Journal of Number Theory **74**, 19–38 (1999)
Article ID jnth.1998.2290, available online at http://www.idealibrary.com on IDEAL®

An Algorithm to Determine the Points with Integral Coordinates in Certain Elliptic Curves

Paulo Ribenboim

*Department of Mathematics and Statistics, Queen's University,
Jeffrey Hall, Kingston, K7L 3N6, Canada*

Communicated by Alan C. Woods

Received September 23, 1997; revised March 9, 1998

We give an algorithm to determine the terms in a Lucas sequence of the first kind which are of the form k times a square. This algorithm is applied to provide the points with integral coordinates in certain elliptic curves, as well as to solve certain exponential equations of the form $a^n - 1 = b\,\square$ (where $a > 1$, b are given positive integers). © 1999 Academic Press

0. INTRODUCTION

Let $U = (U_n)_{n \geqslant 0}$ be a binary recurring sequence with parameters $P > 0$, $Q \neq 0$ and discriminant $D = P^2 - 4Q > 0$, so the sequence U is non-degenerate.

The following Theorem was proved by Shorey and Stewart [24] and also by Pethö [18]:

(0.1) *Let $A > 0$ be an integer. There exists an effectively computable number $C > 0$ (which depends on A), such that if $n > 0$ and $U_n = A\,\square$ then $n < C$.*

The value of C derived from the proof of the theorem is too large. Therefore it is interesting to indicate a practical algorithm which allows to find all indices n such that $U_n = A\,\square$. The algorithm indicated in this paper will require the knowledge of all indices n such that $U_n = \square$.

1. PRELIMINARIES ON LUCAS SEQUENCES

Let $P > 0$, $Q \neq 0$ be integers, $D = P^2 - 4Q$ and let

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

0022-314X/99 $30.00

be the roots of $X^2 - PX + Q$. Thus $P = \alpha + \beta$, $Q = \alpha\beta$, $D = (\alpha - \beta)^2$. We shall assume that $D > 0$, hence $\alpha \neq \beta$.

Let $U = U(P, Q)$, $V = V(P, Q)$ be the Lucas sequences with parameters P, Q, which are defined as follows:

$$\begin{aligned} &U_0 = 0, \qquad &&U_1 = 1, \qquad &&U_{n+2} = PU_{n+1} - QU_n, \\ &V_0 = 2, \qquad &&V_1 = P, \qquad &&V_{n+2} = PV_{n+1} - QV_n. \end{aligned}$$

As is well known,

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad V_n = \alpha^n + \beta^n$$

and

$$V_n^2 - DU_n^2 = 4Q^n$$

for all $n \geqslant 0$. Since $D \neq 0$ then $U_n \neq 0$ (for $n \neq 0$), $V_n \neq 0$. If $\gcd(P, Q) = 1$, we have the following divisibility properties:

- If $U_m \neq 1$ then $U_m \mid U_n$ if and only if $m \mid n$.
- If $V_m \neq 1$ then $V_m \mid V_n$ if and only if $m \mid n$ and n/m is odd.

Moreover, if $d = \gcd(m, n)$ then

$$\gcd(U_m, U_n) = U_d,$$

$$\gcd(V_m, V_n) = \begin{cases} V_d & \text{if } m/d,\ n/d \text{ are odd} \\ 1 \text{ or } 2 & \text{otherwise,} \end{cases}$$

$$\gcd(U_m, V_n) = \begin{cases} V_d & \text{if } m/d \text{ is even} \\ 1 \text{ or } 2 & \text{otherwise.} \end{cases}$$

Also $\gcd(U_m, Q) = \gcd(V_m, Q) = 1$ for all $m \geqslant 1$. Let $\mathscr{P}(U) = \{p \text{ prime} \mid \text{there exists } n > 0 \text{ such that } p \mid U_n\}$. If $p \in \mathscr{P}(U)$ let $\rho(p)$ be the smallest integer $n > 0$ such that $p \mid U_n$. Then $\rho(p) > 1$ and $p \mid U_m$ if and only if $\rho(p) \mid m$.

We shall require the following results:

- If P is even and Q is odd then $\rho(2) = 2$.
- If P is odd and Q is even then $2 \notin \mathscr{P}(U)$.
- If P and Q are odd then $\rho(2) = 3$.

Let p be any odd prime.

- If $p \mid P$, $p \nmid Q$ then $\rho(p) = 2$.
- If $p \nmid P$, $p \mid Q$ then $p \notin \mathscr{P}(U)$.
- If $p \nmid PQ$ but $p \mid D$ then $\rho(p) = p$.
- If $p \nmid PQD$ then $\rho(p)$ divides $p - (D/p) = p \pm 1$ [where (D/p) denotes the Legendre symbol].

We observe that for all primes $p \in \mathscr{P}(U)$ we have $\rho(p) \leqslant p + 1$; so if $p \neq 2$ all prime factors of $\rho(p)$ are at most equal to p.

2. SOME IDENTITIES

We quote the following well-known identities:

$$U_{m+n} = U_m V_n - Q^n U_{m-n},$$
$$V_{m+n} = V_m V_n - Q^n V_{m-n}.$$

Then

$$\begin{aligned} U_{2m} &= U_m V_m, \\ V_{2m} &= V_m^2 - 2Q^m, \\ U_{3m} &= U_m(DU_m^2 + 3Q^m) \\ &= U_m(V_m^2 - Q^m), \\ V_{3m} &= V_m(V_m^2 - 3Q^m). \end{aligned}$$

The following fact is also well-known. If $n = 2^e m$, where $e \geqslant 1$, and m is odd, then

$$U_n = U_m(V_m V_{2m} \cdots V_{2^{e-1}m})$$

and $\gcd(U_m, V_m V_{2m} \cdots V_{2^{e-1}m})$ divides 2^e.

The following results will be very useful.

(2.1) *Let $k \geqslant 1$ be odd. There exists a homogeneous polynomial $f_k \in \mathbb{Z}[X, Y]$, of degree $(k-1)/2$ such that $f_k(0, Y) = kY^{(k-1)/2}$ and such that if $m \geqslant 1$ then $U_{km} = U_m f_k(U_m^2, Q^m)$.*

Proof. Define $f_1 = 1$ and $f_3 = DX + 3Y$, so $U_{3m} = U_m(DU_m^2 + 3Q^m) = U_m f_3(U_m^2, Q^m)$. By induction, let $k \geqslant 5$. $U_{km} = U_{(k-2)m+2m} = U_{(k-2)m} V_{2m} - Q^{2m} U_{(k-4)m}$. Now

$$V_{2m} = V_m^2 - 2Q^m = DU_m^2 + 2Q^m,$$
$$U_{(k-2)m} = U_m f_{k-2}(U_m^2, Q^m),$$
$$U_{(k-4)m} = U_m f_{k-4}(U_m^2, Q^m).$$

So

$$U_{km} = U_m[f_{k-2}(U_m^2, Q^m)(DU_m^2 + 2Q^m) - Q^{2m} f_{k-4}(U_m^2, Q^m)]$$

and we take

$$f_k = f_{k-2}(DX + 2Y) - Y^2 f_{k-4}.$$

Thus $f_k \in \mathbb{Z}[X, Y]$, is homogeneous of degree $(k-1)/2$, and

$$\begin{aligned} f_k(0, Y) &= f_{k-2}(0, Y) \times 2Y - f_{k-4}(0, Y)\ Y^2 \\ &= [2(k-2) - (k-4)]\ Y^{(k-1)/2} \\ &= kY^{(k-1)/2}. \end{aligned}$$

Finally $U_{km} = U_m f_k(U_m^2, Q^m)$ for every $m \geqslant 1$. ▌

We deduce

(2.2) *For all* $k, m \geqslant 1$, $U_{km} = U_m Z$ *where* $\gcd(U_m, Z)$ *divides* k.

Proof. Let $k = 2^e h$, $e \geqslant 0$, h odd. If $e = 0$, $k = h$ is odd, $U_{km} = U_m Z$ where $Z = f_k(U_m^2, Q^m)$. If $d = \gcd(U_m, Z)$ then $d \mid kQ^{m(k-1)/2} = f_k(0, Q^m)$. But $\gcd(U_m, Q) = 1$ so $d \mid k$.

Let $e \geqslant 1$ so

$$\begin{aligned} U_{km} &= U_{hm} V_{hm} V_{2hm} \cdots V_{2^{e-1}hm} \\ &= U_m f_k(U_m^2, Q^m)\ V_{hm} \cdots V_{2^{e-1}hm}. \end{aligned}$$

Let $Z = f_h(U_m^2, Q^m)\ V_{hm} \cdots V_{2^{e-1}hm}$ so $U_{km} = U_m Z$ and $\gcd(U_m, Z)$ divides $\gcd(U_m, f_h(U_m^2, Q^m))\ 2^e$ which divides $h2^e = k$. ▌

3. STATEMENT OF THE PROBLEM

Let $A > 0$, $\delta = \pm 1$. We wish to determine the set $S(A, 4\delta)$ of all (x, y), with $x > 0$, $y > 0$, which are a solution of the equation

$$X^2 - AY^4 = 4\delta. \tag{3.1}$$

Similarly, we wish to determine the set $S(A, \delta)$ of all (x, y) with $x > 0$, $y > 0$ which are a solution of

$$X^2 - AY^4 = \delta. \tag{3.2}$$

It is enough to consider the equation (3.1) because $(x, y) \in S(A, \delta)$ if and only if $(2x, y) \in S(4A, 4\delta)$. The above equations correspond to the elliptic curves with equations

$$X^2Z^2 - AY^4 = 4\delta Z^4, \delta Z^4$$

respectively, which contain the point $(1, 0, 0)$.

Let $A = EB^2$ where $E > 0$ is square-free and $B > 0$. Then $(x, y) \in S(A, 4\delta)$ if and only if $x^2 - E(By^2)^2 = 4\delta$. Thus, we wish to determine all solutions (x, y), $x > 0$, $y > 0$ of

$$X^2 - EY^2 = 4\delta \tag{3.3}$$

with $y = B\square$ (B times a square).

The solution of (3.3) is classical. Let

$$\varepsilon = \frac{v + u\sqrt{E}}{2}$$

be the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{E})$. We note that $4 \nmid E$, and $E \equiv 2$ or $3 \pmod 4$ then v, u are even integers, while if $E \equiv 1 \pmod 4$ then $v \equiv u \pmod 2$. We have also $v > 0$, $u > 0$. The units of $\mathbb{Q}(\sqrt{E})$ greater or equal to 1 are $\varepsilon^n = (v_n + u_n\sqrt{E})/2$ with $n \geqslant 0$.

Let $N(\varepsilon) = (v^2 - Eu^2)/4 = \pm 1$ be the norm of ε. We describe the solutions of (3.3) with $x \geqslant 0$, $y \geqslant 0$. If $N(\varepsilon) = +1$, $\delta = +1$ then the solutions are (v_n, u_n) for all $n \geqslant 0$. If $N(\varepsilon) = +1$, $\delta = -1$, the equation has no solutions. If $N(\varepsilon) = -1$, $\delta = +1$, the solutions are (v_n, u_n) for all even $n \geqslant 0$. If $N(\varepsilon) = -1$, $\delta = -1$ the solutions are (v_n, u_n) for all odd $n \geqslant 0$.

The integers v_n, u_n are obtained by means of a binary recurring relation, as we indicate now.

Let $P = v$, $Q = N(\varepsilon)$ and consider the binary recurring sequence $U(P, Q) = (U_n)_{n \geqslant 0}$, and $V(P, Q) = (V_n)_{n \geqslant 0}$ with parameters P, Q. We show:

(3.4) *For every* $n \geqslant 0$: $u_n = uU_n$ *and* $v_n = V_n$.

Proof. $u_0 = 0 = uU_0$, $u_1 = u = uU_1$, $v_0 = 2 = V_0$, $v_1 = P = V_1$. Assume that $u_{n-1} = uU_{n-1}$ and $v_{n-1} = V_{n-1}$. Then $\alpha = \varepsilon = (v + u\sqrt{E})/2$, $\beta = (v - u\sqrt{E})/2$

are the roots of X^2-PX+Q, so $U_{n-1}=(\alpha^{n-1}-\beta^{n-1})/(\alpha-\beta)$, $V_{n-1}=\alpha^{n-1}+\beta^{n-1}$ and $(\alpha-\beta)^2=u^2E$. We have

$$\frac{v_n+u_n\sqrt{E}}{2}=\frac{v_{n-1}+u_{n-1}\sqrt{E}}{2}\cdot\frac{v+u\sqrt{E}}{2}$$

so

$$\begin{aligned} v_n &=\frac{1}{2}\left[v_{n-1}v+u_{n-1}uE\right] \\ &=\frac{1}{2}\left[(\alpha^{n-1}+\beta^{n-1})(\alpha+\beta)+\frac{\alpha^{n-1}-\beta^{n-1}}{\alpha-\beta}(\alpha-\beta)^2\right] \\ &=\alpha^n+\beta^n=V_n \end{aligned}$$

and

$$\begin{aligned} u_n &=\frac{1}{2}\left[v_{n-1}u+u_{n-1}v\right] \\ &=\frac{1}{2}u\left[\alpha^{n-1}+\beta^{n-1}+\frac{\alpha^{n-1}-\beta^{n-1}}{\alpha-\beta}\cdot(\alpha+\beta)\right] \\ &=uU_n. \quad \blacksquare \end{aligned}$$

In particular, if $E=M^2\mp 4$ then M is odd, the fundamental unit is $\varepsilon=(M+\sqrt{M^2\mp 4})/2$ with $N(\varepsilon)=\pm 1$. Then $P=M$ and $u_n=U_n$, $v_n=V_n$.

By the previous considerations we are led to determine all indices (respectively even indices, odd indices) $n>0$ such that $u_n=uU_n=B\square$. Let $uB=C\square$ where C is square-free. Then $u^2U_n=uB\square=C\square$ so $U_n=C\square$. Thus, we are led to the determination of $\{n>0 \mid U_n=C\square\}$, where $P>0$, $Q=\pm 1$, $D=P^2-4Q=u^2E>0$.

We shall consider the more general problem where Q is not required to be equal to ± 1, but still $\gcd(P,Q)=1$.

Next we observe that if there exists a prime p dividing C but $p\notin\mathscr{P}(U)$ then $U_n\neq C\square$ for all $n\geqslant 1$. So we may assume that every prime factor of C belongs to $\mathscr{P}(U)$.

More generally, let H be a non-empty finite subset of $\mathscr{P}(U)$, let $p[H]$ be the largest prime in H. Let $T(H)$ be the set of square-free positive integers whose prime factors belong to H and which are divisible by $p[H]$. We wish to determine the set $N_{T(H)}=\{n>0 \mid U_n=t\square \text{ where } t\in T(H)\}$. Clearly if H is the set of primes dividing C, then $\{n>0 \mid U_n=C\square\}\in N_{T(H)}$.

In the next section, we shall consider a "saturated" set $H^{(*)}$ containing H and we wish to determine the set $N_{T(H^*)} = \{n > 0 \mid U_n = t\square,$ where $t \in T(H^*)\}$, where $T(H^*)$ is defined in the same way as $T(H)$. Let $N_0 = \{n > 0 \mid U_n = \square\}$ We will indicate an algorithm to determine for all saturated sets H^* the set $N_{T(H^*)}$, *assuming that the set* N_0 *is known.*

4. SATURATED SETS OF PRIMES

Let H be a non-empty finite set of primes, $H \subseteq \mathscr{P}(U)$. Let $p[H]$ be the largest prime in H. If $H = \{2\}$ then H is said to be saturated. If $p[H] > 2$, we say that H is saturated when the following conditions are satisfied:

(1) If $2 \in \mathscr{P}(U)$ then $2 \in H$;

(2) If $q \in H$, $q \neq 2$, if $p \in \mathscr{P}(U)$ and $p \mid \rho(q)$ then $p \in H$.

If H is a finite non-empty set of primes, if q is any prime such that $q \in \mathscr{P}(U)$ and $q \leqslant p[H]$, let $H_q = \{p \in H \mid p \leqslant q\}$. If H is saturated and $q \in \mathscr{P}(U)$, $q \leqslant p[H]$ then H_q is saturated.

Now we show

(4.1) *Let* $\varnothing \neq H \subseteq \mathscr{P}(U)$. *Then there exists a unique minimal saturated set of primes* H^* *such that* $H \subseteq H^* \subseteq \mathscr{P}(U)$ *and* $p[H] = p[H^*]$.

Proof. We prove this by induction on $p[H]$. If $p[H] = 2$ then $H = \{2\}$ and $H^* = H$. We assume now that $p[H] = q > 2$ and proceed by induction. If $\rho(q) = q$ and $H = \{q\}$ let

$$H^* = \begin{cases} \{q\} & \text{if } \ 2 \notin \mathscr{P}(U) \\ \{2, q\} & \text{if } \ 2 \in \mathscr{P}(U). \end{cases}$$

If $H \neq \{q\}$ let $H_1 = H \backslash \{q\}$ so $H_1 \neq \varnothing$ and $p[H1] < q$. Let $H^* = H_1^* \cup \{q\}$. Since $p[H_1^*] = p[H_1] < q$ then $p[H^*] = q$. Moreover H^* is the unique smallest saturated set of primes containing H.

If $\rho(q) \neq q$, we noted previously that each prime factor of $\rho(q)$ is less than q; let $H_1 = (H \backslash \{q\}) \cup \{p$ prime, $p \in \mathscr{P}(U) \mid p$ divides $\rho(q)\}$. So $p[H_1] < p[H]$. Let $H^* = H_1^* \cup \{q\}$, hence $p[H^*] = q$ and again H^* is the unique smallest saturated set containing H. ▮

We give a numerical example. Let $P = 1$, $Q = -1$ so $U(P, Q)$ is the sequence of Fibonacci numbers. Let $H = \{5, 7, 13\}$. We have $\rho(5) = 5$, $\rho(7) = 8$, $\rho(13) = 14$. Hence $H^* = \{2, 5, 7, 13\}$.

5. THE DETERMINATION OF THE SETS $N_{T(H)}$

Let H be a finite, non-empty saturated set of primes contained in $\mathscr{P}(U)$; as before let $p[H]$ be the largest prime in H. Let $T=T(H)$ and

$$\bar{T}=\bar{T}(H)=\bigcup_{q\in H,\, q\leqslant p[H]} T(H_q)$$

where $H_q=\{p\in H \mid p\leqslant q\}$. Explicitly, if $H=\{q_1, q_2, ..., q_k\}$ with $q_1<q_2<\cdots<q_k=p[H]$, then $\bar{T}$ is the set of all $q_1^{e_1}\cdots q_{k-1}^{e_{k-1}}$ with $e_i=0$ or 1 for $i=1, ..., k-1$. By convention, if $H=\{q\}$ then $\bar{T}(H)=\{1\}$. Let $T\Box=\{t\Box \mid t\in T\}$ and similarly $\bar{T}\Box=\{t\Box \mid t\in \bar{T}\}$ and $N=N_T=\{n>0 \mid U_n\in T\Box\}$, $\bar{N}=N_{\bar{T}}=\{n>0 \mid U_n\in \bar{T}\Box\}$. In particular, if $\bar{T}=\{1\}$ then $N_T=N_0=\{n>0 \mid U_n=\Box\}$.

We first consider the following special case:

(5.1) *Let P, Q be odd and $H=\{2\}$. Then $N=\{n\geqslant 1 \mid U_n=2\Box\}\subseteq 3N_0$.*

Proof. Since P, Q are odd, then $\rho(2)=3$. By [16], $N=\{n\geqslant 1 \mid U_n=2\Box\}\subseteq\{3, 6\}$. If $U_3=2\Box$ since $U_1=1=\Box$ then $1\in N_0$ and $3\in 3N_0$. If $U_6=2\Box$ by [16] $U_2=P=\Box$ and again $6\in 3N_0$. So $N\subseteq 3N_0$. ▮

(5.2) *Let $q=p[H]$, $r=\rho(q)$ and assume that if $H=\{2\}$ then PQ is even. Then there exists $l\geqslant 1$ such that $N\subseteq r\bar{N}\cup r^2\bar{N}\cup\cdots\cup r^l\bar{N}/$*

Proof. Suppose there exists $n\in N\backslash(\bigcup_{i=1}^{\infty} r^i\bar{N})$. Let n be the smallest such integer. From $U_n\in T\Box$ then $q \mid U_n$ so $r \mid n$. Let $n=rm$; since $r\geqslant 2$ then $m<n$. By (2.2), $U_n=U_mZ$ and $d=\gcd(U_m, Z)$ divides r. Every prime factor of r is at most equal to q, because if $q=2$ then PQ is even and since $2\in\mathscr{P}(U)$ then $\rho(2)=2$. So every prime factor of d is at most equal to q.

Since $U_n\in T\Box$ then

$$(1)\begin{cases} U_m/d\in T\Box \\ Z/d\in\bar{T}\Box \end{cases} \quad\text{or}\quad (2)\begin{cases} U_m/d\in\bar{T}\Box \\ Z/d\in T\Box. \end{cases}$$

This gives (not necessarily respectively)

$$(1)\begin{cases} U_m\in T\Box \\ Z\in\bar{T}\Box \end{cases} \quad\text{or}\quad (2)\begin{cases} U_m\in\bar{T}\Box \\ Z\in T\Box. \end{cases}$$

Since $m<n$ and n is the smallest integer in $N\backslash(\bigcup_{i=1}^{\infty} r^i\bar{N})$ in case (1) from $m\notin N$ it follows that $m\in U_{i=1}^{\infty} r^i\bar{N}$ hence $n=rm\in\bigcup_{i=1}^{\infty} r^i\bar{N}$, which is impossible. In case (2), $m\in\bar{N}$ so $n=rm\in r\bar{N}$, which is again impossible.

By Theorem (0.1), N is a finite set. Since $r\geqslant 2$ there exists a prime $p \mid r$. Let $e=\max\{v_p(n) \mid n\in N\}$. If $i_0 v_p(r)>e$ then $n\notin\bigcup_{i=0}^{\infty} r^i\bar{N}$ for every $n\in N$

because $v_p(n) \leqslant e < iv_p(r)$ so $r^i \nmid n$. Therefore there exists $l \geqslant 1$ such that $N \subseteq \bigcup_{i=1}^{l} r^i \bar{N}$. ▮

With the same hypothesis and notations of (5.2), we have

(5.3) *Let $i \geqslant 1$ be such that $N \cap r^i \bar{N} = \varnothing$. Then $N \cap r^{hi+j} \bar{N} \subseteq N \cap r^j \bar{N}$ for $j = 1, ..., i$ and $h \geqslant 1$.*

Proof. Let $i \leqslant j \leqslant i$, $h = 1$ and $n \in N \cap r^{i+j} \bar{N}$. So $n = r^j m$ with $m \in r^i \bar{N}$. By (2.2) $U_n = U_m Z$ with $\gcd(U_m, Z) = d$ dividing r^j. By the hypothesis, every prime factor of d is at most equal to q. As in the preceding proof, we have

$$(1) \begin{cases} U_m \in T\square \\ Z \in \bar{T}\square \end{cases} \quad \text{or} \quad (2) \begin{cases} U_m \in \bar{T}\square \\ Z \in T\square. \end{cases}$$

In case (1) $m \in N \cap r^i \bar{N} = \varnothing$, which is impossible. In case (2), $m \in \bar{N}$ so $n = r^j m \in N \cap r^j \bar{N}$.

We proceed by induction on $h > 1$. Let $n \in N \cap r^{hi+j} \bar{N}$ so $n = r^{(h-1)i+j} m$ where $m \in r^i \bar{N}$. Again $U_n = U_m Z$ with $\gcd(U_m, Z) \mid r^{(h-1)i+j}$ and

$$(1) \begin{cases} U_m \in T\square \\ Z \in \bar{T}\square \end{cases} \quad \text{or} \quad (2) \begin{cases} U_m \in \bar{T}\square \\ Z \in T\square. \end{cases}$$

In case (1), $m \in N \cap r^i \bar{N} = \varnothing$, which is impossible. In case (2), $m \in \bar{N}$ so $n \in N \cap r^{(h-1)i+j} \bar{N} \subseteq N \cap r^j \bar{N}$, by induction. ▮

6. THE ALGORITHM

Let H be a finite non-empty saturated set of primes contained in $\mathscr{P}(U)$ and let $p[H]$ be the largest prime in H.

We assume that $N_0 = \{n > 0 \mid U_n = \square\}$ is known. We indicate how to determine $N_{T(H)}$.

(6.1) *Let $H = \{2\}$ and $N_{T(H)} = \{n \geqslant 1 \mid U_n = 2\square\}$.*

(a) *If PQ is odd then $N_{T(H)} \subseteq \{3, 6\}$.*

(b) *If PQ is even (hence P is even, Q is odd because $2 \in \mathscr{P}(U)$), then $N_{T(H)} \subseteq \bigcup_{i=1}^{l} 2^i N_0$ where l is the largest integer such that $N_{T(H)} \cap 2^l N_0 \neq \varnothing$; or $N_{T(H)} = \varnothing$ when $N_{T(H)} \cap 2N_0 = \varnothing$.*

Proof. (a) This statement was proved in [16]. (b) Since PQ is even, we may apply (5.2) and (5.3), thus proving (b). ▮

Now let $p[H]>2$. For each prime $q\in\mathscr{P}(U)$, $q<p[H]$, $H_q=\{p\in H \mid p\leqslant q\}$ is saturated and we assume that $N_{T(H_q)}$ has been determined, so $\bar{N}=N_{\bar{T}(H)}=\bigcup_{q<p[H]} N_{T(H_q)}$ has been determined. As already observed, if $H=\{p[H]\}$ then $\bar{N}=N_0$, which is assumed to be known. Then

(6.2) *$N_T(H)\subseteq\bigcup_{i=1}^{l} r^i\bar{N}$ where $q=p[H]$, $r=\rho(q)$, $l\geqslant 1$ is the largest integer such that $N\cap r^l\bar{N}\neq\varnothing$; or $N_{T(H)}=\varnothing$ when $N\cap r\bar{N}=\varnothing$.*

Proof. This is an immediate consequence of (5.2) and (5.3). ▮

The above results allow to compute $N_{T(H)}$ for all saturated sets of primes contained in $\mathscr{P}(U)$. In the final section we illustrate the method with numerical examples.

The following remark is pertinent. If $t>0$ is a square-free integer and $U_m=t\square$, $U_n=t\square$ (with $n\neq m$) then $U_mU_n=\square$. In this case, we say that U_m, U_n are in the same square-class of the sequence U. If P, Q are odd, the square-classes have been completely determined by Ribenboim and McDaniel [23]. There are finitely many square classes containing 2 or 3 elements; all the other square classes consist of only one element. In [21], it was shown that all the square-classes of the sequences $U(Q+1, Q)$ (where $Q>1$) are trivial; thus for every square-free $C>0$ (and every $Q>1$) there exists at most one index $n>0$ such that $U_n(Q+1, Q)=C\square$. These results imply that the number of steps of the algorithm is small.

7. SQUARES IN LUCAS SEQUENCES

Let $P>0$, $Q\neq 0$ be relatively prime integers such that $D=P^2-4Q>0$. The algorithm indicated requires the knowledge of the set $N_0=\{n>0 \mid U_n(P, Q)=\square\}$. We mention below some cases when N_0 is known.

The first result concerns the squares in the sequence of Fibonacci numbers ($P=1$, $Q=-1$), which were determined independently by Cohn [2, 3] and Wyler [25]:

$$\{n \mid U_n(1,-1)=\square\}=\{1, 2, 12\},$$

that is 1, 144 are the only square Fibonacci numbers. For P odd, $Q=\pm 1$, Cohn [5, 7] determined the squares in the sequences $U(P, \pm 1)$. More generally, if P, Q are odd and as above, then McDaniel and Ribenboim [16] proved that if $U_n(P, Q)=\square$ then $n\in\{1, 2, 3, 6, 12\}$.

Cohn [5, 7], has also determined for all $P>0$, P odd, the sets $\{n \mid U_n(P, \pm 1)=2\square\}$. Again, McDaniel and Ribenboim extended Cohn's result and have shown that for all P, Q odd, as above, $\{n \mid U_n(P, Q) = 2\square\} \subseteq \{3, 6\}$.

For PQ even, N_0 is only known in special cases. If $P = 2$, $Q = -1$ we have the sequence of Pell numbers. Ljunggren showed [12]: $U_n(2, -1) = \square$ if and only if $n = 1$ or 7, thus 1 and 169 are the only square Pell numbers.

It was also shown by Ljunggren [14] and Bumby [1] that if $P = 4$, $Q = -1$ and $U_n(4, -1) = \square$ then $n = 1$ or 2.

Cohn [9] obtained also results for certain pairs of parameters (P, Q), where P is even, $Q = \pm 1$. If $Q > 1$ and $P = Q + 1$ then $U_n = Q^n - 1/Q - 1$. Ljunggren [13] showed that if $n > 2$ and $U_n = \square$ then $(Q, n) = (7, 4)$ or $(3, 5)$. Moreover, $U_2 = \square$ exactly when $Q + 1 = \square$.

For $P = 2P_0$, $Q = \pm 1$ and $C > 0$ square-free, the number of indices $n > 0$ such that $U_n = C\square$ is in relation with the number of solutions of certain diophantine equation as we indicate now.

If $U_n = Cy^2$, from $V_n^2 - (P^2 - 4Q)\, U_n^2 = 4Q^n$ it follows that $V_n = 2x$ and

$$x^2 - (P_0^2 - Q)\, C^2 y^4 = \pm 1.$$

Cohn ([5, 7, 9) and Ljunggren ([10, 12, 15]) studied the equations

$$X^2 - AY^4 = 1, \tag{7.1}$$

$$X^2 - AY^4 = -1 \tag{7.2}$$

as well as

$$X^2 - AY^4 = 4, \tag{7.3}$$

$$X^2 - AY^4 = -4, \tag{7.4}$$

where $A > 0$, A not a square. As shown by Ljunggren, the Eq. (7.1) has at most two solutions. If the fundamental unit ε of the ring $\mathbb{Z}[\sqrt{A}]$ is determined, then the existing solutions are provided by ε and ε^2, except when $A = 1785$, when they are provided by ε, ε^4.

Ljunggren stated that the number of solutions of (7.2) is effectively bounded. If the fundamental unit of the field $\mathbb{Q}(\sqrt{A})$ is not a fundamental unit of the ring $\mathbb{Z}[\sqrt{A}]$ then the Eq. (7.2) has also at most two solutions. Ljunggren showed also that the solutions of (7.1) and (7.2) may be effectively computed.

Ljunggren determined explicitly that the solutions in positive integers of $X^2 - 2Y^4 = -1$ are $(x, y) = (1, 1), (239, 13)$ while $X^2 - 2Y^4 = 1$ has no solutions. It follows that for P even, $Q = \pm 1$ and $C > 0$, C square-free, the set $\{n > 0 \mid U_n = C\square\}$ has at most 2 elements in the cases indicated above.

8. NUMERICAL EXAMPLES

(I) Let $P=1$, $Q=-1$ so U is the sequence of Fibonacci numbers. Then $N_0=\{1, 2, 12\}$, as it was proved by Cohn [2, 3] and also by Wyler [25]. Let $C=35$. We shall determine the set $\{n>0 \mid U_n=35\,\square\}$.

We have $\rho(5)=5$, $\rho(7)=8$ so the smallest saturated set of primes containing $\{5, 7\}$ is $H=\{2, 5, 7\}$. Let $N_1=\{n>0 \mid U_n=2\,\square\}$. As proved by Cohn, $N_1=\{3, 6\}$. Let $H_5=\{2, 5\}$ and $N_2=N_{T(H_5)}=\{n>0 \mid U_n=5\,\square$ or $10\,\square\}$. Let $\bar{N}_2=N_0\cup N_1=\{1, 2, 3, 6, 12\}$. Then $N_2\subseteq 5\bar{N}_2\cup 25\bar{N}_2 \cup \cdots$. But $5\bar{N}_2=\{5, 10, 15, 30, 60\}$ and $U_5=5\,\square$ so $5\in N_2$, while U_{10}, U_{15}, U_{30}, $U_{60}\notin\{5\,\square, 10\,\square\}$. Next $25\bar{N}_2=\{25, 50, 75, 150, 300\}$ but U_{25}, U_{50}, U_{75}, U_{150}, $U_{300}\notin\{5\,\square, 10\,\square\}$. This may be seen by direct computation which is somewhat long. It may also be seen as follows. We note that $2\mid U_n$ exactly when $3\mid n$ and $3\mid U_n$ whenever $4\mid n$. If $k\in\{1, 2, 3, 6, 12\}$ then $U_{25k}=5\,\square$ implies that $U_{25k}U_5=\square$; this is impossible since the square-class of U_5 is trivial—see Ribenboim [20]. Next if $U_{25k}=10\,\square$ then $3\mid k$ so $k\in\{3, 6, 12\}$. But $U_{75}=U_{25}(5U_{25}^2-3)$, $\gcd(U_{25}, 5U_{25}^2-3)=1$ (since $3\nmid U_{25}$), so $U_{25}=\square$ or $5\,\square$—both cases are impossible. If $U_{150}=U_{50}(5U_{50}^2+3)$ again $U_{50}=\square$ or $5\,\square$, impossible. If $U_{300}=U_{100}(5U_{100}^2+3)=10\,\square$, then similarly $U_{50}V_{50}=U_{100}=3\,\square$ or $15\,\square$; but $\gcd(U_{50}, V_{50})=1$ so $U_{50}=\square, 5\,\square$ and both cases are impossible.

Thus $N_2=\{5\}$. Let $\bar{N}_3=N_0\cup N_1\cup N_2=\{1, 2, 3, 5, 6, 12\}$. Let $N_3=\{n\geqslant 1 \mid U_n=7\,\square, 14\,\square, 35\,\square, 70\,\square\}$.

Since $\rho(7)=8$ then $N_3\subseteq 8\bar{N}_3\cup 8^2\bar{N}_3\cup\cdots$. We have $8\bar{N}_3=\{8, 16, 24, 40, 48, 96\}$ and for every $n\in 8\bar{N}_3$, $U_n\notin\{7\,\square, 14\,\square, 35\,\square, 70\,\square\}$. This may be seen by direct calculation or by an argument similar to the preceding one. Thus $N_3=\emptyset$. In particular, $\{n\geqslant 1 \mid U_n=35\,\square\}=\emptyset$. It follows that the only solution in non-negative integers of $X^2-125\times 49Y^4=4$ is (2, 0), while

$$X^2-125\times 49Y^4=-4$$

has no solutions in non-negative integers.

(II) Let $P=2$, $Q=-1$ so $D=P^2-4Q=8$. As already indicated $N_0=\{1, 7\}$. Let $C=91$. We shall determine the set $\{n>0 \mid U_n=91\,\square\}$. We have $\rho(7)=6$, $\rho(13)=7$, $\rho(3)=4$, so the smallest saturated set of primes containing $\{7, 13\}$ is $H=\{2, 3, 7, 13\}$. Let $N_1=\{n>0 \mid U_n=2\,\square\}$. We have $N_1\subseteq 2N_0\cup 2^2N_0\cup\cdots$. But $2N_0=\{2, 14\}$, with $U_2=2\,\square$, $U_{14}\neq 2\,\square$. Also $4N_0=\{4, 28\}$ with U_4, $U_{28}\neq 2\,\square$. Thus $N_1=\{2\}$.

Let $\bar{N}_2=N_0\cup N_1=\{1, 2, 7\}$ and $N_2=\{n>0 \mid U_n=3\,\square, 6\,\square\}$. We have $\rho(3)=4$ so $N_2\subseteq 4\bar{N}_2\cup 4^2\bar{N}_2\cup\cdots$. But $4\bar{N}_2=\{4, 8, 28\}$ and $U_4=3\,\square$, U_8, $U_{28}\notin\{3\,\square, 6\,\square\}$. Also $16\bar{N}_2=\{16, 32, 112\}$ and U_{16}, U_{32}, $U_{112}\notin\{3\,\square, 6\,\square\}$. Hence $N_2=\{3\}$.

Let $\bar{N}_3 = N_0 \cup N_1 \cup N_2 = \{1, 2, 3, 7\}$ and $N_3 = \{n > 0 \mid U_n = 7\square,\ 14\square,\ 21\square,\ 42\square\}$. We have $\rho(7) = 6$ so $N_3 \subseteq 6\bar{N}_3 \cup 6^2\bar{N}_3 \cup \cdots$. But $6\bar{N}_3 = \{6, 12, 18, 42\}$ and $U_n \notin \{7\square, 14\square, 21\square, 42\square\}$ for all $n \in 6\bar{N}_3$. Thus $N_3 = \varnothing$.

Let $\bar{N}_4 = N_0 \cup N_1 \cup N_2 \cup N_3 = \{1, 2, 3, 7\}$. Let $N_4 = \{n > 0 \mid U_n = 13\square,\ 26\square,\ 39\square,\ 91\square,\ 78\square,\ 182\square,\ 273\square,\ 546\square\}$. Since $\rho(13) = 7$ then $N_4 \subseteq 7\bar{N}_4 \cup 7^2\bar{N}_4 \cup \cdots$. But $N_4 \cap 7\bar{N}_4 = \varnothing$. Hence $N_4 = \varnothing$ and in particular $\{n > 0 \mid U_n = 91\square\} = \varnothing$. It follows that the equations

$$X^2 - 8 \times 49 \times 169\, Y^4 = \pm 4$$

have no solutions in positive integers.

(III) In a recent paper [17] Mignotte and Pethö used a different method to prove: If $P \geqslant 4$, $Q = 1$, $n \geqslant 4$ and $U_n(P, Q) \in \{\square, 2\square, 3\square, 6\square\}$ then $P = 338$, $n = 4$, with $U_4(338, 1) = \square$.

We shall obtain their result using our method and a result of Ljunggren already quoted in the preceding section. We first determine all $P \geqslant 4$, $n \geqslant 4$ such that $U_n(P, 1) = \square$. Let P be odd. By [16], $n = 6, 12$. The latter case is excluded, since it implies that $Q \equiv -1 \pmod{120}$ (see [16]). We have $U_6 = U_3 V_3 = (P^2 - 1)(P^2 - 3)\, P$ with $\gcd(P^2 - 1, P^2 - 3) = 2$. Since $U_6 = \square$ and $P > 3$ then $P^2 - 1 = 2\square$, $P^2 - 3 = 2\square$ so 1 would be the difference of two positive squares, an absurdity.

If $P = 2P_0$, from $V_n^2 - (P^2 - 4)\, U_n^2 = 4$ it follows that $V_n = 2v_n$, $U_n = u_n^2$ and (v_n, u_n) is a solution of $X^2 - (P_0^2 - 1)\, Y^4 = 1$. The fundamental unit of the order $\mathbb{Z}[\sqrt{P_0^2 - 1}]$ is $\varepsilon = P_0 + \sqrt{P_0^2 - 1} \in \mathbb{Z}[\sqrt{P_0^2 - 1}]$. It provides the solution $(P_0, 1)$. According to Ljunggren's result, the equation has at most one other solution in positive integers, which corresponds to ε^2 if $\mathbb{Q}(\sqrt{P_0^2 - 1}) \neq \mathbb{Q}(\sqrt{1785})$ and corresponds to ε^4 when $\mathbb{Q}(\sqrt{P_0^2 - 1}) = \mathbb{Q}(\sqrt{1785})$. We consider the first case.

From $\varepsilon^2 = (2P_0^2 - 1) + 2P_0\sqrt{P_0^2 - 1}$, if $(2P_0^2 - 1)^2 - (P_0^2 - 1) \cdot 16P_0^4 = 1$ we deduce that $P_0 = 1$ so $D = P^2 - 4 = 0$, which is contrary to the hypothesis.

In the second case, since the fundamental unit of $\mathbb{Q}(\sqrt{1785})$ is $169 + 16\sqrt{1785}$ then $P = 338$; now ε^4 gives rise to a solution of the above equation; explicitly $U_4(338, 1) = 239^2 \times 26^2$. We note that $U_3 = P^2 - 1 \neq \square$. Thus, we have shown that if $P \neq 338$, $P \geqslant 4$ then $N_0 \subseteq \{1, 2\}$, while if $P = 338$ then $N_0 \subseteq \{1, 2, 4\}$. Moreover, $2 \in N_0$ exactly when $P = \square$. Let $N_1 = \{n \geqslant 1 \mid U_n = 2\square\}$. If P is odd, then by [16], $N_1 \subseteq \{3, 6\}$. But if $U_6 = 2\square$ then $Q \equiv -1 \pmod 8$ (see [16]) and this case is excluded, so $N_1 \subseteq \{3\}$.

The discussion when P is even is somewhat longer but easy. Now $\rho(2) = 2$ and $N_1 \subseteq 2N_0 \cup 2^2N_0 \cup \cdots$ where $N_0 \subseteq \{1, 2, 4\}$ with $2 \in N_0$

when $P=\square$ and $4\in N_0$ when $P=338$. We have $N_1\subseteq\{2,4,8\}\cup\{4,8,16\}\cup\cdots$. $2\in N_1$ exactly when $P=2\square$. If $U_4=2\square$ then

$$\begin{cases} U_2 = P = \square \\ V_2 = P^2-2=2\square \end{cases} \quad \text{or} \quad \begin{cases} =2\square \\ =\square. \end{cases}$$

The first case gives $-1\equiv\square \pmod 8$ which is impossible. The second case is impossible, since $P^2-2\neq\square$. If $U_8=2\square$ then

$$\begin{cases} U_4 = 2\square \\ V_4 = \square \end{cases} \quad \text{or} \quad \begin{cases} =\square \\ =2\square \end{cases}$$

The first case was shown to be impossible. In the second case $P=338$ so $V_4=V_2^2-2\neq 2\square$, as seen by direct computation. If $U_{16}=2\square$ then

$$\begin{cases} U_8 = 2\square \\ U_8 = \square \end{cases} \quad \text{or} \quad \begin{cases} V_8 = \square \\ V_8 = 2\square. \end{cases}$$

Both cases are impossible, since $8\notin N_1$, $8\notin N_0$. This implies that $N_1=\varnothing$ when $P\neq 2\square$ and $N_1=\{2\}$ when $P=2\square$.

We have $\bar{N}_2=N_0\cup N_1\subseteq\{1,2,4\}$ and $2\in\bar{N}_2$ whenever $P=\square$ or $2\square$ and $4\in\bar{N}_2$ when $P=338$. Let $N_2=\{n\geqslant 1 \mid U_n=3\square \text{ or } 6\square\}$. We have

$$\rho(3)=\begin{cases} 2 & \text{if } \ 3\mid P \\ 3 & \text{if } \ 2\nmid P \end{cases}.$$

First we assume that $3\mid P$, so $N_2\subseteq 2\bar{N}_2\cup 4\bar{N}_2\cup\cdots\subseteq\{2,4,8\}\cup\{4,8,16\}\cup\cdots$. If $U_4=3\square$ since $\gcd(U_2,V_2)=2$ then

$$\begin{cases} U_2 = 6\square = P \\ V_2 \qquad\ = P^2-2=2\square \end{cases} \quad \text{or} \quad \begin{cases} =2\square \\ =6\square. \end{cases}$$

But $P^2-2\neq 2\square$ and $P^2-2\neq 6\square$ (as seen modulo 3). If $U_4=6\square$ we have similarly

$$\begin{cases} U_2 = 2\square \\ V_2 = P^2-2=3\square \end{cases} \quad \text{or} \quad \begin{cases} =\square \\ =6\square \end{cases} \quad \text{or} \quad \begin{cases} =6\square \\ =\square \end{cases} \quad \text{or} \quad \begin{cases} =3\square \\ =2\square. \end{cases}$$

The first three cases are impossible, and the last case is also impossible (as seen modulo 3). If $U_8=3\square$ then

$$\begin{cases} U_4 = 2\square \\ V_4 = 6\square \end{cases} \quad \text{or} \quad \begin{cases} =6\square \\ =2\square \end{cases}$$

But $4\notin N_1$ and $U_4\neq 6\square$ as seen above. If $U_8=6\square$ then

$$\begin{cases} U_4 = 2\square \\ V_4 = 3\square \end{cases} \quad \text{or} \quad \begin{cases} =\square \\ =6\square \end{cases} \quad \text{or} \quad \begin{cases} =6\square \\ =\square \end{cases} \quad \text{or} \quad \begin{cases} =3\square \\ =2\square \end{cases}$$

Cases 1, 3, 4 have been shown to be impossible. In case 2, $P = 338$ and this is impossible, since $3 \mid P$. If $U_{16} = 3\square$ then

$$\begin{cases} U_8 = 2\square \\ V_8 = 6\square \end{cases} \quad \text{or} \quad \begin{cases} = 6\square \\ = 2\square \end{cases}$$

and both cases are impossible, as seen above. If $U_{16} = 6\square$ then

$$\begin{cases} U_8 = 2\square \\ V_8 = 3\square \end{cases} \quad \text{or} \quad \begin{cases} = \square \\ = 6\square \end{cases} \quad \text{or} \quad \begin{cases} = 6\square \\ = \square \end{cases} \quad \text{or} \quad \begin{cases} = 3\square \\ = 2\square \end{cases}$$

and all cases are impossible, as seen above. Thus $N_2 \subseteq \{2\}$ and $2 \in N_2$ exactly when $P = 3\square$ or $6\square$.

Now we assume that $3 \nmid P$ hence $\rho(3) = 3$ and therefore $N_2 \subseteq 3\bar{N}_2 \cup 9\bar{N}_2 \cup \cdots \subseteq \{3, 6, 12\} \cup \{9, 18, 36\} \cup \cdots$. We have $U_6 = U_3 V_3$ with $\gcd(U_3, V_3) = 1$, $V_3 = P(P^2 - 3)$ so $3 \nmid V_3$ and $\gcd(P, P^2 - 3) = 1$. If $U_6 = 3\square$ then

$$\begin{cases} U_3 = 3\square \\ V_3 = \square \end{cases}$$

hence

$$\begin{cases} P = \square \\ P^2 - 3 = \square \end{cases}$$

therefore $P = 2$, an absurdity. If $U_6 = 6\square$ then

$$\begin{cases} U_3 = 3\square \\ V_3 = 2\square \end{cases}$$

hence

$$\begin{cases} P = 2\square \\ P^2 - 3 = \square \end{cases}$$

so $P = 2$, which was excluded. If $U_{12} = 3\square$ then

$$\begin{cases} U_6 = 2\square \\ V_6 = 6\square \end{cases} \quad \text{or} \quad \begin{cases} = 6\square \\ = 2\square. \end{cases}$$

Since $V_6 = V_3^2 - 2 \not\equiv 0 \pmod 3$ then the first case is impossible while the second case was already excluded. If $U_{12} = 6\,\square$ then

$$\begin{cases} U_6 = 2\,\square \\ V_6 = 3\,\square \end{cases} \quad\text{or}\quad \begin{cases} = \square \\ = 6\,\square \end{cases} \quad\text{or}\quad \begin{cases} = 6\,\square \\ = \square \end{cases} \quad\text{or}\quad \begin{cases} = 3\,\square \\ = 2\,\square \end{cases}$$

and as before we see that all cases are impossible.

We have $U_9 = U_3(V_3^2 - 1) = U_3(DU_3^2 + 3)$ so $\gcd(U_3, V_3^2 - 1) = 3$. If $U_9 = 3$ then

$$\begin{cases} U_3 = 3\square \\ V_3^2 - 1 = \square \end{cases} \quad\text{or}\quad \begin{cases} = \square \\ = 3\,\square. \end{cases}$$

The first case implies that $V_3 = P(P^2 - 3) = 1$ which is impossible. Since $3 \notin N_0$ then the second case is impossible. Since U_9 is odd then $U_9 \neq 6\,\square$. Let $U_{18} = U_9 V_9 = 3\,\square$ or $6\,\square$. We have $\gcd(U_9, V_9) = 1$ and since $2 \nmid U_9$, we have the following cases:

$$\begin{cases} U_9 = \square \\ V_9 = 3\,\square \end{cases} \quad\text{or}\quad \begin{cases} = 3\,\square \\ = \square, \end{cases}$$

respectively

$$\begin{cases} U_9 = \square \\ V_9 = 6\,\square \end{cases} \quad\text{or}\quad \begin{cases} = 3\,\square \\ = 2\,\square. \end{cases}$$

But $9 \notin N_0$ and $U_9 \neq 3\,\square$ so both cases are impossible. If $U_{36} = U_{18} V_{18} = 3\,\square$ or $6\,\square$ since $\gcd(U_{18}, V_{18} = 2$ then

$$\begin{cases} U_{18} = 2\,\square \\ V_{18} = 6\,\square \end{cases} \quad\text{or}\quad \begin{cases} = 6\,\square \\ = 3\,\square, \end{cases}$$

respectively

$$\begin{cases} U_{18} = 2\,\square \\ V_{18} = 3\,\square \end{cases} \quad\text{or}\quad \begin{cases} = \square \\ = 6\,\square \end{cases} \quad\text{or}\quad \begin{cases} = 6\,\square \\ = \square \end{cases} \quad\text{or}\quad \begin{cases} = 3\,\square \\ = 2\,\square. \end{cases}$$

As already seen, all cases are impossible. We conclude that $N_2 \subseteq \{3\}$. This concludes the proof of the result of Mignotte and Pethö.

This result may be interpreted in terms of diophantine equations as follows: Let $P \geqslant 4$. The only solution (x, y), with $x > 0$, $y \geqslant P$ of

$$X^2 - (P^2 - 4)\, Y^4 = 4$$

is $P=338$, $y=26\times 239$. If $P\geqslant 4$ the equations

$$X^2-(P^2-4)\,4Y^4=4,$$
$$X^2-(P^2-4)\,9Y^4=4,$$
$$X^2-(P^2-4)\,36Y^4=4$$

have no solution in positive integers x, y where $y\geqslant P$.

(IV) Let $Q>1$, $P=Q+1$ so $U_n=(Q^n-1)/(Q-1)$. As already quoted, $N_0=\{n\geqslant 1 \mid U_n=\square\}$ has been determined:

$$N_0=\begin{cases}\{1\} & \text{if } Q\neq 3,7, \quad P\neq\square,\\ \{1,2\} & \text{if } Q\neq 3,7, \quad P=\square,\\ \{1,2,5\} & \text{if } Q=3,\\ \{1,4\} & \text{if } Q=7.\end{cases}$$

We shall apply our method to determine $N_1=\{n\geqslant 1 \mid U_n=2\square\}$. If Q is even then P is odd, so $2\notin\mathscr{P}(U)$, hence $N_1=\emptyset$. Now we assume Q odd, so P is even and $\rho(2)=2$. Thus

$$N_1\subseteq 2N_0\cup 4N_0\cup\cdots.$$

We distinguish several cases:

(a) $Q\neq 3,7$, $P\neq\square$.

We have $2\in N_1$ exactly when $P=2\square$. We show that $4\notin N_1$. If $2\square=U_4=U_2V_2$, with $\gcd(U_2,V_2)=2$, then

$$\begin{cases}U_2=P=\square\\ V_2=P^2-2Q=Q^2+1=2\square\end{cases} \quad\text{or}\quad \begin{cases}=2\square\\ =\square\end{cases}.$$

The first case is impossible and so is the second case. Thus

$$N_1=\begin{cases}\emptyset & \text{if } P\neq 2\square\\ \{2\} & \text{if } P=2\square.\end{cases}$$

(b) $Q\neq 3,7$, $P=\square$.

Now $2\notin N_1$ and $4\in N_1$ if and only if $Q^2+1=2\square$. We show that $8\notin N_1$. If $2\square=U_8=U_4V_4$ with $\gcd(U_4,V_4)=2$ then

$$\begin{cases}U_4=\square\\ V_4=2\square\end{cases} \quad\text{or}\quad \begin{cases}=2\square\\ =\square.\end{cases}$$

The first case is impossible. In the second case $U_4 = 2\square$ implies that $Q^2+1=2\square$. On the other hand $\square = V_2^2 - 2Q^2 = Q^4+1 \neq \square$. Similarly $16 \notin N_1$. Thus

$$N_3 = \begin{cases} \varnothing & \text{if } \ Q^2+1 \neq 2\square \\ \{4\} & \text{if } \ Q^2+1 = 2\square. \end{cases}$$

(c) $Q=3$, so that $P=4$. We have $U_n = (3^n-1)/2 = 2\square$ if and only if $3^n - 1 = \square$. Now $N_1 \subseteq \{2, 4, 10\} \cup \{4, 8, 20\} \cup \cdots$.

We have $3^2-1 \neq \square$, $3^4-1 \neq \square$, $3^{10}-1 \neq \square$ thus $N_1 = \varnothing$.

(d) $Q=7$ so $P=8=2\square$ hence $2 \in N_1$. We have $U_n = (7^n-1)/6 = 2\square$ if and only if $7^n - 1 = 3\square$. Now $N_1 \subseteq \{2, 8\}, \{4, 16\}$. But $7^4-1 \neq 3\square$, $7^8-1 \neq 3\square$, $7^{16}-1 \neq 3\square$, hence $N_1 = \{2\}$.

This concludes the determination of N_1 in all cases.

(V) Let $a > 1$, $b \geqslant 1$ be given integers where b is square-free. We illustrate how the algorithm may be applied to find all integers $n \geqslant 1$ such that

$$a^n - 1 = b\square.$$

Since $a-1$ divides a^n-1 then $b\square/(a-1) = c\square$, where c is square-free and therefore we are required to determine the exponents n such that $U_n(a+1, a) = c\square$.

For example, we indicate how to solve $11^n - 1 = 7\square$. Then $U_n(12, 11) = 70\square$. Since $\rho(5)=5$, $\rho(7)=3$ then $H^* = \{2, 3, 5, 7\}$. Let $N_0 = \{n \geqslant 1 \mid U_n = \square\}$. As already indicated $N_0 = \{1\}$. Let $N_1 = \{n \geqslant 1 \mid U_n = 2\square\}$. Since $\rho(2)=2$ then $N_1 \subseteq \{2, 4, ...\}$. But $2 \notin N_1$ since $(11^2-1)/(11-1) \neq \square$. Thus $N_1 = \varnothing$.

Let $\bar{N}_2 = N_0 \cup N_1 = \{1\}$ and $N_2 = \{n \geqslant 1 \mid U_n = 3\square, 6\square\}$. We have $\rho(3)=2$, so $N_2 \subseteq 2\bar{N}_2 \cup 4\bar{N}_2 \cup \cdots = \{2, 4, ...\}$. We have $U_2 = 3\square$, so $2 \in N_2$. Also $U_2 \neq 6\square$. If $U_2V_2 = U_4 = 3\square$ or $6\square$ then

$$\begin{cases} U_2 = 6\square \\ V_2 = 2\square \end{cases} \quad \text{or} \quad \begin{cases} = 2\square \\ = 6\square, \end{cases}$$

respectively

$$\begin{cases} U_2 = 3\square \\ V_2 = 2\square \end{cases} \quad \text{or} \quad \begin{cases} = 6\square \\ = \square \end{cases} \quad \text{or} \quad \begin{cases} = \square \\ = 6\square \end{cases} \quad \text{or} \quad \begin{cases} = 2\square \\ = 3\square. \end{cases}$$

All cases are impossible as seen at once. Thus $N_2 = \{2\}$.

Let $\bar{N}_3 = N_0 \cup N_1 \cup N_2 = \{1, 2\}$. Since $\rho(5)=5$ then $N_3 = \{n \geqslant 1 \mid U_n = 5\square,\ 10\square,\ 15\square,\ 30\square\} \subseteq 5\bar{N}_3 \cup 25\bar{N}_3 \cup \cdots$. But $3 \mid 11^5 - 1$, so

$11^5-1\neq 3\,\square,\ 6\,\square$. Also $11^5-1\neq\square,\ 2\,\square$. It follows that $5\notin N_3$. We show that $11^{10}-1\neq\square,\ 2\,\square,\ 3\,\square,\ 6\,\square$, otherwise

$$\begin{cases}11^5-1=2\,\square\\ 11^5+1=2\,\square\end{cases}\quad\text{or}\quad\begin{cases}\square\\ 2\,\square\end{cases}\quad\text{or}\quad\begin{cases}2\,\square\\ \square\end{cases}$$

$$\text{or}\quad\begin{cases}6\,\square\\ 2\,\square\end{cases}\quad\text{or}\quad\begin{cases}2\,\square\\ 6\,\square\end{cases}\quad\text{or}\quad\begin{cases}3\,\square\\ 2\,\square\end{cases}$$

$$\text{or}\quad\begin{cases}6\,\square\\ \square\end{cases}\quad\text{or}\quad\begin{cases}\square\\ 6\,\square\end{cases}\quad\text{or}\quad\begin{cases}3\,\square\\ 2\,\square\end{cases}$$

and by the above all cases are impossible. Thus $N_3=\varnothing$. Let $\bar{N}_4=\bar{N}_3\cup N_3=\{1,2\}$ and $N_4=\{n\mid U_n=7\,\square,\ 14\,\square,\ 21\,\square,\ 35\,\square,\ 42\,\square,\ 70\,\square,\ 105\,\square,\ 210\,\square\}$. We have $\rho(7)=3$, so $N_4\subseteq 3\bar{N}_4\cup 9\bar{N}_4\ldots=\{3,6,9,18,\ldots\}$. But $U_3\neq 70\,\square$. If $U_3V_3=U_6=70\,\square$ then

$$\begin{cases}U_3=70\,\square\\ V_3=\square\end{cases}\quad\text{or}\quad\begin{cases}35\,\square\\ 2\,\square\end{cases}\quad\text{or}\quad\begin{cases}14\,\square\\ 5\,\square\end{cases}$$

$$\text{or}\quad\begin{cases}10\,\square\\ 7\,\square\end{cases}\quad\text{or}\quad\begin{cases}5\,\square\\ 14\,\square\end{cases}\quad\text{or}\quad\begin{cases}2\,\square\\ 35\,\square\end{cases}\quad\text{or}\quad\begin{cases}2\,\square\\ 70\,\square\end{cases}$$

But $U_3=7\times 19$, so all the above cases are impossible. This proves that $11^n-1\neq 7\,\square$ for all $n\geqslant 1$.

REFERENCES

1. R. T. Bumby, The diophantine equation $3x^2-2y^2=1$, *Math. Scand.* **21** (1967), 141–148.
2. J. H. E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.* **39** (1964), 537–540.
3. J. H. E. Cohn, Square Fibonacci numbers, etc., *Fibonacci Quart.* **2** (1964), 109–113.
4. J. H. E. Cohn, Lucas and Fibonacci numbers and some diophantine equations, *Proc. Glasgow Math. Assoc.* **7** (1965), 24–28.
5. J. H. E. Cohn, Eight diophantine equations, *Proc. London Math. Soc. (3)* **16** (1966), 153–166; **17** (1967), 381.
6. J. H. E. Cohn, The diophantine equation $x^2=Dy^4+1$, *J. London Math. Soc.* **40** (1967), 475–476.
7. J. H. E. Cohn, Five diophantine equations, *Math. Scand.* **21** (1967), 61–70.
8. J. H. E. Cohn, Some quartic diophantine equations, *Pacific J. Math* **26** (1968), 233–243.
9. J. H. E. Cohn, Squares in some recurrence sequences, *Pacific J. Math.* **41** (1972), 631–646.
10. W. Ljunggren, Einige Eigenschaften der Einheiten reeller quadratischer und rein biquadratisher Zahlkörper mit Anwendungen auf die Lösung einer Klasse unbestimmter Gleichungen vierten Grades, *Skr. Norske Vidensk. Akad. Oslo I Klasse* **12** (1936),.
11. W. Ljunggren, Über die unbestimmte Gleichung $Ax^2-By^4=C$, *Arch. Math.-Naturvid.* **41** (1938), 3–18.
12. W. Ljunggren, Zur Theorie der Gleichung $x^2+1=Dy^4$, *Abh. Norsk Vid. Akad. Oslo* **1**, No. 5 (1942), 1–27.

13. W. Ljunggren, New propositions about the indeterminate equation $x^n - 1/x - 1 = y^q$, *Norske Mat. Tidsskrift* **25** (1943), 17–20. [In Norwegian]
14. W. Ljunggren, On the diophantine equation $x^2 + 4 = Ay^4$, *Kong. Norske Vidensk. Selskab Vorhandl.* **21**, No. 18 (1951), 82–84.
15. W. Ljunggren, Some remarks on the diophantine equations $x^2 - Dy^4 = 1$ and $x^4 - Dy^2 = 1$, *J. London Math. Soc.* **41** (1966), 542–544.
16. W. L. McDaniel and P. Ribenboim, The square terms in Lucas sequences, *J. Number Theory* **58** (1996), 104–123.
17. M. Mignotte and A. Pethö, Sur les carrés dans certaines suites de Lucas, *J. Th. Nombres Bordeaux* **5** (1993), 333–341.
18. A. Pethö, Perfect powers in second order linear recurrences, *J. Number Theory* **15** (1982), 5–13.
19. P. Ribenboim, The Fibonnacci numbers and the Arctic Ocean, *in* "Symposia Gaussian a Conf. A." (M. Behara, R. Fritsch, and R. G. Lintz, Eds.), pp. 41–83, de Gruyter, Berlin, 1995.
20. P. Ribenboim, Square-classes of Fibonacci numbers, *Portugal Math.* **46** (1989), 159–175.
21. P. Ribenboim, Square-classes of $a^n - 1/a - 1$ and $a^n + 1$, *J. Sichuan Univ. Nat. Sci. Ed.* **26** (1989), 196–199.
22. P. Ribenboim and W. L. McDaniel, Square-classes in Lucas sequences, *Portugal. Math.* **48** (1991), 469–473.
23. P. Ribenboim and W. L. McDaniel, The square-classes of Lucas sequences having odd parameters, *C.R. Math. Rep. Acad. Sci. Canada* **18** (1996), 223–226.
24. T. N. Shorey and C. L. Stewart, On the diophantine equation $ax^{2t} + bx^t y + cy^2 = 1$ and pure powers in recurrence sequences, *Math. Scand.* **52** (1983), 24–36.
25. O. Wyler, Squares in the Fibonacci series, *Amer. Math. Monthly* **71** (1964), 220–222.