\begin{cases} U_n(-P,Q) = (-1)^{n-1}\, U_n(P,Q)\,, \\ V_n(-P,Q) = (-1)^n\, V_n(P,Q)\,. \end{cases} \tag{1–7}$$

Fermat's Little Theorem. *If p is a prime number and if a is an integer, then*

$$a^p \equiv a\,[p]\,. \tag{1–8}$$

In particular, if p does not divide a then $a^{p-1} \equiv 1\,[p]$.

External recurrence principle [4]**.** *For all internal or external formula $F(n)$, we have*

$$\left[F(0) \quad \textit{and} \quad \forall^{st} n\ (F(n) \Longrightarrow F(n+1))\right] \Longrightarrow \forall^{st} n\, F(n)\,. \tag{1–9}$$

Notations. Let x, y be real numbers (not necessarily integers) .

(i) $x \approx 0$ (resp. $x \approx +\infty$) denotes that x is *infinitesimal* (resp. x is *positive unlimited)*. We have an analogous definition for $x \approx -\infty$.

(ii) x and y are called *infinitely close,* denoted by $x \approx y$, if $x - y \approx 0$.

(iii) We say that x is *appreciable* if it is neither unlimited nor infinitesimal.

(iv) The inequality $x \gtrapprox y$ means that $x > y$ and $x \not\approx y$. We have an analogous definition for $\lessapprox$.

(v) The Greek letter ϕ is used for an infinitesimal strictly positive. Two occurrences of ϕ are not necessarily equal.

(vi) $\mathbb{P}$ represents the set of all prime integers.

2 Main result

Theorem 2.1 *If P, Q are such that $D > 0$, then, for unlimited n, each of the integers U_n and V_n differs by a limited integer from a product of two unlimited integers.*

Let P and Q be such that $D > 0$ and let $n \approx +\infty$. We put $\lambda = \dfrac{P}{\sqrt{D}}$. In order to prove the main result we need the following lemmas.

Lemma 2.2 *(a)* $\alpha \neq \beta$, $\max\left(|\alpha|, |\beta|\right) \gtrapprox 1$ *and*

$$\frac{\beta}{\alpha} = \frac{\lambda - 1}{\lambda + 1}. \tag{2–1}$$

(b) If $P > 0$, then

(i) $|\alpha| > |\beta|$,

(ii) $1 - \dfrac{\beta}{\alpha}$ *is positive infinitesimal* $\iff \lambda \approx +\infty$,

(iii) $1+\dfrac{\beta}{\alpha}$ *is positive infinitesimal* $\iff$ λ *is positive infinitesimal,*

(iv) $\dfrac{\beta}{\alpha} \not\approx \pm 1$ *if and only if* λ *is appreciable and positive.*

(c) *If* $P<0$,

(i) $|\alpha|<|\beta|$,

(ii) $1-\dfrac{\alpha}{\beta}$ *is positive infinitesimal* $\iff$ $\lambda \approx -\infty$,

(iii) $1+\dfrac{\alpha}{\beta}$ *is positive infinitesimal* $\iff$ λ *is negative infinitesimal,*

(iv) $\dfrac{\alpha}{\beta} \not\approx \pm 1$ *if and only if* λ *is appreciable and negative.*

Proof (a) $\alpha \neq \beta$ because $\alpha = \dfrac{P+\sqrt{D}}{2}$ and $\beta = \dfrac{P-\sqrt{D}}{2}$. The following are the possible cases.

(i) $P>1$. In this case $\alpha \gtrapprox 1$.

(ii) $P=1$. In this case Q must be strictly negative and therefore $\alpha \gtrapprox 1$.

(iii) $P=-1$. In this case Q must be strictly negative and therefore $|\beta| \gtrapprox 1$.

(iv) $P<-1$. In this case $|\beta| \gtrapprox 1$.

Hence

$$\max\left(|\alpha|,|\beta|\right) \gtrapprox 1.$$

By (1.1), $\dfrac{\beta}{\alpha} = \dfrac{\lambda-1}{\lambda+1}$.

(b) If $P>0$, then it is immediate that $|\alpha|>|\beta|$. Furthermore, $\lambda>0$ and the remainder of the proof can be deduced from the graph of the function $\dfrac{\beta}{\alpha}(\lambda) = \dfrac{\lambda-1}{\lambda+1}$ which is strictly increasing from $[0,+\infty[$ onto $[-1,1[$, where $\lim\limits_{\lambda \longrightarrow 0^+} \dfrac{\beta}{\alpha}(\lambda) = -1$ and $\lim\limits_{\lambda \longrightarrow +\infty} \dfrac{\beta}{\alpha}(\lambda) = 1$.

(c) This is similar to (b). □

Remark. By (1–7) we need to prove the following lemmas only for $P>0$ in which case α is positive and according to Lemma 2.2 $\alpha > |\beta|$. Consequently $\alpha \gtrapprox 1$.

Lemma 2.3 *Each of* $|U_n|$ *and* $|V_n|$ *is of the form* ωn, *where* ω *is unlimited (* ω *is not necessarily the same in each case).*

Proof By (1–2)

$$\text{(2–2)} \qquad \begin{cases} U_n &= \alpha^{n-1}\left(\dfrac{1-\left(\beta/\alpha\right)^n}{1-\left(\beta/\alpha\right)}\right), \\ V_n &= \alpha^n\left(1+\left(\beta/\alpha\right)^n\right). \end{cases}$$

We divide the proof into three cases.

(A) $\dfrac{\beta}{\alpha} = 1-\phi$. Then $0 < \left(\beta/\alpha\right)^n < \beta/\alpha < 1$. Hence $1-\left(\beta/\alpha\right)^n > 1-\left(\beta/\alpha\right) > 0$. By (2–2) it follows $U_n = \alpha^{n-1}c$ with $c > 1$ and therefore $U_n = \omega n$, where $\omega \approx +\infty$. Also $V_n = \alpha^n d$ with $d > 1$ and consequently $V_n = \omega n$, where $\omega \approx +\infty$.

(B) $\dfrac{\beta}{\alpha} = -1+\phi$. According to Lemma 2.2, λ is positive infinitesimal. There are two subcases.

(1) n is odd. By (2–2)

$$\begin{aligned} U_n &= \alpha^{n-1}\left(\frac{1-(-1+\phi)^n}{1-(-1+\phi)}\right) = \alpha^{n-1}\frac{\left(1+(1-\phi)^n\right)}{2-\phi} \\ &= \alpha^{n-1}a, \end{aligned}$$

where a is appreciable and positive. Therefore $U_n = \omega n$, where $\omega \approx +\infty$. Concerning V_n by (2–1) and (2–2), $V_n = \alpha^n\left(1+\left(\dfrac{\lambda-1}{\lambda+1}\right)^n\right)$. Hence

$$V_n = \alpha^n\left(1-\left(\frac{1-\lambda}{\lambda+1}\right)^n\right) > \alpha^n\left(1-\frac{1}{(\lambda+1)^n}\right)$$

and then $V_n > \alpha^n\dfrac{n\lambda}{(\lambda+1)^n}$ which implies $\dfrac{V_n}{n} > \alpha^n\dfrac{\lambda}{(\lambda+1)^n}$. Moreover $\dfrac{\lambda}{(\lambda+1)^n}\alpha^n \approx +\infty$, indeed replacing α by $\dfrac{P+\sqrt{D}}{2}$ we get

$$\begin{aligned} \frac{\lambda}{(\lambda+1)^n}\alpha^n &= \frac{\lambda}{(\lambda+1)^n}(1+\lambda)^n\left(\frac{\sqrt{D}}{2}\right)^n \\ &= \frac{P}{2}\left(\frac{\sqrt{D}}{2}\right)^{n-1}, \end{aligned}$$

where $\dfrac{P}{2}\left(\dfrac{\sqrt{D}}{2}\right)^{n-1} \approx +\infty$ because $\sqrt{D} \approx +\infty$. Therefore V_n is of the form ωn, where $\omega \approx +\infty$.

(2) n is even. By (2–2)

$$U_n = \alpha^{n-1}\left(\frac{1-(\beta/\alpha)^n}{1-(\beta/\alpha)}\right) = \frac{\alpha^{n-1}}{2-\phi}\left(1-(\beta/\alpha)^n\right) = \frac{\alpha^{n-1}}{a}\left(1-(\beta/\alpha)^n\right),$$

where $a = 2-\phi$ is appreciable. By (2–1), $\dfrac{\beta}{\alpha} = \dfrac{\lambda-1}{\lambda+1}$ where λ is positive infinitesimal, and since n is even,

$$U_n = \frac{\alpha^{n-1}}{a}\left(1-\left(\frac{1-\lambda}{\lambda+1}\right)^n\right).$$

From $\dfrac{1}{(\lambda+1)^n} > \left(\dfrac{1-\lambda}{\lambda+1}\right)^n$ it follows that $0 < 1-\dfrac{1}{(\lambda+1)^n} < 1-\left(\dfrac{1-\lambda}{\lambda+1}\right)^n$, hence $U_n > \dfrac{\alpha^{n-1}}{a}\left(1-\dfrac{1}{(\lambda+1)^n}\right)$ and then $U_n > \dfrac{\alpha^{n-1}}{a}\dfrac{n\lambda}{(\lambda+1)^n}$. So

$$\frac{U_n}{n} > \frac{\alpha^{n-1}}{a}\frac{\lambda}{(\lambda+1)^n}.$$

Replacing α (resp. λ) by $\dfrac{P+\sqrt{D}}{2}$ (resp. $\dfrac{P}{\sqrt{D}}$), we get

$$\frac{\alpha^{n-1}}{a}\frac{\lambda}{(\lambda+1)^n} = \frac{\left(\sqrt{D}\right)^{n-2}P}{2^{n-1}a\,(1+\lambda)}.$$

Finally, from $D \approx +\infty$, $\lambda \approx 0$ and a is appreciable we obtain $\dfrac{\alpha^{n-1}}{a}\dfrac{\lambda}{(\lambda+1)^n} \approx +\infty$ and it follows that $\dfrac{U_n}{n} \approx +\infty$. Therefore $U_n = \omega n$, where $\omega \approx +\infty$.

Concerning V_n, the fact that

$$V_n = \alpha^n\left(1+\left(\frac{\beta}{\alpha}\right)^n\right) = \alpha^n\left(1+(-1+\phi)^n\right)$$

implies $V_n = \omega n$ with $\omega \approx +\infty$ because $\left(1+(-1+\phi)^n\right) > 1$.

(C) $\dfrac{\beta}{\alpha} \not\approx \pm 1$: By (2–2), $U_n = \alpha^{n-1}\left(\dfrac{1-(\beta/\alpha)^n}{1-(\beta/\alpha)}\right)$ hence $U_n = \alpha^{n-1}a$, where a is appreciable. Therefore $U_n = \omega n$, where $\omega \approx +\infty$. $V_n = \alpha^n\left(1+\left(\dfrac{\beta}{\alpha}\right)^n\right) = \alpha^n a$ where a is appreciable, therefore $V_n = \omega n$ with $\omega \approx +\infty$, and the proof is complete. □

Lemma 2.4 *If n is of the form n_1n_2 with $n_1 > 1$ and $n_2 > 1$, then $\dfrac{|U_{n_1n_2}|}{|U_{n_1}|}$ and $\dfrac{|V_{n_1n_2}|}{|V_{n_1}|}$ are unlimited.*

Proof Since $n \approx +\infty$, at least one of n_1 and n_2 is unlimited. By (1–2)

$$\text{(2–3)} \qquad \begin{cases} \dfrac{U_{n_1n_2}}{U_{n_1}} &= \dfrac{\alpha^{n_1n_2}}{\alpha^{n_1}}\left(\dfrac{1-(\beta/\alpha)^{n_1n_2}}{1-(\beta/\alpha)^{n_1}}\right), \\ \dfrac{V_{n_1n_2}}{V_{n_1}} &= \dfrac{\alpha^{n_1n_2}}{\alpha^{n_1}}\left(\dfrac{1+(\beta/\alpha)^{n_1n_2}}{1+(\beta/\alpha)^{n_1}}\right). \end{cases}$$

We have three cases.

(A) $\dfrac{\beta}{\alpha} = 1-\phi$. By (2–3) and the fact that $1-\left(\dfrac{\beta}{\alpha}\right)^{n_1n_2} > 1-\left(\dfrac{\beta}{\alpha}\right)^{n_1} > 0$ we have

$$\frac{U_{n_1n_2}}{U_{n_1}} = \alpha^{n_1(n_2-1)}c = \alpha^{n-n_1}c,$$

where $c > 1$. Since $(n-n_1) \approx +\infty$ then $\dfrac{U_{n_1n_2}}{U_{n_1}} \approx +\infty$. Also by (2–3), $\dfrac{V_{n_1n_2}}{V_{n_1}} = \alpha^{n_1(n_2-1)}c = \alpha^{n-n_1}c$, where c is positive and appreciable. From the fact that $(n-n_1) \approx +\infty$ we have $\dfrac{V_{n_1n_2}}{V_{n_1}} \approx +\infty$.

(B) $\dfrac{\beta}{\alpha} = -1+\phi$. By Lemma 2.2, λ is positive infinitesimal. There are three subcases.

(1) n_1 is even. Then n_1n_2 is even and $\dfrac{U_{n_1n_2}}{U_{n_1}} = \alpha^{n_1(n_2-1)}c$ with $c > 1$ because $1-\left(\dfrac{\beta}{\alpha}\right)^{n_1n_2} > 1-\left(\dfrac{\beta}{\alpha}\right)^{n_1} > 0$. Hence $\dfrac{U_{n_1n_2}}{U_{n_1}} \approx +\infty$. Concerning V_n we have $\dfrac{V_{n_1n_2}}{V_{n_1}} = \dfrac{\alpha^{n_1n_2}}{\alpha^{n_1}}\left(\dfrac{1+(\beta/\alpha)^{n_1n_2}}{1+(\beta/\alpha)^{n_1}}\right)$. Since n_1 and n_1n_2 are even and $-1 < \beta/\alpha < 0$, then

$$\begin{aligned} \frac{V_{n_1n_2}}{V_{n_1}} &= \frac{\alpha^{n_1n_2}}{\alpha^{n_1}}c \\ &= \alpha^{n_1(n_2-1)}c \approx +\infty \end{aligned}$$

because c is positive and appreciable and $\alpha^{n_1(n_2-1)} \approx +\infty$.

(2) n_1 and n_2 are both odd. From $\dfrac{U_{n_1n_2}}{U_{n_1}} = \alpha^{n_1(n_2-1)}\dfrac{\left(1-(-1+\phi)^{n_1n_2}\right)}{\left(1-(-1+\phi)^{n_1}\right)}$ we have

$$\begin{aligned} \frac{U_{n_1n_2}}{U_{n_1}} &= \alpha^{n_1(n_2-1)}\frac{\left(1+(1-\phi)^{n_1n_2}\right)}{\left(1+(1-\phi)^{n_1}\right)} \\ &= \alpha^{n_1(n_2-1)}a \approx +\infty \end{aligned}$$

because a is positive and appreciable. Also

$$\begin{aligned}\frac{V_{n_1n_2}}{V_{n_1}} &= \alpha^{n_1(n_2-1)}\frac{\left(1+(-1+\phi)^{n_1n_2}\right)}{\left(1+(-1+\phi)^{n_1}\right)}\\ &= \alpha^{n_1(n_2-1)}\frac{\left(1-(1-\phi)^{n_1n_2}\right)}{\left(1-(1-\phi)^{n_1}\right)}\end{aligned}$$

Since $1-(1-\phi)^{n_1n_2} > 1-(1-\phi)^{n_1} > 0$, then $\frac{V_{n_1n_2}}{V_{n_1}} = \alpha^{n_1(n_2-1)}c$ with $c \geq 1$ which implies $\frac{V_{n_1n_2}}{V_{n_1}} \approx +\infty$ because $\alpha^{n_1(n_2-1)} \approx +\infty$.

(3) n_1 is odd, n_2 is even. Then $\frac{U_{n_1n_2}}{U_{n_1}} = \frac{\alpha^{n_1(n_2-1)}}{a}\left(1-\left(\frac{\beta}{\alpha}\right)^{n_1n_2}\right)$, where $a = \left(1-\left(\frac{\beta}{\alpha}\right)^{n_1}\right)$ is appreciable and strictly positive because $-1 < \left(\frac{\beta}{\alpha}\right)^{n_1} < 0$. Since λ is positive infinitesimal and $\frac{\beta}{\alpha} = \frac{\lambda-1}{\lambda+1}$ then

$$\frac{U_{n_1n_2}}{U_{n_1}} = \frac{\alpha^{n_1(n_2-1)}}{a}\left(1-\left(\frac{1-\lambda}{1+\lambda}\right)^{n_1n_2}\right).$$

Now

$$\begin{aligned}\frac{\alpha^{n_1(n_2-1)}}{a}\left(1-\left(\frac{1-\lambda}{1+\lambda}\right)^{n_1n_2}\right) &> \frac{\alpha^{n_1(n_2-1)}}{a}\left(1-\frac{1}{(1+\lambda)^{n_1n_2}}\right)\\ &> \frac{\alpha^{n_1(n_2-1)}}{a}\frac{n_1n_2\lambda}{(1+\lambda)^{n_1n_2}}.\end{aligned}$$

Replacing λ by $\frac{P}{\sqrt{D}}$, we get

$$\frac{\alpha^{n_1(n_2-1)}}{a}\frac{n_1n_2\lambda}{(1+\lambda)^{n_1n_2}} = \frac{n_1n_2P\left(\sqrt{D}\right)^{n_1n_2-1}}{\alpha^{n_1}a.2^{n_1n_2}}$$

which implies

$$\frac{\alpha^{n_1(n_2-1)}}{a}\frac{n_1n_2\lambda}{(1+\lambda)^{n_1n_2}} \geq \frac{n_1n_2P\left(\sqrt{D}\right)^{n_1n_2-n_1-1}}{a.2^{n_1n_2}}$$

because $\alpha < \sqrt{D}$. Since $\sqrt{D} > 2^3$,

$$\frac{n_1n_2P\left(\sqrt{D}\right)^{n_1n_2-n_1-1}}{a.2^{n_1n_2}} \geq \frac{n_1n_2P.2^{n_1(2n_2-3)-3}}{a}.$$

Therefore

$$\frac{\alpha^{n_1(n_2-1)}}{a}\frac{n_1n_2\lambda}{(1+\lambda)^{n_1n_2}} \geq \frac{n_1n_2P.2^{n_1(2n_2-3)-3}}{a} \approx +\infty$$

and then $\dfrac{U_{n_1n_2}}{U_{n_1}} \approx +\infty$.

Concerning $\dfrac{V_{n_1n_2}}{V_{n_1}}$, we have $\dfrac{V_{n_1n_2}}{V_{n_1}} = \alpha^{n_1(n_2-1)}\dfrac{\left(1+(1-\phi)^{n_1n_2}\right)}{\left(1-(1-\phi)^{n_1}\right)}$. The facts that $1+(1-\phi)^{n_1n_2}$ is appreciable, $1-(1-\phi)^{n_1} \in]0,1[$ and $\alpha^{n_1(n_2-1)} \approx +\infty$ lead to $\dfrac{V_{n_1n_2}}{V_{n_1}} \approx +\infty$.

(C) $\dfrac{\beta}{\alpha} \not\approx \pm 1$. The fact that $\dfrac{U_{n_1n_2}}{U_{n_1}} = \alpha^{n_1(n_2-1)}a$, $\dfrac{V_{n_1n_2}}{V_{n_1}} = \alpha^{n_1(n_2-1)}b$, where $\alpha^{n_1(n_2-1)} \approx +\infty$, a and b are appreciable and positive mean that $\dfrac{U_{n_1n_2}}{U_{n_1}} \approx +\infty$ and $\dfrac{V_{n_1n_2}}{V_{n_1}} \approx +\infty$ which finishes the proof. □

Lemma 2.5 *For every $i \geq 2$, $|U_i| < |U_{i+1}|$ & $|V_i| < |V_{i+1}|$.*

Proof Let $i \geq 2$. We have three cases.

(A) $\dfrac{\beta}{\alpha} = 1-\phi$. By Lemma 2.2, $\lambda \approx +\infty$ and then $\alpha \approx +\infty$. Now $\dfrac{U_{i+1}}{U_i} = \dfrac{\alpha^{i+1}-\beta^{i+1}}{\alpha^i-\beta^i} = \alpha\dfrac{\left(1-r^{i+1}\right)}{(1-r^i)}$, where $r = \dfrac{\beta}{\alpha} = 1-\phi$. Since $1-r^{i+1} > 1-r^i > 0$ and $\alpha \approx +\infty$, then $\dfrac{U_{i+1}}{U_i} > 1$. Also we have $\dfrac{V_{i+1}}{V_i} = \alpha\dfrac{\left(1+r^{i+1}\right)}{(1+r^i)}$. Since $\dfrac{\left(1+r^{i+1}\right)}{(1+r^i)}$ is appreciable and $\alpha \approx +\infty$, then $\dfrac{V_{i+1}}{V_i} \approx +\infty$. That is, $\dfrac{V_{i+1}}{V_i} > 1$.

(B) $\dfrac{\beta}{\alpha} = -1+\phi$. By Lemma 2.2, λ is positive infinitesimal. Since P is supposed positive and λ is positive infinitesimal, we directly get $Q \approx -\infty$. Therefore, from $Q < 0$, we obtain $0 < U_2 < U_3 < U_4 < \ldots$. Similarly, $0 < V_2 < V_3 < V_4 < \ldots$.

(C) $\dfrac{\beta}{\alpha} \not\approx \pm 1$. According to Lemma 2.2, λ is appreciable and strictly positive. $\dfrac{U_{i+1}}{U_i} = \alpha\dfrac{\left(1-r^{i+1}\right)}{(1-r^i)}$ with $r = \dfrac{\beta}{\alpha} = \dfrac{\lambda-1}{\lambda+1}$, where λ is different from 1 because otherwise $Q = 0$. We divide the rest of the proof into the following cases.

(1) $\lambda \in]0,1[$. Then $0 < \dfrac{P}{\sqrt{P^2-4Q}} < 1$ and consequently $Q < 0$. Hence, as in the case B) of this lemma, we have $0 < U_2 < U_3 < U_4 < \ldots$ and $0 < V_2 < V_3 < V_4 < \ldots$.

(2) $\lambda > 1$. Then r is appreciable and positive and $r < 1$. Since $\dfrac{U_{i+1}}{U_i} = \alpha\dfrac{\left(1-r^{i+1}\right)}{(1-r^i)}$ and $1-r^{i+1} > 1-r^i > 0$, then $\dfrac{U_{i+1}}{U_i} > \alpha > 1$. Concerning $\dfrac{V_{i+1}}{V_i}$, the fact that $\lambda = \dfrac{P}{\sqrt{P^2-4Q}} > 1$ implies $Q > 0$ and consequently $P \geq 3$ because $D = P^2 - 4Q > 0$. Then $\alpha \geq 2$ and $\beta > 0$ because $\beta = \dfrac{P-\sqrt{P^2-4Q}}{2}$. Therefore,

$$\alpha^i(\alpha-1) > \beta^i(1-\beta).$$

Indeed, if $0 < \beta \leq 1$, then $\beta^i \leq 1$ and $0 \leq 1-\beta < 1$ which implies $0 \leq \beta^i(1-\beta) < 1$. Moreover, $\alpha^i(\alpha-1) \geq 1$. Hence

$$\alpha^i(\alpha-1) > \beta^i(1-\beta)$$

which is evidently verified when $\beta > 1$. Therefore $\alpha^{i+1} + \beta^{i+1} > \alpha^i + \beta^i$; i.e. $V_{i+1} > V_i$ and the proof is complete. □

Lemma 2.6 *If (P,Q) is not standard then $\dfrac{|V_2|}{|V_1|} \approx +\infty$.*

Proof We have two cases.

(A) $P \approx +\infty$. We divide the proof of A) further into the following cases.

(1) Q standard. Then $\dfrac{V_2}{V_1} = \dfrac{P^2-2Q}{P} \approx +\infty$.

(2) $Q \approx -\infty$. Then $\dfrac{V_2}{V_1} = \dfrac{P^2-2Q}{P} \approx +\infty$.

(3) $Q \approx +\infty$. Suppose that $\dfrac{V_2}{V_1} = l$ with l being limited. Then $\dfrac{P^2-2Q}{P} = l > 0$ ($P^2-2Q > 0$ because $D > 0$). Hence $P^2 - Pl = 2Q$ which implies $Q = \dfrac{1}{2}\left(P^2 - Pl\right)$. Then

$$D = P^2 - 4Q = P^2 - 2\left(P^2 - Pl\right) = -P^2 + 2Pl$$

which means that $D < 0$ and this is a contradiction. Then $\dfrac{V_2}{V_1} \approx +\infty$.

(B) P standard. In this case $Q \approx -\infty$ and we show easily that $\dfrac{V_2}{V_1} \approx +\infty$. This finishes the proof. □

Lemma 2.7 *n may be written according to one and only one of the following forms.*

(i) $n = p \approx +\infty$ *is a prime.*

(ii) $n = 2^s p$, *where* $s \geq 1$ *is a limited and* $p \approx +\infty$ *is a prime.*

(iii) $n = n_1 n_2$ *where one of* n_1, n_2 *is odd greater than or equal to* 3, *the other is unlimited.*

(iv) $n = 2^{\omega+1}$ *with* $\omega \approx +\infty$.

Proof It is well-known that n must be written uniquely as $t_1^{\alpha_1} t_2^{\alpha_2} ... t_r^{\alpha_r}$, where $2 \leq t_1 < t_2 < .. < t_r$ are prime numbers, $\alpha_i \geq 1$ $(i = 1, 2, ..., r)$. Two cases arise.

(1) $r = 1$. Either $t_1 = 2$, in which case n is of the fourth form, or $t_1 > 2$ which implies that n is of the first form if $\alpha_1 = 1$ because in this case $n = t_1$, otherwise ($\alpha_1 > 1$), $n = t_1^{\alpha_1} = t_1 t_1^{\alpha_1 - 1}$ which shows that n is of the third form because the quantities t_1 and $t_1^{\alpha_1 - 1}$ are both odd and obviously at least one of them is unlimited.

(2) $r > 1$. Here two subcases arise.

a) $t_1 = 2$.

If α_1 is limited, then we divide the proof into two further cases.

(a1) $\alpha_2 = 1$. If $r = 2$, then $n = 2^{\alpha_1} t_2$ which shows that t_2 is unlimited and consequently n is of the second form, otherwise (i.e. $r > 2$) the fact that $n = 2^{\alpha_1} t_2 t_3^{\alpha_3} ... t_r^{\alpha_r}$ where t_2 is odd and $2^{\alpha_1} t_3^{\alpha_3} ... t_r^{\alpha_r} \approx +\infty$ because $2^{\alpha_1} t_3^{\alpha_3} ... t_r^{\alpha_r} > t_2$ and the product $t_2 . 2^{\alpha_1} t_3^{\alpha_3} ... t_r^{\alpha_r} = n \approx +\infty$, shows that n is of the third form.

(a2) $\alpha_2 > 1$. In this case n is of the third form because $n = 2^{\alpha_1} t_2^{\alpha_2} t_3^{\alpha_3} ... t_r^{\alpha_r} = t_2 . 2^{\alpha_1} t_2^{\alpha_2 - 1} t_3^{\alpha_3} ... t_r^{\alpha_r}$ where t_2 is odd and by the same reasoning as (a1) above, $r > 2$) $2^{\alpha_1} t_2^{\alpha_2 - 1} t_3^{\alpha_3} ... t_r^{\alpha_r} \approx +\infty$.

If α_1 is unlimited, then the fact that $n = 2^{\alpha_1} t_2^{\alpha_2} t_3^{\alpha_3} ... t_r^{\alpha_r} = t_2 . 2^{\alpha_1} t_2^{\alpha_2 - 1} t_3^{\alpha_3} ... t_r^{\alpha_r}$, where t_2 is odd and $2^{\alpha_1} t_2^{\alpha_2 - 1} t_3^{\alpha_3} ... t_r^{\alpha_r} \approx +\infty$ permits us to conclude that n is of the third form.

(b) $t_1 > 2$. Here also, using the same reasoning as above and the fact that $n = t_1^{\alpha_1} t_2^{\alpha_2} ... t_r^{\alpha_r} = t_1 t_1^{\alpha_1 - 1} t_2^{\alpha_2} ... t_r^{\alpha_r} \approx +\infty$, we conclude that n is of the third form.

We now prove that n cannot be written simultaneously according to two of the above indicated forms. Indeed, we prove this for the second and the third form (the other cases are trivial). Suppose that $n = 2^s p$ where $s \geq 1$ is a limited and $p \approx +\infty$ is a prime and also $n = n_1 n_2$, where for example n_1 is odd greater than or equal to 3 and n_2 is unlimited. Since the decomposition of n in prime factors is unique, then $n_1 = p$, $n_2 = 2^s$ which is contradictory because n_2 is unlimited and cannot be equal to 2^s. □

3 Proof of Theorem 2.1.

3.1 Proof for U_n.

We consider the following two subcases.

(I) n is a prime. By (1–5), $U_n = \left(\frac{D}{n}\right) mod\,(n)$. Then $U_n = u + kn$, where $u \in \{-1, 0, +1\}$. Since $|U_n|$ is, according to Lemma 2.3, of the form ωn with ω is an unlimited real number, the integer k must be unlimited. Consequently the proof is finished for this case.

(II) n is a composite i.e. $n = n_1 n_2$, where $n_1 \geq n_2 > 1$. By (1–6), $U_n = CU_{n_1}$, where C is an integer which is, according to Lemma 2.4, unlimited. On the other hand since $n_1 \approx +\infty$, then by Lemma 2.5, U_{n_1} is unlimited. Thus the proof is finished for U_n.

3.2 Proof for V_n

By Lemma 2.7, we need to consider the following four cases.

(I) $n = p \approx +\infty$ is a prime. We have two subcases to consider.

(a) P limited. By (1–5), $V_p = P\ mod(p)$; i.e. $V_p = P + kp$. Since P is limited, k must be, according to Lemma 2.3, unlimited.

(b) P unlimited. According to (1–6), $V_1 \mid V_p$; i.e $V_p = V_1 N$. By Lemma 2.5, we have

$$|V_2| < |V_3| < ... < |V_n| < ... .$$

By Lemma 2.6, $\frac{|V_2|}{|V_1|} \approx +\infty$ which implies from $\frac{|V_2|}{|V_1|} < \frac{|V_p|}{|V_1|}$ that $\frac{|V_p|}{|V_1|} \approx +\infty$ and then N is unlimited. Thus the proof is finished for this case because $V_1 = P$ and $|P| \approx +\infty$.

(II) $n = 2^s p$, where $s \geq 1$ is a limited and $p \approx +\infty$ is a prime.

(a) P and Q are both limited. For $s \geq 1$ define the formula

$A(s) \equiv$ "For n of the form $2^s p$, V_n may be written as $g_1 + g_2 p$ where g_1 (resp. g_2) is a limited (resp. is an unlimited) integer".

We have $A(1)$. Indeed, let $n = 2p$; by (1–4)

$$V_n = V_{2p} = \left(V_p\right)^2 - 2Q^p.$$

Applying (1–5) and (1–8) yields $V_{2p} = (P + kp)^2 - 2(Q + lp)$. Hence

$$\begin{aligned} V_n &= V_{2p} = P^2 + 2Pkp + k^2p^2 - 2Q - 2lp \\ &= P^2 - 2Q + \left(2Pk + k^2p - 2l\right)p. \end{aligned}$$

If $g_1 = P^2 - 2Q$ and $g_2 = 2Pk + k^2p - 2l$, then g_1 is limited and, according to Lemma 2.3, g_2 is unlimited. Consequently, $A(1)$.

Suppose $A(s)$ for $s \geq 1$ a limited integer and prove $A(s+1)$. Indeed, by (1–4)

$$V_{2^{s+1}p} = V_{2(2^sp)} = \left(V_{2^sp}\right)^2 - 2Q^{2^sp}.$$

From $A(s)$ (resp. (1–8)) we have $V_{2^sp} = g_1 + g_2p$, where g_1 is limited and g_2 is unlimited (resp. $Q^{2^sp} = \left(Q^{2^s}\right)^p = Q^{2^s} + fp$ with f an integer). Replacing by these values, we get

$$\begin{aligned} V_{2^{s+1}p} &= \left(V_{2^sp}\right)^2 - 2Q^{2^sp} \\ &= (g_1 + g_2p)^2 - 2\left(Q^{2^s} + fp\right) \\ &= g_1^2 - 2Q^{2^s} + \bar{f}p, \end{aligned}$$

where $\bar{f} = 2g_1g_2 + g_2^2p - 2f$. Since g_1, Q and s are limited, then $g_1^2 - 2Q^{2^s}$ is limited; the integer $\bar{f}$, according to Lemma 2.3, must be unlimited. Consequently, $A(s+1)$.

Then by (1–9),

$$\forall^{st} s \geq 1 \quad A(s).$$

(b) P or Q is unlimited. By (1–6), $V_{2^s} | V_{2^sp}$, i.e. $V_{2^sp} = V_{2^s}c$ with c being an integer. By Lemma 2.4, c is unlimited. By Lemma 2.6, $|V_2| \approx +\infty$ and by Lemma 2.5, $|V_2| < |V_3| < |V_4| < \ldots$. Hence V_{2^s} is unlimited. This completes the proof for this case.

(III) $n = n_1n_2$, where one of n_1, n_2 is odd greater than or equal to 3, the other is unlimited.

Suppose $n_1 \geq 3$ is odd and $n_2 \approx +\infty$. Then

$$V_{n_1n_2} = V_{n_2}C,$$

where by (1–6) C is an integer which is, according to Lemma 2.4., unlimited. Since $n_2 \approx +\infty$, then by Lemma 2.5 V_{n_2} is unlimited. This finishes the proof for this case.

(IV) $n = 2^{\omega+1}$ with $\omega \approx +\infty$.

(a) Q is even ($Q = 2t$, $t \in \mathbb{Z}^*$). By (1–4), we have

$$V_n = V_{2^{\omega+1}} = V_{2.2^\omega} = V_{2^\omega}^2 - 2Q^{2^\omega}.$$

Applying the fact that $2^{\omega} = 2.2^{\omega-1}$ and (1–4) yield

$$V_{2^{\omega}} = V_{2.2^{\omega-1}} = V_{2^{\omega-1}}^2 - 2Q^{2^{\omega-1}}$$

which, when substituted in $V_n = V_{2^{\omega}}^2 - 2Q^{2^{\omega}}$, gives

$$\begin{aligned} V_n &= V_{2^{\omega+1}} = \left(V_{2^{\omega-1}}^2 - 2Q^{2^{\omega-1}}\right)^2 - 2Q^{2^{\omega}} \\ &= \left(V_{2^{\omega-1}}\right)^4 mod\left(Q^{2^{\omega-1}}\right). \end{aligned} \tag{3–1}$$

Similarly, the fact that $V_{2^{\omega-1}} = V_{2.2^{\omega-2}}$ and (1–4) give

$$V_n = V_{2^{\omega+1}} = \left(V_{2^{\omega-2}}\right)^8 mod\left(Q^{2^{\omega-2}}\right) \tag{3–2}$$

and so on.

Let $f \approx +\infty$ be an integer such that $\omega - f \approx +\infty$. The previous process permits to write

$$V_n = V_{2^{\omega+1}} = \left(V_{2^{\omega-f}}\right)^{2^{f+1}} mod\left(Q^{2^{\omega-f}}\right), \tag{3–3}$$

where $V_{2^{\omega-f}}$ is unlimited.

Now, if $V_{2^{\omega-f}}$ is even then $V_{2^{\omega+1}} = 2^{\gamma}t$, where $\gamma = \min\left(2^{f+1}, 2^{\omega-f}\right) \approx +\infty$ and t is an integer. This shows that

$$V_n = V_{2^{\omega+1}} = 2^{\gamma_1}2^{\gamma_2}t,$$

where γ_1 and γ_2 are two unlimited integers satisfying $\gamma_1 + \gamma_2 = \gamma$. Otherwise (i.e. $V_{2^{\omega-f}}$ is odd), we have

$$V_n - 1 = \left[\left(V_{2^{\omega-f}}\right)^{2^{f+1}} - 1\right] + kQ^{2^{\omega-f}}.$$

Since $\left(V_{2^{\omega-f}}\right)^{2^{f+1}} - 1$ is a difference between squares, then

$$V_n - 1 = \left[\left(V_{2^{\omega-f}}\right)^{2^f} - 1\right]\left[\left(V_{2^{\omega-f}}\right)^{2^f} + 1\right] + kQ^{2^{\omega-f}}.$$

By the same reasoning about the difference $\left(V_{2^{\omega-f}}\right)^{2^f} - 1$

$$V_n - 1 = \left[\left(V_{2^{\omega-f}}\right)^{2^{f-1}} - 1\right]\left[\left(V_{2^{\omega-f}}\right)^{2^{f-1}} + 1\right]\left[\left(V_{2^{\omega-f}}\right)^{2^f} + 1\right] + kQ^{2^{\omega-f}}$$

and so on. Thus we can write $V_n - 1$ as

$$\begin{aligned} V_n - 1 = &\left[\left(V_{2^{\omega-f}}\right)^{2^{f-t}} - 1\right]\left[\left(V_{2^{\omega-f}}\right)^{2^{f-t}} + 1\right]\left[\left(V_{2^{\omega-f}}\right)^{2^{f-(t-1)}} + 1\right] + \ldots \\ &+ \left[\left(V_{2^{\omega-f}}\right)^{2^{f-1}} + 1\right]\left[\left(V_{2^{\omega-f}}\right)^{2^f} + 1\right] + kQ^{2^{\omega-f}}, \end{aligned}$$

where t is an integer satisfying $1 \leq t < f$. Now choose $t_0 \approx +\infty$ such that $t_0 < f$ and $t_0 + 2 < 2^{\omega-f}$. This is possible because, from the fact that $\min\left(f, 2^{\omega-f}\right) \approx +\infty$, we can choose an integer $s \approx +\infty$ such that $s \leq \min\left(f, 2^{\omega-f}\right)$ and take thereafter $t_0 = s - 3$. Since $Q^{2^{\omega-f}}$ contains the factor $2^{2^{\omega-f}}$ and the product $\left[\left(V_{2^{\omega-f}}\right)^{2^{f-t_0}} - 1\right] \prod_{i=0}^{t_0} \left[\left(V_{2^{\omega-f}}\right)^{2^{f-i}} + 1\right]$ contains 2^k with $k \geq t_0 + 2$, then

$$V_n - 1 = 2^{t_0+2}N,$$

where N is an integer. Therefore

$$V_n - 1 = V_{2^{\omega+1}} - 1 = 2^{t_1}2^{t_2}N,$$

where t_1 and t_2 are two unlimited integers satisfying $t_1 + t_2 = t_0 + 2$.

(b) Q is odd ($Q = 2t + 1$, $t \in \mathbb{Z}$). We put $n_o = 2^\omega$. If $Q = \pm 1$, then by (1–4)

$$\begin{aligned} V_n = V_{2n_0} &= \left(V_{n_0}\right)^2 - 2Q^{n_0} \\ &= \left(V_{n_0}\right)^2 - 2 \end{aligned}$$

because n_0 is even. V_{n_0} is, by Lemma 2.3, unlimited. Otherwise (i.e. $Q \neq \pm 1$) we divide the proof into the following cases.

(1) P is even. By (1–3) and the induction, we show easily that each V_l ($l \geq 0$) is even. Moreover $V_2 \neq 2$, because otherwise $P^2 - 2Q = 2$ which implies $D = P^2 - 4Q = 2 - 2Q$. The fact that $D > 0$ implies that $2 - 2Q > 0$ i.e. $Q < 0$ (because $Q \in \mathbb{Z}^*$) and this contradicts $P^2 - 2Q = 2$. In the same way $V_2 \neq -2$.

Now, we prove that $V_n - 2$ is the product of two unlimited integers. Indeed, by (1–4)

$$V_n = V_{2^{\omega+1}} = V_{2n_0} = V_{n_0}^2 - 2Q^{n_0}.$$

Then

$$\begin{aligned} V_n - 2 &= V_{n_0}^2 - 4 - 2Q^{n_0} + 2 \\ &= \left(V_{n_0} - 2\right)\left(V_{n_0} + 2\right) - 2\left(Q^{n_0} - 1\right) \end{aligned}$$

which implies

$$V_n - 2 = \left(V_{n_0} - 2\right)\left(V_{n_0} + 2\right) - 2\left(Q^{n_0/2} - 1\right)\left(Q^{n_0/2} + 1\right). \tag{3–4}$$

Because n_0 is divisible by 2, then applying (1–4) shows that $V_{n_0} - 2$ can be written as

$$V_{n_0} - 2 = V_{2(n_0/2)} - 2 = V_{(n_0/2)}^2 - 4 - 2\left(Q^{n_0/2} - 1\right)$$

which, when substituted in (3–4), gives

$$V_n - 2 = \left[V_{(n_0/2)}^2 - 4 - 2\left(Q^{n_0/2} - 1\right)\right]\left(V_{n_0} + 2\right) - 2\left(Q^{n_0/2} - 1\right)\left(Q^{n_0/2} + 1\right).$$

Hence,

$$\begin{aligned} V_n - 2 &= \left(V_{(n_0/2)} - 2\right)\left(V_{(n_0/2)} + 2\right)\left(V_{n_0} + 2\right) \\ &\quad -2\left(Q^{n_0/4} - 1\right)\left(Q^{n_0/4} + 1\right)\left(V_{n_0} + 2\right) \\ &\quad -2\left(Q^{n_0/4} - 1\right)\left(Q^{n_0/4} + 1\right)\left(Q^{n_0/2} + 1\right). \end{aligned} \tag{3–5}$$

Because $n_0/2$ is divisible by 2, then applying (1–4) shows that $V_{n_0/2} - 2$ can be written as

$$\begin{aligned} V_{(n_0/2)} - 2 &= V^2_{(n_0/4)} - 2Q^{n_0/4} - 4 + 2 \\ &= \left(V^2_{(n_0/4)} - 4\right) - 2\left(Q^{n_0/4} - 1\right) \end{aligned}$$

which, when substituted in (3–5), gives

$$\begin{aligned} V_{2n_0} - 2 &= \left(V_{(n_0/4)} - 2\right)\left(V_{(n_0/4)} + 2\right)\left(V_{(n_0/2)} + 2\right)\left(V_{n_0} + 2\right) \\ &\quad -2\left(Q^{n_0/8} - 1\right)\left(Q^{n_0/8} + 1\right)\left(V_{(n_0/2)} + 2\right)\left(V_{n_0} + 2\right) \\ &\quad -2\left(Q^{n_0/8} - 1\right)\left(Q^{n_0/8} + 1\right)\left(Q^{n_0/4} + 1\right)\left(V_{n_0} + 2\right) \\ &\quad -2\left(Q^{n_0/8} - 1\right)\left(Q^{n_0/8} + 1\right)\left(Q^{n_0/4} + 1\right)\left(Q^{n_0/2} + 1\right) \end{aligned} \tag{3–6}$$

and so on.

So the process of applying (1–4) and putting the difference between squares as a product of two factors, yields by induction

$$\begin{aligned} &V_n - 2 = V_{2n_0} - 2 \\ &= \left(V_{n_0/2^{i-1}} - 2\right)\left(V_{n_0/2^{i-1}} + 2\right) \ldots \left(V_{n_0/2} + 2\right)\left(V_{n_0} + 2\right) \\ &\quad -2\left(Q^{n_0/2^i} - 1\right)\left(Q^{n_0/2^i} + 1\right)\left(V_{n_0/2^{i-2}} + 2\right) \ldots \left(V_{n_0/2} + 2\right)\left(V_{n_0} + 2\right) \\ &\quad -2\left(Q^{n_0/2^i} - 1\right)\left(Q^{n_0/2^i} + 1\right)\left(Q^{n_0/2^{i-1}} + 1\right)\left(V_{n_0/2^{i-3}} + 2\right) .. \left(V_{n_0} + 2\right) \\ &\quad -2\left(Q^{n_0/2^i} - 1\right)\left(Q^{n_0/2^i} + 1\right)\left(Q^{n_0/2^{i-1}} + 1\right)\left(Q^{n_0/2^{i-2}} + 1\right)\left(V_{n_0/2^{i-4}} + 2\right) \ldots \left(V_{n_0} + 2\right) \\ &\quad \ldots\ldots \\ &\quad -2\left(Q^{n_0/2^i} - 1\right)\left(Q^{n_0/2^i} + 1\right)\left(Q^{n_0/2^{i-1}} + 1\right) \ldots \left(Q^{n_0/2^2} + 1\right)\left(V_{n_0} + 2\right) \\ &\quad -2\left(Q^{n_0/2^i} - 1\right)\left(Q^{n_0/2^i} + 1\right)\left(Q^{n_0/2^{i-1}} + 1\right) \ldots \left(Q^{n_0/2^2} + 1\right)\left(Q^{n_0/2} + 1\right), \end{aligned} \tag{3–7}$$

where $1 \leq i \leq \omega$. In this formula, if we replace i by 1 we recover (3–4), by 2 we recover (3–5), etc.

We take $i_0 \approx +\infty$ such that $\dfrac{n_0}{2^{i_0}} \geq 1$.We show that $V_n - 2$ is of the form $2^{i_0+1}t$, where t is an integer. Indeed, each element $V_{n_0/2^j}$ $(0 \leq j \leq i_0 - 1)$ is even and, according to Lemma 2.5, different from ± 2 giving the fact that V_2 is different from these values. On the other hand Q is odd and different from ± 1. Hence the formula (3–7) is the sum of $i_0 + 1$ terms, where each term is the product of $i_0 + 1$ non-zero even integers. Therefore

$$V_n - 2 = 2^{i_0+1}t = 2^{t_1}2^{t_2}t,$$

where t_1 and t_2 are two unlimited integers satisfying $t_1 + t_2 = i_0 + 1$ and t is an integer.

(2) P is odd. We prove by induction that V_{2^l} $(l \geq 1)$ is odd. Indeed, $V_{2^1} = P^2 - 2Q$ this shows that V_2 is odd. Now suppose that V_{2^l} is odd with $l \geq 1$. Then $V_{2^{l+1}} = \left(V_{2^l}\right)^2 - 2Q^{2^l}$ so $V_{2^{l+1}}$ is also odd. On the other hand $V_2 \neq 1$, otherwise $P^2 - 2Q = 1$ then the fact that $D = P^2 - 4Q = 1 - 2Q > 0$ implies that $Q < 0$ and this contradicts $P^2 - 2Q = 1$. In the same way $V_2 \neq -1$.

By (1–4)

$$V_n = V_{2^{\omega+1}} = V_{2n_0} = V_{n_0}^2 - 2Q^{n_0}$$

Then

$$V_n + 1 = V_{n_0}^2 - 1 + 2 - 2Q^{n_0} = \left(V_{n_0} - 1\right)\left(V_{n_0} + 1\right) + 2\left(1 - Q^{n_0}\right)$$

So

$$V_n + 1 = \left(V_{n_0} + 1\right)\left(V_{n_0} - 1\right) + 2\left(1 - Q^{n_0/2}\right)\left(1 + Q^{n_0/2}\right). \tag{3–8}$$

By (1–4)

$$\begin{aligned} V_{n_0} + 1 &= V_{2(n_0/2)} + 1 \\ &= \left[V_{(n_0/2)}^2 - 1 + 2 - 2Q^{(n_0/2)}\right] \\ &= \left[\left(V_{(n_0/2)} - 1\right)\left(V_{(n_0/2)} + 1\right) + 2\left(1 - Q^{(n_0/2)}\right)\right] \end{aligned}$$

which, when substituted in (3–8), gives

$$\begin{aligned} V_n + 1 &= \left[\left(V_{(n_0/2)} - 1\right)\left(V_{(n_0/2)} + 1\right) + 2\left(1 - Q^{(n_0/2)}\right)\right]\left(V_{n_0} - 1\right) \\ &\qquad +2\left(1 - Q^{n_0/2}\right)\left(1 + Q^{n_0/2}\right) \\ &= \left(V_{(n_0/2)} - 1\right)\left(V_{(n_0/2)} + 1\right)\left(V_{n_0} - 1\right) + 2\left(1 - Q^{(n_0/2)}\right)\left(V_{n_0} - 1\right) \\ &\qquad +2\left(1 - Q^{(n_0/2)}\right)\left(1 + Q^{(n_0/2)}\right) \end{aligned}$$

Then

$$\begin{aligned} V_n+1 &= \left(V_{(n_0/2)}-1\right)\left(V_{(n_0/2)}+1\right)\left(V_{n_0}-1\right) \\ &+2\left(1-Q^{(n_0/4)}\right)\left(1+Q^{(n_0/4)}\right)\left(V_{n_0}-1\right) \\ &+2\left(1-Q^{(n_0/4)}\right)\left(1+Q^{(n_0/4)}\right)\left(1+Q^{(n_0/2)}\right) \end{aligned} \tag{3–9}$$

Again, setting $\frac{n_0}{2}=2.\frac{n_0}{4}$ and calculating by (1–4) an expression for $V_{(n_0/2)}+1$ and substituting in (3–9), we get another formula for V_n+1, and so on.

So this process yields by induction

$$\begin{aligned} &V_n+1=V_{2^{\omega+1}}+1 \\ &=\left(V_{n_0/2^i}+1\right)\left(V_{n_0/2^i}-1\right)\left(V_{n_0/2^{i-1}}-1\right)\ldots\left(V_{n_0/2}-1\right)\left(V_{n_0}-1\right) \\ &+2\left(1-Q^{n_0/2^{i+1}}\right)\left(1+Q^{n_0/2^{i+1}}\right)\left(V_{n_0/2^{i-1}}-1\right)\left(V_{n_0/2^{i-2}}-1\right)\ldots\left(V_{n_0}-1\right) \\ &+2\left(1-Q^{n_0/2^{i+1}}\right)\left(1+Q^{n_0/2^{i+1}}\right)\left(1+Q^{n_0/2^i}\right)\left(V_{n_0/2^{i-2}}-1\right)\ldots\left(V_{n_0}-1\right) \\ &+2\left(1-Q^{n_0/2^{i+1}}\right)\left(1+Q^{n_0/2^{i+1}}\right)\left(1+Q^{n_0/2^i}\right)\left(1+Q^{n_0/2^{i-1}}\right)\left(V_{n_0/2^{i-3}}-1\right)..\left(V_{n_0}-1\right)+ \\ &\cdots \\ &+2\left(1-Q^{n_0/2^{i+1}}\right)\left(1+Q^{n_0/2^{i+1}}\right)\left(1+Q^{n_0/2^i}\right)\left(1+Q^{n_0/2^{i-1}}\right)\cdots\left(1+Q^{n_0/2^2}\right)\left(V_{n_0}-1\right) \\ &+2\left(1-Q^{n_0/2^{i+1}}\right)\left(1+Q^{n_0/2^{i+1}}\right)\left(1+Q^{n_0/2^i}\right)\left(1+Q^{n_0/2^{i-1}}\right)\ldots\left(1+Q^{n_0/2}\right), \end{aligned} \tag{3–10}$$

where $0\leq i\leq\omega-1$. In this formula, if we replace i by 0 we recover (3–8), by 1 we recover (3–9) etc... .

We take $i_0\approx+\infty$ such that $\frac{n_0}{2^{i_0}}\geq 2$. We show that V_n+1 is of the form $2^{i_0+2}t$, where t is an integer. Indeed, each element $V_{n_0/2^j}$ $(0\leq j\leq i_0)$ is odd and, according to Lemma 2.5, different from ±1 giving the fact that V_2 is different from these values. On the other hand Q is odd and different from ±1. Hence the formula (3–10) is the sum of i_0+2 terms, where each term is the product of i_0+2 non-zero even integers. From this

$$V_n+1=V_{2n_0}+1=2^{t_1}2^{t_2}t,$$

where t_1 and t_2 are two unlimited integers satisfying $t_1+t_2=i_0+2$ and t is an integer. This finishes the proof of this case and therefore the theorem.

4 In classical terms

In order to find the classical equivalence of our result we use the reduction algorithm of external formulas of Nelson [5]. We denote the standard set

$$\left\{(P,Q)\in\left(\mathbb{Z}^*\right)^2\ :\ P^2-4Q>0\right\}$$

by H. Theorem 2.1 may be written as

$$\forall n\ \forall(P,Q)$$

$$\left[\begin{array}{l}\left(\forall^{st}t:n\geq t\right)\Rightarrow\exists^{st}(U,V)\,\exists\left(l_1,l_2,l_1',l_2'\right)\forall^{st}i\in\mathbb{N}\\ \qquad\left(U_n=U+l_1l_2,V_n=V+l_1'l_2'\ \&\ \min\left(\left|l_1\right|,\left|l_2\right|,\left|l_1'\right|,\left|l_2'\right|\right)>i\right)\end{array}\right],$$

where n, t, i range over $\mathbb{N}$, (P,Q) range over H and $U,V,\ l_1,l_2,l_1',l_2'$ range over $\mathbb{Z}$. Using idealization, this formula is equivalent to

$$\forall n\forall(P,Q)$$

$$\left[\begin{array}{l}\left(\forall^{st}t:n\geq t\right)\Rightarrow\exists^{st}(U,V)\,\forall^{stfini}I\,\exists\left(l_1,l_2,l_1',l_2'\right)\forall i\in I\\ \qquad\left(U_n=U+l_1l_2,V_n=V+l_1'l_2'\ \&\ \min\left(\left|l_1\right|,\left|l_2\right|,\left|l_1'\right|,\left|l_2'\right|\right)>i\right)\end{array}\right],$$

where I belongs to $\mathcal{P}_f(\mathbb{N})$ the set of finite subsets of $\mathbb{N}$. This formula is equivalent to

$$\forall(n,(P,Q))\ \exists^{st}(t,(U,V))\ \forall^{stfini}I$$

$$\left[\begin{array}{l}(n\geq t)\Rightarrow\exists\left(l_1,l_2,l_1',l_2'\right)\forall i\in I\\ \qquad\left(U_n=U+l_1l_2,V_n=V+l_1'l_2'\ \&\ min\left(\left|l_1\right|,\left|l_2\right|,\left|l_1'\right|,\left|l_2'\right|\right)>i\right)\end{array}\right].$$

If we refer to $\forall\exists^{st}\forall^{st}$ in the lexicon cited in [5], the last formula is equivalent to

$$\forall\widetilde{I}\ \exists^{fini}\mathcal{R}\forall(n,(P,Q))\ \exists(t,(U,V))\in\mathcal{R}$$

$$\left[\begin{array}{l}(n\geq t)\Rightarrow\exists\left(l_1,l_2,l_1',l_2'\right)\forall i\in\widetilde{I}(t,(U,V))\\ \left(U_n=U+l_1l_2,V_n=V+l_1'l_2'\ \&\ \min\left(\left|l_1\right|,\left|l_2\right|,\left|l_1'\right|,\left|l_2'\right|\right)>i\right)\end{array}\right],$$

(4–1)

where $\widetilde{I}$ is a mapping that associates with each $(t,(U,V))\in\mathbb{N}\times\mathbb{Z}^2$ a finite subset $\widetilde{I}(t,(U,V))\subset\mathbb{N}$. Now we prove that (4–1) is equivalent to

$$\forall \widetilde{I}\ \exists (T,W) \in \mathbb{N}^2\ \forall (n,(P,Q))\ \exists (t,(U,V)) \in [0,T] \times [-W,W]^2$$

$$\left[\begin{array}{l} (n \geq t) \Rightarrow \exists \left(l_1, l_2, l_1', l_2'\right) \forall i \in \widetilde{I}(t,(U,V)) \\ \left(U_n = U + l_1 l_2, V_n = V + l_1' l_2' \ \&\ \min\left(|l_1|, |l_2|, \left|l_1'\right|, \left|l_2'\right|\right) > i\right) \end{array} \right].$$

(4–2)

Indeed, let $\widetilde{I} : \mathbb{N} \times \mathbb{Z}^2 \to \mathcal{P}_f(\mathbb{N})$ be a set-valued mapping. Then according to (4–1) $\exists^{fini}\mathcal{R} \subset \mathbb{N} \times \mathbb{Z}^2$ and therefore there exist smaller integers T and W such that $\mathcal{R} \subset [0,T] \times [-W,W]^2$. Let $(n,(P,Q)) \in \mathbb{N} \times H$, by (4–1) $\exists (t,(U,V)) \in \mathcal{R} \subset [0,T] \times [-W,W]^2$; that is, $(t,(U,V)) \in [0,T] \times [-W,W]^2$. Now if $n \geq t$, then $\exists \left(l_1, l_2, l_1', l_2'\right) \forall i \in \widetilde{I}(t,(U,V))$

$U_n = U + l_1 l_2, V_n = V + l_1' l_2' \& \min\left(|l_1|, |l_2|, \left|l_1'\right|, \left|l_2'\right|\right) > i$ which shows that (4–1)$\Rightarrow$(4–2). For the converse one takes, $\mathcal{R} = [0,T] \times [-W,W]^2$.

Hence we have the following internal formulation of Theorem 2.1.

Proposition 4.1 *For any set-valued mapping $\widetilde{I} : \mathbb{N} \times \mathbb{Z}^2 \to P_f(\mathbb{N})$ there exists $(T,W) \in \mathbb{N}^2$ such that for all $(n,(P,Q)) \in \mathbb{N} \times H$ there exists $(t,(U,V)) \in [0,T] \times [-W,W]^2$ such that if $n \geq t$, then U_n (resp. V_n) differs by U (resp. V) from a product of two integers whose absolute value is greater than or equal to i for all $i \in \widetilde{I}(t,(U,V))$.*

Below we formulate, from the proof of Theorem 2.1, two particular cases of that result, and give their reductions separately.

(1) U_n differs from a product of two unlimited integers by an integer U with $-1 \leq U \leq 1$.

(2) If n is not of the form $2^s p$ with $s \geq 0$ being a limited integer and $p \approx +\infty$ being a prime, then V_n differs from a product of two unlimited integers by an integer V with $-2 \leq V \leq 2$.

The reductions of these particular cases are as follows.

(1) The first is equivalent to

$$\forall n \forall (P,Q) \left[\begin{array}{c} \left(\forall^{st} t : n \geq t\right) \Longrightarrow \exists (U,l_1,l_2) \forall^{st} i \\ \left(U_n(P,Q) = U + l_1 l_2 : |U| \leq 1\ \&\ \min\left(|l_1|, |l_2|\right) \geq i\right) \end{array} \right],$$

where n, t, $i \in \mathbb{N}$, $(U,l_1,l_2) \in \mathbb{Z}^3$. By idealization and transfer the previous formula transforms, while remaining equivalent, to

$$\forall^{fini} I\ \exists^{fini} T\ \forall (n,(P,Q))\,\exists t \in T$$

$$\left[\begin{array}{c} n \geq t \Longrightarrow \exists (U,l_1,l_2)\,\forall i \in I \\ \left(U_n(P,Q) = U + l_1 l_2 : |U| \leq 1\ \&\ \min\left(|l_1|,|l_2|\right) \geq i\right) \end{array}\right], \tag{4–3}$$

where I and T belong to the power set of $\mathbb{N}$. (4–3) is equivalent to

$$\forall i \in \mathbb{N}\ \exists \widetilde{T} \in \mathbb{N}\ \forall (n,(P,Q)) \in \mathbb{N}\times H$$

$$\left[\begin{array}{c} n \geq \widetilde{T} \Longrightarrow \\ \exists (U,l_1,l_2)\ \ \left(U_n(P,Q) = U + l_1 l_2 \text{ with } |U| \leq 1\ \&\ \min\left(|l_1|,|l_2|\right) \geq i\right) \end{array}\right]. \tag{4–4}$$

Indeed, let $i \in \mathbb{N}$. Then, according to (4–3), $\exists^{fini} T \subset \mathbb{N}$. Now put $\widetilde{T} = \max_{t\in T}\ t$. Now if $(n,(P,Q)) \in \mathbb{N}\times H$ such that $n \geq \widetilde{T}$, then $n \geq t,\ \ \forall t \in T$. Hence from (4–3) $\exists (U,l_1,l_2)$ with $U_n(P,Q) = U + l_1 l_2$, $|U| \leq 1$ and $\min\left(|l_1|,|l_2|\right) \geq i$. Consequently (4–3) $\Longrightarrow$ (4–4).

Conversely, let I be a finite subset of $\mathbb{N}$ and put $\overline{i} = \max_{i\in I}\ i$. For $\overline{i}$ there is, according to (4–4), $\widetilde{T} \in \mathbb{N}$. Consider $T = \left\{\widetilde{T}\right\}$ as a finite subset of $\mathbb{N}$. Now if $(n,(P,Q)) \in \mathbb{N}\times H$ such that $n \geq \widetilde{T}$, then $\exists (U,l_1,l_2)$ with $U_n(P,Q) = U + l_1 l_2$ with $|U| \leq 1$ and $\min\left(|l_1|,|l_2|\right) \geq \overline{i}$; that is, $\min\left(|l_1|,|l_2|\right) \geq i\ \forall i \in I$. Hence (4–4) $\Longrightarrow$ (4–3) and consequently we have the following proposition.

Proposition 4.2 *For any integer $i \in \mathbb{N}$ there exists an integer $\widetilde{T} \in \mathbb{N}$ such that for all $(n,(P,Q)) \in \mathbb{N}\times H$ satisfying $n \geq \widetilde{T}$, the term $U_n(P,Q)$ differs from a product of two integers whose absolute value is greater than or equal to i by an integer U with $-1 \leq U \leq 1$.*

(2) The second particular case is equivalent to

$$\forall n\ \forall (P,Q)$$

$$\left[\begin{array}{c} \forall^{st}(t_1,t_2)\left(n \geq t_1\ \&\ \dfrac{n}{2^{t_2}} \notin \mathbb{P}\right) \Longrightarrow \\ \exists\left(V,l_1',l_2'\right)\forall^{st} i\left(V_n(P,Q) = V + l_1' l_2' \text{ with } V \in \{0,\pm 1,\pm 2\} \text{ and } \min\left(\left|l_1'\right|,\left|l_2'\right|\right) \geq i\right) \end{array}\right],$$

where $n,\ i \in \mathbb{N}$, $(t_1,t_2) \in \mathbb{N}^2$, $\left(V,l_1',l_2'\right) \in \{0,\pm 1,\pm 2\}\times\mathbb{Z}\times\mathbb{Z}$. Using idealization and transfer the previous formula transforms, while remaining equivalent, to

$$\forall^{fini} I\ \exists^{fini} T\ \forall (n,(P,Q))$$

$$\left[\begin{array}{c} \forall (t_1,t_2) \in T\ \left(n \geq t_1\ \&\ \dfrac{n}{2^{t_2}} \notin \mathbb{P}\right) \Longrightarrow \exists\left(V,l_1',l_2'\right)\forall i \in I \\ \left(V_n(P,Q) = V + l_1' l_2' : V \in \{0,\pm 1,\pm 2\} \text{ and } \min\left(\left|l_1'\right|,\left|l_2'\right|\right) \geq i\right) \end{array}\right], \tag{4–5}$$

where I (resp. T) belongs to the power set of $\mathbb{N}$ (resp. $\mathbb{N}^2$). Then (4–5) is equivalent to

$$\forall i \in \mathbb{N}\ \exists (T_1, T_2) \in \mathbb{N}^2\ \forall (n, (P, Q))$$

$$\text{(4–6)} \quad \left[\begin{array}{c} \left(n \geq T_1, \frac{n}{2^i} \notin \mathbb{P}\ (i = 0, 1, .., T_2)\right) \Longrightarrow \exists \left(V, l_1', l_2'\right) \\ \left(V_n(P, Q) = V + l_1' l_2' : V \in \{0, \pm 1, \pm 2\} \text{ and } \min\left(\left|l_1'\right|, \left|l_2'\right|\right) \geq i\right) \end{array} \right].$$

Indeed, let $i \in \mathbb{N}$. According to (4–5), $\exists^{fini} T \subset \mathbb{N}^2$. Suppose

$T_1 = \max\{t_1 : (t_1, t_2) \in T\}$ and $T_2 = \max\{t_2 : (t_1, t_2) \in T\}$. Let $(n, (P, Q)) \in \mathbb{N} \times H$. Suppose that $n \geq T_1$ and $\frac{n}{2^i} \notin \mathbb{P}$ for $i = 0, 1, .., T_2$. Then for all $(t_1, t_2) \in T$, $n \geq t_1$ and $\frac{n}{2^{t_2}} \notin \mathbb{P}$. Hence, according to (4–5), $\exists \left(V, l_1', l_2'\right)\ V_n(P, Q) = V + l_1' l_2'$ with $V \in \{0, \pm 1, \pm 2\}$ and $\min\left(\left|l_1'\right|, \left|l_2'\right|\right) \geq i$. Consequently (4–5)$\Rightarrow$(4–6).

Conversely, let I be a finite subset of $\mathbb{N}$. Put $\bar{i} = \max_{i \in I} i$. Then for $\bar{i}$ there is, according to (4–6), $(T_1, T_2) \in \mathbb{N}^2$. Set $T = \{0, 1, ..., T_1\} \times \{0, 1, ..., T_2\}$, then T is finite. Let $(n, (P, Q)) \in \mathbb{N} \times H$ and suppose that for all $(t_1, t_2) \in T$, $n \geq t_1$ & $\frac{n}{2^{t_2}} \notin \mathbb{P}$. Then $n \geq T_1$ and $\frac{n}{2^i} \notin \mathbb{P}$ $(i = 0, 1, .., T_2)$. Hence, according to (4–6), $\exists \left(V, l_1', l_2'\right)$ such that $V_n(P, Q) = V + l_1' l_2'$ with $V \in \{0, \pm 1, \pm 2\}$ and $\min\left(\left|l_1'\right|, \left|l_2'\right|\right) \geq \bar{i}$; that is $\forall i \in I$ *min* $\left(\left|l_1'\right|, \left|l_2'\right|\right) \geq i$. Hence (4–6)$\Longrightarrow$(4–5) and consequently we have the following proposition.

Proposition 4.3 *For any integer $i \in \mathbb{N}$ there exists two integers $(T_1, T_2) \in \mathbb{N}^2$ such that for all $(n, (P, Q)) \in \mathbb{N} \times H$ satisfying $n \geq T_1$ and $\frac{n}{2^i} \notin \mathbb{P}$ for $i = 0, 1, .., T_2$ the term $V_n(P, Q)$ differs from a product of two integers whose absolute value is greater than or equal to i, by an integer V with $-2 \leq V \leq 2$.*

General remark. In the classical literature concerning Lucas sequences, generally the studies are concerned with the terms U_k and V_k for k belonging to a particular family of integers (see for example [6, 7]). In this work we note from the previous propositions that the main result expresses a property of uniformity because the conclusion is valid for all k beyond a certain rank.

Moreover, the ideas used in proofs here can also be used to deduce standard results. For example one sees without pain that Lemma 2.3 gives the size of $|U_k|$ and $|V_k|$ whereas Lemma 2.5 gives the growth of $|U_k|$ and $|V_k|$. In addition, the translation

by the reduction algorithm of lemmas used previously, which is an operation that is not difficult, gives more classical results. But giving further details would increase the length of this paper.

Acknowledgment The author wishes to thank the referees and editor for their comments and suggestions for improving an earlier version of this paper.

References

[1] A. Balog, $p + a$ without large prime factors, *Séminaire de théorie des nombres de Bordeaux* , Exposé **31**(1983-84).

[2] A. Boudaoud, La conjecture de Dickson et classes particulières d'entiers, *Annales Mathématiques Blaise Pascal* **13**(2006), 103-109.

[3] Chen, M.J.R, On the representation of a large even integer as the sum of a prime and the product of at most two primes, *Scientia Sinica* **16**(1973), 157 - 176.

[4] F. Diener et G. Reeb, *Analyse Non-Standard*, Hermann, Éditeurs des Sciences et des Arts, 1989.

[5] E. Nelson, Internal set theory: A new approach to nonstandard analysis, *Bull. Amer. Math. Soc.* **83**(1977), 1165-1198; doi:10.1090/S0002-9904-1977-14398-X.

[6] Paulo Ribenboim, *The Little Book of Big Primes*, Springer-Verlag, 1991.

[7] Paulo Ribenboim, *My numbers my friends*, Springer-Verlag 2000.

[8] S. Salerno - A. Vitolo, $p + 2$ with few and bounded prime factors, *Analysis* **11**(1991), 129-148.

Department of Mathematics, University of Msila, Ichbilia BP 166 - 28000 - Msila, Algeria

boudaoudab@yahoo.fr

Received: 25 March 2008 Revised: 25 November 2008