1

The Fibonacci Numbers and the Arctic Ocean

Introduction

There is indeed not much relation between the Fibonacci numbers and the Arctic Ocean, but I thought that this title would excite your curiosity for my lecture. You will be disappointed if you wished to hear about the Arctic Ocean, as my topic will be the sequence of Fibonacci numbers and similar sequences.

Like the icebergs in the Arctic Ocean, the sequence of Fibonacci numbers is the most visible part of a theory which goes deep: the theory of linear recurring sequences.

The so-called Fibonacci numbers appeared in the solution of a problem by Fibonacci (also known as Leonardo Pisano), in his book *Liber Abaci* (1202), concerning reproduction patterns of rabbits. The first significant work on the subject is by Lucas, with his seminal paper of 1878. Subsequently, there appeared the classical papers of Bang (1886) and Zsigmondy (1892) concerning prime divisions of special sequences of binomials. Carmichael (1913) published another fundamental paper where he extended to Lucas sequences the results previously obtained in special cases. Since then, I note the work of Lehmer, the applications of the theory in primality tests giving rise to many developments.

The subject is very rich and I shall consider here only certain aspects of it.

If, after all, your only interest is restricted to Fibonacci and Lucas numbers, I advise you to read the booklets by Vorob'ev (1963), Hoggatt (1969), and Jarden (1958).

1 Basic definitions

A. Lucas sequences

Let P, Q be non-zero integers, let $D = P^2 - 4Q$, be called the *discriminant*, and assume that $D \neq 0$ (to exclude a degenerate case).

Consider the polynomial $X^2 - PX + Q$, called the *characteristic polynomial*, which has the roots

$$\alpha = \frac{P + \sqrt{D}}{2} \quad \text{and} \quad \beta = \frac{P - \sqrt{D}}{2}.$$

Thus, $\alpha \neq \beta$, $\alpha + \beta = P$, $\alpha \cdot \beta = Q$, and $(\alpha - \beta)^2 = D$.

For each $n \geq 0$, define $U_n = U_n(P, Q)$ and $V_n = V_n(P, Q)$ as follows:

$$U_0{=}0\,,\ U_1{=}1\ ,\ U_n{=}P \cdot U_{n-1} - Q \cdot U_{n-2} \quad (\text{for } n \geq 2),$$
$$V_0{=}2\,,\ V_1{=}P\,,\ V_n{=}P \cdot V_{n-1} - Q \cdot V_{n-2} \quad (\text{for } n \geq 2).$$

The sequences $U = (U_n(P, Q))_{n\geq 0}$ and $V = (V_n(P, Q))_{n\geq 0}$ are called the (first and second) *Lucas sequences with parameters* (P, Q). $(V_n(P, Q))_{n\geq 0}$ is also called the *companion* Lucas sequence with parameters (P, Q).

It is easy to verify the following formal power series developments, for any (P, Q):

$$\frac{X}{1 - PX + QX^2} = \sum_{n=0}^{\infty} U_n X^n \qquad \text{and}$$
$$\frac{2 - PX}{1 - PX + QX^2} = \sum_{n=0}^{\infty} V_n X^n.$$

The Lucas sequences are examples of sequences of numbers produced by an algorithm.

At the nth step, or at time n, the corresponding numbers are $U_n(P, Q)$, respectively, $V_n(P, Q)$. In this case, the algorithm is a linear

recurrence with two parameters. Once the parameters and the initial values are given, the whole sequence—that is, its future values—is completely determined. But, also, if the parameters and two consecutive values are given, all the past (and future) values are completely determined.

B. Special Lucas sequences

I shall repeatedly consider special Lucas sequences, which are important historically and for their own sake. These are the sequences of Fibonacci numbers, of Lucas numbers, of Pell numbers, and other sequences of numbers associated to binomials.

(a) Let $P = 1$, $Q = -1$, so $D = 5$. The numbers $U_n = U_n(1, -1)$ are called the *Fibonacci numbers*, while the numbers $V_n = V_n(1, -1)$ are called the *Lucas numbers*. Here are the initial terms of these sequences:

Fibonacci numbers : 0, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...
Lucas numbers : 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 99, 322, ...

(b) Let $P = 2$, $Q = -1$, so $D = 8$. The numbers $U_n = U_n(2, -1)$ and $V_n = V_n(2, -1)$ are the *Pell numbers* and the *companion Pell numbers*. Here are the first few terms of these sequences:

$U_n(2, -1)$: 0, 1, 2, 5, 12, 29, 70, 169, ...
$V_n(2, -1)$: 2, 2, 6, 14, 34, 82, 198, 478, ...

(c) Let a, b be integers such that $a > b \geq 1$. Let $P = a + b$, $Q = ab$, so $D = (a - b)^2$. For each $n \geq 0$, let $U_n = \frac{a^n - b^n}{a-b}$ and $V_n = a^n + b^n$. Then it is easy to verify that $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = a+b = P$, and $(U_n)_{n\geq 0}$, $(V_n)_{n\geq 0}$ are the first and second Lucas sequences with parameters P, Q.

In particular, if $b = 1$, one obtains the sequences of numbers $U_n = \frac{a^n - 1}{a-1}$, $V_n = a^n + 1$; now the parameters are $P = a + 1$, $Q = a$. Finally, if also $a = 2$, one gets $U_n = 2^n - 1$, $V_n = 2^n + 1$, and now the parameters are $P = 3$, $Q = 2$.

C. Generalizations

At this point, it is appropriate to indicate extensions of the notion of Lucas sequences which, however, will not be discussed in this lecture. Such generalizations are possible in four directions, namely,

by changing the initial values, by mixing two Lucas sequences, by not demanding that the numbers in the sequences be integers, or by having more than two parameters.

Even though many results about Lucas sequences have been extended successfully to these more general sequences, and have found interesting applications, for the sake of definiteness I have opted to restrict my attention only to Lucas sequences.

(a) Let P, Q be integers, as before. Let T_0, T_1 be any integers such that T_0 or T_1 is non-zero (to exclude the trivial case). Let

$$W_0 = PT_0 + 2T_1 \quad \text{and} \quad W_1 = 2QT_0 + PT_1.$$

Let

$$\begin{aligned} T_n &= P \cdot T_{n-1} - Q \cdot T_{n-2} \qquad \text{and} \\ W_n &= P \cdot W_{n-1} - Q \cdot W_{n-2} \qquad (\text{for } n \geq 2). \end{aligned}$$

The sequences $(T_n(P,Q))_{n\geq 0}$ and $W_n(P,Q))_{n\geq 0}$ are the (first and the second) *linear recurrence sequences* with parameters (P,Q) and *associated to the pair* (T_0,T_1). The Lucas sequences are special, normalized, linear recurrence sequences with the given parameters; they are associated to $(0,1)$.

(b) Lehmer (1930) considered the following sequences. Let P, Q be non-zero integers, α, β the roots of the polynomial $X^2 - \sqrt{P}\cdot X + Q$, and define

$$L_n(P,Q) = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } n \text{ is odd,} \\ \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{if } n \text{ is even.} \end{cases}$$

$L = (L_n(P,Q))_{n\geq 0}$ is the *Lehmer sequence* with parameters P, Q. Its elements are integers. These sequences have been studied by Lehmer and subsequently by Schinzel and Stewart in several papers which also deal with Lucas sequences and are quoted in the bibliography.

(c) Let $\mathcal{R}$ be an integral domain which need not be $\mathbb{Z}$. Let P, $Q \in \mathcal{R}$, P, $Q \neq 0$, such that $D = P^2 - 4Q \neq 0$. The sequences $(U_n(P,Q))_{n\geq 0}$, $(V_n(P,Q))_{n\geq 0}$ of elements of $\mathcal{R}$ may be defined as for the case when $\mathcal{R} = \mathbb{Z}$.

Noteworthy cases are when $\mathcal{R}$ is the ring of integers of a number field (for example, a quadratic number field), or $\mathcal{R} = \mathbb{Z}[x]$ (or other

polynomial ring), or $\mathcal{R}$ is a finite field. For this latter situation, see SELMER (1966).
(d) Let P_0, P_1, ..., P_{k-1} (with $k \geq 1$) be given integers, usually subjected to some restrictions to exclude trivial cases. Let S_0, S_1, ..., S_{k-1} be given integers. For $n \geq k$, define:

$$S_n = P_0 \cdot S_{n-1} - P_1 \cdot S_{n-2} + P_2 \cdot S_{n-3} - \ldots + (-1)^{k-1} P_{k-1} \cdot S_{n-k}.$$

Then $(S_n)_{n\geq 0}$ is called a *linear recurrence sequence of order k, with parameters P_0, P_1, ..., P_{k-1} and initial values S_0, S_1, ..., S_{k-1}*. The case when $k = 2$ was seen above. For $k = 1$, one obtains the geometric progression $(S_0 \cdot P_0^n)_{n\geq 0}$.

There is great interest and still much to be done in the theory of linear recurrence sequences of order greater than 2.

2 Basic properties

The numbers in Lucas sequences satisfy many, many properties that reflect the regularity in generating these numbers.

A. Binet's formulas

BINET (1843) indicated the following expression in terms of the roots α, β of the polynomial $X^2 - PX + Q$:

(2.1) Binet's formulas:

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

The proof is, of course, very easy. Note that by Binet's formulas,

$$U_n(-P, Q) = (-1)^{n-1} U_n(P, Q) \qquad \text{and}$$
$$V_n(-P, Q) = (-1)^n V_n(P, Q).$$

So, for many of the following considerations, it will be assumed that $P \geq 1$.

B. Degenerate Lucas sequences

Let (P, Q) be such that the ratio $\eta = \alpha/\beta$ of roots of $X^2 - Px + Q$ is a root of unity. Then the sequences $U(P, Q)$, $V(P, Q)$ are said to be *degenerate*.

Now I describe all degenerate sequences. Since

$$\eta + \eta^{-1} = \frac{\alpha}{\beta} + \frac{\beta}{\alpha} = \frac{P^2 - 2Q}{Q}$$

is an algebraic integer and rational, it is an integer. From $|\frac{\alpha}{\beta} + \frac{\beta}{\alpha}| \le 2$ it follows $P^2 - 2Q = 0$, $\pm Q$, $\pm 2Q$, and this gives $P^2 = Q$, $2Q$, $3Q$, $4Q$. If $\gcd(P, Q) = 1$, then $(P, Q) = (1, 1)$, $(-1, 1)$, $(2, 1)$, or $(-2, 1)$, and the sequences are

$$\begin{array}{lrrrrrrrrrrr}
U(1,1) & : & 0, & 1, & 1, & 0, & -1, & -1, & 0, & 1, & 1, & 0, & \dots \\
U(-1,1) & : & 0, & 1, & -1, & 0, & 1, & -1, & 0, & \dots & & & \\
V(1,1) & : & 2, & 1, & -1, & -2, & -1, & 1, & 2, & 1, & -1, & -2, & \dots \\
V(-1,1) & : & 2, & -1, & -1, & 2, & -1, & -1, & 2, & \dots & & & \\
U(2,1) & : & 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & \dots & & \\
U(-2,1) & : & 0, & 1, & -2, & 3, & -4, & 5, & -6, & 7, & \dots & & \\
V(2,1) & : & 2, & 2, & 2, & 2, & 2, & 2, & 2, & 2, & \dots & & \\
V(-2,1) & : & 2, & -2, & 2, & -2, & 2, & -2, & 2, & -2, & \dots & &
\end{array}$$

From the discussion, if the sequence is degenerate, then $D = 0$ or $D = -3$.

C. Growth and numerical calculations

First, I note results about the growth of the sequence $U(P, Q)$.

(2.2) If the sequences $U(P, Q)$, $V(P, Q)$ are non-degenerate, then $|U_n|$, $|V_n|$ tend to infinity (as n tends to ∞).

This follows from a result of Mahler (1935) on the growth of coefficients of Taylor series. Mahler also showed

(2.3) If $Q \ge 2$, $\gcd(P, Q) = 1$, $D < 0$, then, for every $\varepsilon > 0$ and n sufficiently large,

$$|U_n| \ge |\beta^n|^{1-\varepsilon}.$$

The calculations of U_n, V_n may be performed as follows. Let

$$M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}.$$

Then for $n \ge 1$,

$$\begin{pmatrix} U_n \\ U_{n-1} \end{pmatrix} = M^{n-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

and

$$\begin{pmatrix} V_n \\ V_{n-1} \end{pmatrix} = M^{n-1} \begin{pmatrix} 2 \\ P \end{pmatrix}.$$

To compute a power M^k of the matrix M, the quickest method is to compute successively the powers M, M^2, M^4, ..., M^{2^e} where $2^e \leq k < 2^{e+1}$; this is done by successively squaring the matrices. Next, if the 2-adic development of k is $k = k_0 + k_1 \times 2 + k_2 \times 2^2 + \ldots + k_e \times 2^e$, where $k_i = 0$ or 1, then $M^k = M^{k_0} \times (M^2)^{k_1} \times \ldots \times (M^{2^e})^{k_e}$.

Note that the only factors actually appearing are those where $k_i = 1$.

Binet's formulas allow also, in some cases, a quick calculation of U_n and V_n.

If $D \geq 5$ and $|\beta| < 1$, then

$$\left| U_n - \frac{\alpha^n}{\sqrt{D}} \right| < \frac{1}{2} \quad (\text{for } n \geq 1),$$

and $|V_n - \alpha^n| < \frac{1}{2}$ (for n such that $n \cdot (-\log|\beta|) > \log 2$). Hence, cU_n is the closest integer to $\frac{\alpha^n}{\sqrt{D}}$, and V_n is the closest integer to α^n. This applies in particular to Fibonacci and Lucas numbers for which $D = 5$, $\alpha = (1 + \sqrt{5})/2 = 1.616\ldots$, (the golden number), $\beta = (1 - \sqrt{5})/2 = -0.616\ldots$.

It follows that the Fibonacci number U_n and the Lucas number V_n have approximately $n/5$ digits.

D. Algebraic relations

The numbers in Lucas sequences satisfy many properties. A look at the issues of *The Fibonacci Quarterly* will leave the impression that there is no bound to the imagination of mathematicians whose endeavor it is to produce newer forms of these identities and properties. Thus, there are identities involving only the numbers U_n, in others only the numbers V_n appear, while others combine the numbers U_n and V_n. There are formulas for U_{m+n}, U_{m-n}, V_{m+n}, V_{m-n} (in terms of U_m, U_n, V_m, V_n); these are the addition and subtraction formulas. There are also formulas for U_{kn}, V_{kn}, and U_{n^k}, V_{n^k}, U_n^k, cV_n^k (where $k \geq 1$) and many more.

I shall select a small number of formulas that I consider most useful. Their proofs are almost always simple exercises, either by applying Binet's formulas or by induction.

It is also convenient to extend the Lucas sequences to negative indices in such a way that the same recursion (with the given parameters P, Q) still holds.

(2.4) Extension to negative indices:

$$U_{-n} = -\frac{1}{Q^n}U_n, \quad V_{-n} = \frac{1}{Q^n}V_n \quad (\text{for } n \geq 1).$$

(2.5) U_n and V_n may be expressed in terms of P, Q. For example,

$$U_n = P^{n-1} - \binom{n-2}{1}P^{n-3}Q + \binom{n-3}{2}P^{n-5}Q^2 + \dots$$
$$+ (-1)^k\binom{n-1-k}{k}P^{n-1-2k}Q^k + \cdots + (\text{last summand})$$

where

$$(\text{last summand}) = \begin{cases} (-1)^{\frac{n}{2}-1}\binom{\frac{n}{2}}{\frac{n}{2}-1}PQ^{\frac{n}{2}-1} & \text{if } n \text{ is even,} \\ (-1)^{\frac{n-1}{2}}Q^{\frac{n-1}{2}} & \text{if } n \text{ is odd.} \end{cases}$$

Thus, $U_n = f_n(P, Q)$, where $f_n(X, Y) \in \mathbb{Z}[X, Y]$. The function f_n is isobaric of weight $n-1$, where X has weight 1 and Y has weight 2.

Similarly, $V_n = g_n(P, Q)$, where $g_n \in \mathbb{Z}[X, Y]$. The function g_n is isobaric of weight n, where X has weight 1, and Y has weight 2.

(2.6) Quadratic relations:

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

for every $n \in \mathbb{Z}$.

This may also be put in the form:

$$U_{n+1}^2 - PU_{n+1}U_n + QU_n^2 = Q^n.$$

(2.7) Conversion formulas:

$$DU_n = V_{n+1} - QV_{n-1},$$
$$V_n = U_{n+1} - QU_{n-1},$$

for every $n \in \mathbb{Z}$.

(2.8) Addition of indices:

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

for all m, $n \in \mathbb{Z}$.

Other formulas of the same kind are:

$$2U_{m+n} = U_m V_n + U_n V_m,$$
$$2Q^n U_{m-n} = U_m V_n - U_n V_m,$$

for all m, $n \in \mathbb{Z}$.

(2.9) Multiplication of indices:

$$U_{2n} = U_n V_n,$$
$$V_{2n} = V_n^2 - 2Q^n,$$
$$U_{3n} = U_n(V_n^2 - Q^n) = U_n(DU_n^2 + 3Q^n),$$
$$V_{3n} = V_n(V_n^2 - 3Q^n),$$

for every $n \in \mathbb{Z}$.

More generally, if $k \geq 3$ it is possible to find by induction on k formulas for U_{kn} and V_{kn}, but I shall refrain from giving them explicitly.

E. Divisibility properties

(2.10) Let $U_m \neq 1$. Then, U_m divides U_n if and only if $m \mid n$.
Let $V_m \neq 1$. Then, V_m divides V_n if and only if $m \mid n$ and n/m is odd.

For the next properties, it will be assumed that $\gcd(P, Q) = 1$.

(2.11) $\gcd(U_m, U_n) = U_d$, where $d = \gcd(m, n)$.

(2.12)

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

where $d = \gcd(m, n)$.

(2.13)

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

where $d = \gcd(m, n)$.

(2.14) If $n \geq 1$, then $\gcd(U_n, Q) = 1$ and $\gcd(V_n, Q) = 1$.

3 Prime divisors of Lucas sequences

The classical results about prime divisors of terms of Lucas sequences date back to EULER, (for numbers $\frac{a^n - b^n}{a-b}$), to LUCAS (for Fibonacci and Lucas numbers), and to CARMICHAEL (for other Lucas sequences).

A. The sets $\mathcal{P}(U)$, $\mathcal{P}(V)$, and the rank of appearance.

Let $\mathcal{P}$ denote the set of all prime numbers. Given the Lucas sequences $U = (U_n(P,Q))_{n\geq 0}$, $V = (V_n(P,Q))_{n\geq 0}$, let

$$\mathcal{P}(U) = \{p \in \mathcal{P} \mid \exists n \geq 1 \text{ such that } U_n \neq 0 \text{ and } p \mid U_n\},$$
$$\mathcal{P}(V) = \{p \in \mathcal{P} \mid \exists n \geq 1 \text{ such that } V_n \neq 0 \text{ and } p \mid V_n\}.$$

If U, V are degenerate, then $\mathcal{P}(U)$, $\mathcal{P}(V)$ are easily determined sets.

Therefore, it will be assumed henceforth that U, V are non-degenerate and thus, $U_n(P,Q) \neq 0$, $V_n(P,Q) \neq 0$ for all $n \geq 1$.

Note that if p is a prime dividing both p, q, then $p \mid U_n(P,Q)$, $p \mid V_n(P,Q)$, for all $n \geq 2$. So, for the considerations which will follow, there is no harm in assuming that $\gcd(P,Q) = 1$. So, (P,Q) belongs to the set

$$\mathcal{S} = \{(P,Q) \mid P \geq 1,\ \gcd(P,Q) = 1,\ P^2 \neq Q,\ 2Q,\ 3Q,\ 4Q\}.$$

For each prime p, define

$$\rho_U(p) = \begin{cases} n & \text{if } n \text{ is the smallest positive index where } p \mid U_n, \\ \infty & \text{if } p \nmid U_n \text{ for every } n > 0, \end{cases}$$

$$\rho_V(p) = \begin{cases} n & \text{if } n \text{ is the smallest positive index where } p \mid V_n, \\ \infty & \text{if } p \nmid V_n \text{ for every } n > 0. \end{cases}$$

We call $\rho_U(n)$ (respectively $\rho_V(p)$)) is called the *rank of appearance* of p in the Lucas sequence U (respectively V).

First, I consider the determination of even numbers in the Lucas sequences.

(3.1) Let $n \geq 0$. Then:

$$U_n \text{ even} \iff \begin{cases} P \text{ even} & Q \text{ odd}, & n \text{ even}, \\ & \text{or} & \\ P \text{ odd} & Q \text{ odd}, & 3 \mid n, \end{cases}$$

and

$$V_n \text{ even} \iff \begin{cases} P \text{ even} & Q \text{ odd}, & n \geq 0, \\ & \text{or} & \\ P \text{ odd} & Q \text{ odd}, & 3 \mid n. \end{cases}$$

Special Cases. For the sequences of Fibonacci and Lucas numbers ($P = 1$, $Q = -1$), one has:
U_n is even if and only if $3 \mid n$,
V_n is even if and only if $3 \mid n$.
For the sequences of numbers $U_n = \frac{a^n - b^n}{a-b}$, $V_n = a^n + b^n$, with $a > b \geq 1$, $\gcd(a, b) = 1$, $p = a + b$, $q = ab$, one has:
If a, b are odd, then U_n is even if and only if n is even, while V_n is even for every n.
If a, b have different parity, then U_n, V_n are always odd (for $n \geq 1$).

With the notations and terminology introduced above the result **(3.1)** may be rephrased in the following way:

(3.2) $2 \in \mathcal{P}(U)$ if and only if Q is odd

$$\rho_U(2) = \begin{cases} 2 & \text{if} \quad P \text{ even}, & Q \text{ odd}, \\ 3 & \text{if} \quad P \text{ odd}, & Q \text{ odd}, \\ \infty & \text{if} \quad P \text{ odd}, & Q \text{ even}, \end{cases}$$

$2 \in \mathcal{P}(V)$ if and only if Q is odd

$$\rho_V(2) = \begin{cases} 1 & \text{if} \quad P \text{ even}, & Q \text{ odd}, \\ 3 & \text{if} \quad P \text{ odd}, & Q \text{ odd}, \\ \infty & \text{if} \quad P \text{ odd}, & Q \text{ even}. \end{cases}$$

Moreover, if Q is odd, then $2 \mid U_n$ (respectively $2 \mid V_n$) if and only if $\rho_U(2) \mid n$ (respectively $\rho_V(2) \mid n$).

This last result extends to odd primes:

(3.3) Let p be an odd prime.
If $p \in \mathcal{P}(U)$, then $p \mid U_n$ if and only if $\rho_U(p) \mid n$.
If $p \in \mathcal{P}(V)$, then $p \mid V_n$ if and only if $\rho_V(p) \mid n$ and $\frac{n}{\rho_V(p)}$ is odd.

Now I consider odd primes p and indicate when $p \in \mathcal{P}(U)$.

(3.4) Let p be an odd prime.
If $p \nmid P$ and $p \mid Q$, then $p \nmid U_n$ for every $n \geq 1$.
If $p \mid P$ and $p \nmid Q$, then $p \mid U_n$ if and only if n is even.
If $p \nmid PQ$ and $p \mid D$, then $p \mid U_n$ if and only if $p \mid n$.
If $p \nmid PQD$, then p divides $U_{\psi_D}(p)$ where $\psi_D(p) = p - (\frac{D}{p})$ and $(\frac{D}{p})$ denotes the Legendre symbol.

Thus,

$$\mathcal{P}(U) = \{p \in \mathcal{P} \mid p \nmid Q\},$$

so $\mathcal{P}(U)$ is an infinite set.

The more interesting assertion concerns the case where $p \nmid PQD$, the other ones being very easy to establish.

The result may be expressed in terms of the rank of appearance:

(3.5) Let p be an odd prime.
If $p \nmid P$, $p \mid Q$, then $\rho_U(p) = \infty$.
If $p \mid P$, $p \nmid Q$, then $\rho_U(p) = 2$.
If $p \nmid PQ$, $p \mid D$, then $\rho_U(p) = p$.
If $p \nmid PQD$, then $\rho_U(p) \mid \Psi_D(p)$.

Special Cases. For the sequences of Fibonacci numbers ($P = 1$, $Q = -1$), $D = 5$ and $5 \mid U_n$ if and only if $5 \mid n$.
If p is an odd prime, $p \neq 5$, then $p \mid U_{p-(\frac{5}{p})}$, so $\rho_U(p) \mid (p - (\frac{5}{p}))$.
Because $U_3 = 2$, it follows that $\mathcal{P}(U) = \mathcal{P}$.
Let $a > b \geq 1$, $\gcd(a, b)$, $P = a + b$, $Q = ab$, $U_n = \frac{a^n - b^n}{a-b}$.
If p divides a or b but not both a, b, then $p \nmid U_n$ for all $n \geq 1$.
If $p \nmid ab$, $p \mid a + b$, then $p \mid U_n$ if and only if n is even.
If $p \nmid ab(a + b)$ but $p \mid a - b$, then $p \mid U_n$ if and only if $p \mid n$.
If $p \nmid ab(a + b)(a - b)$, then $p \mid U_{p-1}$. (Note that $D = (a - b)^2$).
Thus, $\mathcal{P}(U) = \{p : p \nmid ab\}$.

Taking $b = 1$, if $p \nmid a$, then $p \mid U_{p-1}$, hence $p \mid a^{p-1} - 1$ (this is Fermat's Little Theorem, which is therefore a special case of the last assertion of **(3.4)**); it is trivial if $p \mid (a+1)(a-1)$.

The result **(3.4)** is completed with the so-called *law of repetition*, first discovered by LUCAS for the Fibonacci numbers:

(3.6) Let p^e (with $e \geq 1$) be the exact power of p dividing U_n. Let $f \geq 1$, $p \nmid k$. Then, p^{e+f} divides U_{nkp^f}. Moreover, if $p \nmid Q$, $p^e \neq 2$, then p^{e+f} is the exact power of p dividing U_{nkp^e}.

It was seen above that Fermat's Little Theorem is a special case of the assertion that if p is a prime and $p \nmid PQD$, then p divides $U_{\Psi_D(p)}$. I indicate now how to reinterpret EULER's classical theorem.

If α, β are the roots of the characteristic polynomial $X^2 - PX + Q$, define the symbol

$$\left(\frac{\alpha,\beta}{2}\right) = \begin{cases} 1 & \text{if } Q \text{ is even,} \\ 0 & \text{if } Q \text{ is odd, } P \text{ is even,} \\ -1 & \text{if } Q \text{ is odd, } P \text{ is odd,} \end{cases}$$

and for any odd prime p

$$\left(\frac{\alpha,\beta}{p}\right) = \begin{cases} \left(\dfrac{D}{p}\right) & \text{if } p \nmid D, \\ 0 & \text{if } p \mid D. \end{cases}$$

Let $\Psi_{\alpha,\beta}(p) = p - (\frac{\alpha,\beta}{p})$ for every prime p. Thus, using the previous notation, $\Psi_{\alpha,\beta}(p) = \Psi_D(p)$ when p is odd and $p \nmid D$.

For $n = \prod_p p^e$, define the *generalized Euler function*

$$\Psi_{\alpha,\beta}(n) = n \prod_r \frac{\Psi_{\alpha,\beta}(p)}{p},$$

so $\Psi_{\alpha,\beta}(p^e) = p^{e-1}\Psi_{\alpha,\beta}(p)$ for each prime p and $e \geq 1$. Define also the *Carmichael function* $\lambda_{\alpha,\beta}(n) = \operatorname{lcm}\{\Psi_{\alpha,\beta}(p^e)\}$. Thus, $\lambda_{\alpha,\beta}(n)$ divides $\Psi_{\alpha,\beta}(n)$.

In the special case where $\alpha = a$, $\beta = 1$, and a is an integer, then $\Psi_{a,1}(p) = p - 1$ for each prime p not dividing a. Hence, if $\gcd(a,n) = 1$, then $\Psi_{a,1}(n) = \varphi(n)$, where φ denotes the classical Euler function.

The generalization of EULER's theorem by CARMICHAEL is the following:

(3.7) n divides $U_{\lambda_{\alpha,\beta}(n)}$ hence, also, $U_{\Psi_{\alpha,\beta}(n)}$.

It is an interesting question to evaluate the quotient $\frac{\Psi_D(p)}{\rho_U(p)}$. It was shown by JARDEN (1958) that for the sequence of Fibonacci numbers,

$$\sup\left\{\frac{p-(\frac{5}{p})}{\rho_U(D)}\right\}=\infty$$

(as p tends to ∞). More generally, KISS (1978) showed:

(3.8) (a) For each Lucas sequence $U_n(P,Q)$,

$$\sup\left\{\frac{\Psi_D(p)}{\rho_U(p)}\right\}=\infty.$$

(b) There exists $C>0$ (depending on P, Q) such that

$$\frac{\Psi_D(p)}{\rho_U(p)}<C\frac{p}{\log p}.$$

Now I turn my attention to the companion Lucas sequence $V=(V_n(P,Q))_{n\geq 0}$ and I study the set of primes $\mathcal{P}(V)$. It is not known how to describe explicitly, by means of finitely many congruences, the set $\mathcal{P}(V)$. I shall indicate partial congruence conditions that are complemented by density results.

Because $U_{2n}=U_nV_n$, it then follows that $\mathcal{P}(V)\subseteq\mathcal{P}(U)$. It was already stated that $2=\mathcal{P}(V)$ if and only if Q is odd.

(3.9) Let p be an odd prime.
If $p\nmid P$, $p\mid Q$, then $p\nmid V_n$ for all $n\geq 1$.
If $p\mid P$, $p\nmid Q$, then $p\mid V_n$ if and only if n is odd.
If $p\nmid PQ$, $p\mid D$, then $p\nmid V_n$ for all $n\geq 1$.
If $p\nmid PQD$, then $p\mid V_{\frac{1}{2}\Psi_D(p)}$ if and only if $(\frac{Q}{P})=-1$.
If $p\nmid PQD$ and $(\frac{Q}{p})=1$, $(\frac{D}{p})=-(\frac{-1}{p})$, then $p\nmid V_n$ for all $n\geq 1$.

The above result implies that $\mathcal{P}(V)$ is an infinite set.* One may further refine the last two assertions; however, a complete determination of $\mathcal{P}(V)$ is not known.

In terms of the rank of appearance, **(3.9)** can be rephrased as follows:

*This was extended by WARD (1954) for all binary linear recurrences

(3.10) Let p be an odd prime.
If $p \mid P$, $p \nmid Q$, then $\rho_V(p) = 1$.
If $p \nmid P$, $p \mid Q$, then $\rho_V(p) = \infty$.
If $p \nmid PQ$, $p \mid D$, then $\rho_V(p) = \infty$.
If $p \nmid PQD$, $(\frac{Q}{p}) = -1$, then $\rho_V(p)$ divides $\frac{1}{2}\Psi_D(p)$.
If $p \nmid PQD$, $(\frac{Q}{p}) = 1$, $(\frac{D}{p}) = -(\frac{-1}{p})$, then $\rho_V(p) = \infty$.

The following conjecture has not yet been established in general, but has been verified in special cases, described below:

Conjecture. For each companion Lucas sequence V, the limit

$$\delta(V) = \lim \frac{\pi_V(x)}{\pi(x)}$$

exists and is strictly greater than 0.

Here, $\pi(x) = \#\{p \in \mathcal{P} \mid p \le x\}$ and $\pi_V(x) = \#\{p \in \mathcal{P}(V) \mid p \le x\}$. The limit $\delta(V)$ is the *density* of the set of prime divisors of V among all primes.

Special Cases. Let $(P, Q) = (1, -1)$, so V is the sequence of Lucas numbers. Then the above results may be somewhat completed. Explicitly:
If $p \equiv 3, 7, 11, 19 \pmod{20}$, then $p \in \mathcal{P}(V)$.
If $p \equiv 13, 17 \pmod{20}$, then $p \notin \mathcal{P}(V)$.
If $p \equiv 1, 9 \pmod{20}$ it may happen that $p \in \mathcal{P}(V)$ or that $p \notin \mathcal{P}(V)$.

Jarden (1958) showed that there exist infinitely many primes $p \equiv 1 \pmod{20}$ in $\mathcal{P}(V)$ and also infinitely many primes $p \equiv 1 \pmod{20}$ not in $\mathcal{P}(V)$. Further results were obtained by Ward (1961) who concluded that there is no finite set of congruences to decide if an arbitrary prime p is in $\mathcal{P}(V)$.

Inspired by a method of Hasse (1966), and the analysis of Ward (1961), Lagarias (1985) showed that, for the sequence V of Lucas numbers, the density is $\delta(V) = \frac{2}{3}$.

Brauer (1960) and Hasse (1966) studied a problem of Sierpiński, namely, determine the primes p such that 2 has an even order modulo p, equivalently, determine the primes p dividing the numbers $2^n + 1 = V_n(3, 2)$. He proved that $\delta(V(3, 2)) = 17/24$. Lagarias pointed out that Hasse's proof shows also that if $a \ge 3$ is square-free, then $\delta(V(a + 1, a)) = 2/3$; see also a related paper of Hasse (1965).

Laxton (1969) considered, for each $a \geq 2$, the set $\mathcal{W}(a)$ of all binary linear recurrences W with W_0, W_1 satisfying $W_1 \neq W_0$, $W_1 \neq aW_0$, and $W_n = (a+1)W_{n-1} - aW_{n-2}$, for $n \geq 2$. This set includes the Lucas sequences $U(a+1, a)$, $V(a+1, a)$. For each prime p, let

$$e_p(a) = \begin{cases} 0 & \text{if } p \mid a, \\ \text{order of } a \bmod b & \text{if } p \nmid a. \end{cases}$$

Laxton gave a heuristic argument to the effect that if the limit, as x tends to ∞, of

$$\frac{1}{\pi(x)} \sum_{p \leq x} \frac{e_p(a)}{p-1}$$

exists, then it is the expected (or average value), for any $W \in \mathcal{W}(a)$, of the density of primes in $\mathcal{P}(\mathcal{W})$ (that is, the set of primes dividing some W_n).

Stephens (1976) used a method of Hooley (1967) who had proved, under the assumption of a generalized Riemann's hypothesis, Artin's conjecture that 2 is a primitive root modulo p for infinitely many primes p. Let $a \geq 2$, a not a proper power. Assume the generalized Riemann hypothesis for the Dedekind ζ function of all fields $\mathbb{Q}(a^{1/n}, \zeta_k)$, where ζ_k is a primitive kth root of 1. Then, for every $x \geq 2$,

$$\sum_{p \leq x} \frac{e_p(a)}{p-1} = c(a) \frac{x}{\log x} + \mathrm{O}\left(\frac{x \log\log x}{(\log x)^2} \right);$$

by the Prime Number Theorem, the limit considered above exists and is equal to $c(a)$. Stephens evaluated $c(a)$. Let

$$C = \prod_p \left(1 - \frac{p}{p^3 - 1} \right),$$

let $a = a_1 \cdot (a_2)^2$ where a_1 is square-free, let r be the number of distinct prime factors of a_1, and let f be defined as

$$f = \begin{cases} -\dfrac{2}{5} & \text{if } a_1 \equiv 1 \pmod 4, \\ -\dfrac{1}{64} & \text{if } a_1 \equiv 2 \pmod 4, \\ -\dfrac{1}{20} & \text{if } a_1 \equiv 3 \pmod 4. \end{cases}$$

Then,

$$c(a) = C\left[1 - (-1)^r f \prod_{\substack{q \mid a_1 \\ q \text{ prime}}} \frac{q}{q^3 - q - 1}\right].$$

Stephens also showed that even without the assumption of the generalized Riemann hypothesis the above estimation holds on average. Precisely, given $a \geq 2$ (as before), $e > 1$, and $x \geq 1$, there exists $c_1 > 0$ such that if $N > \exp\{c_1(\log x)^{\frac{1}{2}}\}$, then

$$\sum_{x \leq N} \sum_{p \leq x} \frac{e_p(a)}{p-1} = C \int_1^x \frac{dt}{t} + \mathrm{O}\left(\frac{x}{(\log x)^e}\right).$$

B. Primitive factors of Lucas sequences

Let p be a prime. If $\rho_U(p) = n$ (respectively $\rho_V(p) = n$), then p is called a *primitive factor* of $U_n(P,Q)$ (respectively $V_n(P,Q)$). Denote by $\mathrm{Prim}(U_n)$ the set of primitive factors of U_n, similarly, by $\mathrm{Prim}(V_n)$ the set of primitive factors of V_n. Let $U_n = U_n^* \cdot U_n'$, $V_n = V_n^* \cdot V_n'$, where $\gcd(U_n^*, U_n') = 1$, $\gcd(V_n^*, V_n^1) = 1$, $p \mid U_n^*$ (respectively $p \mid V_n^*$) if and only if p is a primitive factor of U_n (respectively V_n). U_n^*, (respectively V_n^*) is called the *primitive part* of U_n (respectively V_n). From $U_{2n} = U_n \cdot V_n$ it follows that $U_{2n}^* \mid V_n^*$, hence, $\mathrm{Prim}(U_{2n}) \subseteq \mathrm{Prim}(V_n^*)$. It is not excluded that $U_n^* = 1$ (respectively $V_n^* = 1$); I shall discuss this question.

a Existence of primitive factors

The study of primitive factors of Lucas sequences originated with Bang and Zsigmondy for special Lucas sequences (see below). The first main theorem is due to Carmichael (1913):

(3.11) Let $(P,Q) \in \mathcal{S}$ and assume that $D > 0$.

1. If $n \neq 1, 2, 6$, then $\mathrm{Prim}(U_n) \neq \varnothing$, with the only exception $(P,Q) = (1,-1)$, $n = 12$ (which gives the Fibonacci number $U_{12} = 144$).
   Moreover, if D is a square and $n \neq 1$, then $\mathrm{Prim}(U_n) \neq \varnothing$, with the only exception $(P,Q) = (3,2)$, $n = 6$ (which gives the number $2^6 - 1 = 63$).
2. If $n \neq 1, 3$, then $\mathrm{Prim}(V_n) \neq \varnothing$, with the only exception $(P,Q) = (1,-1)$, $n = 6$ (which gives the Lucas numbers

$V_6 = 18$).
Moreover, if D is a square and $n \neq 1$, then $\mathrm{Prim}(V_n) \neq \varnothing$, with the only exception $(P, Q) = (3, 2)$, $n = 3$ (which gives the number $2^3 + 1 = 9$).

In his paper, CARMICHAEL also proved that if p does not divide D and $p \in \mathrm{Prim}(U_n)$, then $p \equiv \pm 1 \pmod{n}$, while if $p \in \mathrm{Prim}(V_n)$, then $p \equiv \pm 1 \pmod{2n}$.

The result of CARMICHAEL was extended by LEKKERKERKER (1953):

Even without assuming that $\gcd(P, Q) = 1$, if $D > 0$, there exist only finitely many n such that $U_n(P, Q)$ (respectively $V_n(P, Q)$) does not have a primitive factor.

DURST (1961) proved:

(3.12) Let $(P, Q) \in \mathcal{S}$ and $D > 0$. Then, $U_6(P, Q)$ has no primitive factor if and only if one the following conditions holds:

1. $P = 2^{t+1} - 3r$, $Q = (2^t - r)(2^t - 3r)$ where $t \geq 1$, $2^{t+1} > 3r$, and r is odd and positive.
2. $P = 3^s k$, $Q = 3^{2s-1}k^2 - 2^t$ where $s \geq 1$, $t \geq 0$, $k \equiv \pm 1 \pmod{6}$, and $3^{2s-1}k^2 < 2^{t+2}$.

Thus, there exist infinitely many (P, Q) as above with $U_6(P, Q)$ having no primitive factor. DURST dealt also with parameters (P, Q) where $\gcd(P, Q)$ may be greater than 1.

(3.13) Let I be a finite set of integers, with $1 \in I$. Then, there are infinitely many pairs (P, Q), with $P \geq 1$, $P \neq Q$, $2Q$, $3Q$, $4Q$, $P^2 - 4Q > 0$, such that $\mathrm{Prim}(U(P, Q)) = I$.

If $D < 0$, the above result does not hold without modification. For example, for $(P, Q) = (1, 2)$ and $n = 1, 2, 3, 5, 8, 12, 13, 18$, $\mathrm{Prim}(U_n) = \varnothing$.

In 1962, SCHINZEL investigated the case when $D < 0$. In 1974, he proved a general result of which the following is a corollary.

(3.14) There exists $n_0 > 0$ such that for all $n \geq n_0$, $(P, Q) \in \mathcal{S}$, $U_n(P, Q)$, $V_n(P, Q)$ have a primitive factor.

The proof involves Baker's lower bounds for linear forms in logarithms and n_0 is effectively computable. It is important to stress that n_0 is independent of the parameters. Stewart (1977a) showed that $n_0 \leq e^{452}4^{67}$. Stewart also showed that if $4 < n$, $n \neq 6$, there exist only finitely many Lucas sequences $U(P,Q)$, $V(P,Q)$ (of the kind indicated), which may in principle be explicitly determined, and such that $U_n(P,Q)$ (respectively $V_n(P,Q)$) does not have a primitive factor.

Voutier (1995) used a method developed by Tzanakis (1989) to solve Thue's equations and determined for each n, $4 < n \leq 30$, $n \neq 6$, the finite set of parameters $(P,Q) \in \mathcal{S}$ such that $U_r(P,Q)$ has no primitive factor.

The next result of Győry (1981) concerns terms of Lucas sequences with prime factors in a given set. If E is a finite set of primes, let $E^{\times}$ denote the set of natural numbers, all of whose prime factors belong to E.

(3.15) Let $s > 1$ and $E = \{p \text{ prime} \mid p \leq s\}$. There exist $c_1 = c_1(s) > 0$, $c_2 = c_2(s) > 0$, effectively computable, such that if $(P,Q) \in \mathcal{S}$, $4 < n$, and $U_n(P,Q) \in E^{\times}$, then

$$n \leq \max\{s+1,\, e^{452} \cdot 2^{67}\},$$

$\max\{P, |Q|\} \leq c_1$, and $|U_n(P,Q)| \leq c_2$.

In 1982, Győry gave an explicit value for the constants. An interesting corollary is the following:

(3.16) Let $s > 1$ and $E = \{p \text{ prime} \mid p \leq s\}$. There exists $c_3 = c_3(s) > 0$, effectively computable, such that if $a > b \geq 1$ are integers, $\gcd(a,b) = 1$, if $3 < n$, $\frac{a^n - b^n}{a-b} = m \in E^{\times}$, then $n < s$ and $\max\{a, m\} < c_3$.

Special Cases. The following very useful theorem was proved by Zsigmondy (1892); the particular case where $a = 2$, $b = 1$ had been obtained earlier by Bang (1886). Zsigmondy's theorem was rediscovered many times (Birkhoff (1904), Carmichael (1913), Kanold (1950), Artin (1955), and Lüneburg (1981) who gave a simpler proof). For an accessible proof, see Ribenboim (1994)

Let $a > b \geq 1$, $\gcd(a,b) = 1$, and consider the sequence of binomials

$$(a^n - b^n)_{n \geq 0}.$$

If $P = a + b$, $Q = ab$, then $a^n - b^n = U_n(P, Q) \cdot (a - b)$. The prime p is called a *primitive factor* of $a^n - b^n$ if $p \mid a^n - b^n$ but $p \nmid a^m - b^m$ for all m, $1 \leq m < n$. Let $\mathrm{Prim}(a^n - b^n)$ denote the set of all primitive factors of $a^n - b^n$. Clearly, if $n > 1$, then $\mathrm{Prim}(a^n - b^n) = \mathrm{Prim}(U_n(P, Q)) \setminus \{p \mid p \text{ divides } a - b\}$.

(3.17) Let $a > b \geq 1$, $\gcd(a, b) = 1$.

1. For every $n > 1$, the binomial $a^n - b^n$ has a primitive factor, except in the following cases:

   $a = 2$, $b = 1$, $n = 6$ (this gives $2^6 - 1 = 63$),
   a, b are odd, $a + b$ is a power of 2, $n = 2$.

   Moreover, each primitive factor of $a^n - b^n$ is of the form $kn + 1$.
2. For every $n > 1$, the binomial $a^n + b^n$ has a primitive factor, except for $a = 2$, $b = 1$, $n = 3$ (this gives $2^3 + 1 = 9$).

b The number of primitive factors

Now I consider the primitive part of terms of Lucas sequences and discuss the number of distinct prime factors of U_n^*, V_n^*. The following question remains open: Given $(P, Q) \in \mathcal{S}$, do there exist infinitely many $n \geq 1$ such that $\#(\mathrm{Prim}(U_n)) = 1$, respectively $\#(\mathrm{Prim}(V_n)) = 1$, that is, U_n^* (respectively V_n^*) is a prime power? This question is probably very difficult to answer. I shall discuss a related problem in the next subsection (c).

Now I shall indicate conditions implying

$$\#(\mathrm{Prim}(U_n)) \geq 2 \quad \text{and} \quad \#(\mathrm{Prim}(V_n)) \geq 2.$$

If c is any non-zero integer, let $k(c)$ denote the *square-free kernel* of c, that is, c divided by its largest square factor. If $(P, Q) \in \mathcal{S}$, let $M = \max\{P^2 - 4Q, P^2\}$, let $\kappa = \kappa(P, Q) = k(MQ)$, and define

$$\eta = \eta(P, Q) = \begin{cases} 1 & \text{if } \kappa \equiv 1 \pmod 4, \\ 2 & \text{if } \kappa \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

Schinzel (1963a) proved (see also Rotkiewicz (1962) for the case when $Q > 0$ and $D > 0$):

(3.18) There exist effectively computable finite subsets $\mathcal{M}_0$, $\mathcal{N}_0$ of $\mathcal{S}$ and for every $(P, Q) \in \mathcal{S}$ an effectively computable integer $n_0(P, Q) > 0$ such that if $(P, Q) \in \mathcal{S}$, $\neq 1, 2, 3, 4, 6$, and $\frac{n}{\eta\kappa}$ is odd, then $\#(\mathrm{Prim}(U_n(P, Q))) \geq 2$, with the following exceptions:

1. $D = P^2 - 4Q > 0$:

$$n = \eta \cdot |\kappa| \text{ and } (P,Q) \in \mathcal{M}_0\,;$$
$$n = 3 \cdot \eta \cdot |\kappa| \text{ and } (P,Q) \in \mathcal{N}_0\,;$$
$$(n,P,Q) = (2D,1,-2),\ (2D,3,2)$$

2. $D = P^2 - 4Q < 0$:

$$(n,P,Q) \text{ with } n \le n_0(P,Q).$$

Thus, for each $(P,Q) \in \mathcal{S}$ there exist infinitely many n with $\#(\mathrm{Prim}(U_n(P,Q))) \ge 2$. Schinzel gave explicit finite sets $\mathcal{M}$, $\mathcal{N}$ containing respectively the exceptional set $\mathcal{M}_0, \mathcal{N}_0$, which were later completely determined by Brillhart and Selfridge, but this calculation remained unpublished. Later, I shall invoke the following corollary:

(3.19) Let $(P,Q) \in \mathcal{S}$ with Q a square and $D > 0$. If $n > 3$, then

$$\#(\mathrm{Prim}(U_n(P,Q))) \ge 2,$$

with the exception of $(n,P,Q) = (5,3,1)$.

Thus, in particular, $U_n(P,Q)$ is not a prime when $n > 3$ and Q is a square, except for $(n,P,Q) = (5,3,1)$.

Since $\mathrm{Prim}(U_n(P,Q)) \subseteq \mathrm{Prim}(V_n(P,Q))$, it is easy to deduce from **(3.16)** conditions which imply that $\#(\mathrm{Prim}(V_n(P,Q))) \ge 2$; in particular, for each $(P,Q) \in \mathcal{S}$ there are infinitely many such indices n.

These results have been strengthened in subsequent papers by Schinzel (1963), (1968), but it would be too technical to quote them here. It is more appropriate to consider:

Special Cases. Let $a > b \ge 1$ be relatively prime integers, let $P = a+b$, $Q = ab$, so $U_n(P,Q) = \frac{a^n-b^n}{a-b}$, $V_n(P,Q) = a^n+b^n$. Even for these special sequences it is not known if there exist infinitely many n such that $\#\,\mathrm{Prim}(U_n(P,Q)) = 1$, respectively $\#\,\mathrm{Prim}(V_n(P,Q)) = 1$.

Schinzel (1962b) showed the following result, which is a special case of **(3.16)**. Let $\kappa = k(a,b)$,

$$\eta = \begin{cases} 1 & \text{if } \kappa \equiv 1 \pmod 4, \\ 2 & \text{if } \kappa \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

(3.20) Under the above hypotheses:

1. If $n > 20$ and $\frac{n}{\eta\kappa}$ is an odd integer, then $\#\operatorname{Prim}(\frac{a^n-b^n}{a-b}) \geq 2$.
2. If $n > 10$, κ is even, and $\frac{n}{\kappa}$ is an odd integer, then $\#\operatorname{Prim}(a^n+b^n) \geq 2$.

Thus, there exist infinitely many n such that $\#\operatorname{Prim}(\frac{a^n-b^n}{a-b}) \geq 2$, respectively $\#\operatorname{Prim}(a^n+b^n) \geq 2$. SCHINZEL also showed:

(3.21) With the above hypotheses, if $\kappa = c^h$ where $h \geq 2$ when $k(c)$ is odd, and $h \geq 3$ when $k(c)$ is even, then there exist infinitely many n such that $\#\operatorname{Prim}(\frac{a^n-b^n}{a-b}) \geq 3$.

However, for arbitrary (a,b) with $a > b \geq 1$, $\gcd(a,b) = 1$, it is not known if there exist infinitely many n with $\#\operatorname{Prim}(\frac{a^n-b^n}{a-b}) \geq 3$.

c Powers dividing the primitive part

Nothing is known about powers dividing the primitive part, except that it is a rare occurrence. To size up the difficulty of the question, it is convenient to consider right away the very special case where $(P,Q) = (3,2)$, so $U_n = 2^n - 1$, $V_n = 2^n + 1$. Recall that if $n = q$ is a prime, then $U_q = 2^q - 1$ is called a *Mersenne number*, usually denoted $M_q = U_q = 2^q - 1$. Also, if $n = 2^m$, then $V_{2^m} = 2^{2^m} + 1$ is called a *Fermat number* and the notation $F_m = V_{2^m} = 2^{2^m} + 1$ is used.

The following facts are easy to show: $\gcd(M_q, M_p) = 1$ when $p \neq q$, and $\gcd(F_m, F_n) = 1$ when $m \neq n$. It follows that M_q, F_m are equal to their primitive parts.

A natural number which is a product of proper powers is said to be a *powerful number*.

I indicate below several statements which are related, but have never been proved to be true.

(M) There exist infinitely many primes p such that M_p is square-free.
(M′) There exist infinitely many primes such that M_p is not powerful.
(F) There exist infinitely many n such that F_n is square-free.
(F′) There exist infinitely many n such that F_n is not powerful.
(B) There exist infinitely many n such that the primitive part of $2^n - 1$ is square-free.
(B′) There exist infinitely many n such that the primitive part of $2^n - 1$ is not powerful.
(C) There exist infinitely many n such that the primitive part of $2^n + 1$ is square-free.

(C′) There exist infinitely many n such that the primitive part of $2^n + 1$ is not powerful.

I shall discuss these and related conjectures in Chapter 9 where it will be explained why the proof of any of the above conjectures should be very difficult.

d The greatest prime factor of terms of Lucas sequences.

The problem of estimating the size of the greatest prime division of terms of Lucas sequences has been the object of many interesting papers.

If n is a natural number, let $P[n]$ denote the greatest prime factor of n, and let $\nu(n)$ denote the number of distinct prime factors of n. So, the number $q(n)$ of distinct square-free factors of n is $q(n) = 2^{\nu(n)}$. There have also been studies to estimate the size of $Q[n]$, the largest square-free factor of n, but I shall not consider this question.

For every $n \geq 1$, let $\Phi_n(X, Y) \in \mathbb{Z}[X, Y]$ be the nth homogenized cyclotomic polynomial

$$\Phi_n(X, Y) = \prod_{\substack{\gcd(i,n)=1 \\ 1 \leq i \leq n}} (X - \zeta^i Y)$$

where ζ is a primitive nth root of 1; so, $\Phi_n(X, Y)$ has degree $\varphi(n)$ (the EULER totient of n).

If P, Q are non-zero integers, $D = P^2 - 4Q \neq 0$ and α, β the roots of $X^2 - PX + Q$, then $\Phi_n(\alpha, \beta) \in \mathbb{Z}$ (for $n \geq 2$) and $\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha, \beta)$.

It follows easily that

$$P\left[\frac{\alpha^n - \beta^n}{\alpha - \beta}\right] \geq P[\Phi_n(\alpha, \beta)],$$

$$P[\alpha^n - \beta^n] \geq P[\Phi_n(\alpha, \beta)],$$

$$P[\alpha^n + \beta^n] \geq P[\Phi_{2n}(\alpha, \beta)].$$

Therefore, it suffices to find lower estimates for $P[\Phi_n(\alpha, \beta)]$.

The first result was given by ZSIGMONDY (1892) and again by BIRKHOFF (1904): *If a, b are relatively prime integers, $a > b \geq 1$, then $P[a^n - b^n] \geq n + 1$ and $P[a^n + b^n] \geq 2n + 1$ (with the exception $2^3 + 1 = 9$).* SCHINZEL added to this result (1962): *If ab is a square*

or the double of a square, then $P[a^n - b^n] \geq 2n+1$, *except for* $a = 2$, $b = 1$, *and* $n = 4$, 6, 12.

In his work on primitive factors of LUCAS sequences with $D > 0$, CARMICHAEL (1913) showed that if $n > 12$, then $P[U_n] \geq n - 1$ and $P[V_n] \geq 2n - 1$. ERDÖS (1965) conjectured:

$$\lim_{n\to\infty} \frac{P[2^n - 1]}{n} = \infty.$$

This problem, as well as related questions which are still unsolved, has been extensively studied by STEWART (see STEWART (1975, 1977b); SHOREY (1981); STEWART (1982, 1985)). Several of the results which I shall describe concern the greatest prime factor when the index n belongs to some set with asymptotic density 1.

A subset S of $\mathbb{N}$ has asymptotic density γ, $0 \leq \gamma \leq 1$, where

$$\lim_{N\to\infty} \frac{\#\{n \in S \mid n \leq N\}}{N} = \gamma.$$

For example, the set $\mathcal{P}$ of prime numbers has asymptotic density 0.

Combining the Prime Number Theorem with the fact that each primitive factor of $\Phi_n(a, b)$ is of the form $hn + 1$ yields:

(3.22) There exists a set T of asymptotic density 1 such that

$$\lim_{\substack{n\to\infty \\ n\in T}} \frac{P[\Phi(a, b)]}{n} = \infty.$$

In particular, $\lim_{n\to\infty, n\in T} \frac{P[2^n-1]}{n} = \infty$ where T is a set with asymptotic density 1. The above result was made more precise and extended for sequences with arbitrary discriminant $D \neq 0$. Let $0 \leq \kappa \leq 1/\log 2$ and define the set

$$\mathcal{N}_\kappa = \{n \in \mathbb{N} \mid n \text{ has at most } \kappa \log\log n \text{ distinct prime factors}\}.$$

For example, $\mathcal{P} \subset \mathcal{N}_\kappa$, for every κ as above. A classical result (see the book of HARDY and WRIGHT (1938)) is the following: If $0 \leq \kappa \leq 1/\log 2$, then $\mathcal{N}_\kappa$ has asymptotic density equal to 1.

In other words, "most" natural numbers have "few" distinct prime factors.

The following result is due to STEWART (1977b) for α, β real, and to SHOREY (1981) for arbitrary α, β.

(3.23) Let κ, α, β be as above. If $n \in \mathcal{N}_\kappa$, $n \geq 3$, then

$$P[\Phi_n(\alpha,\beta)] \geq C\varphi(n)\frac{\log n}{q(n)}$$

where $C \geq 0$ is an effectively computable number depending only on α, β, and κ.

Recall that $q(n) = 2^{\nu(n)}$ and $\nu(n) \leq \kappa \log\log n$. It follows, with appropriate constants $C_1 > 0$ and $C_2 > 0$, that

$$P[\Phi_n(\alpha,\beta)] > C_1\frac{n\log n}{2^{\nu(n)}\log(1+\nu(n))}$$

and

$$P[\Phi_n(\alpha,\beta)] > C_2\frac{n\log n^{1-\kappa\log 2}}{\log\log\log n}.$$

In particular, the above estimates hold for $n \in \mathcal{N}_\kappa$, $n > 3$, and each Lucas sequence $U_n(P,Q)$, $V_n(P,Q)$, and $\alpha^n - \beta^n$.

Since $\nu(p) = 1$ for each prime p, then

$$P[a^p - b^p] \geq Cp\log p,$$
$$P[a^p + b^p] \geq Cp\log p$$

(with appropriate $C > 0$). In particular, for the Mersenne numbers $M_p = 2^p - 1$,

$$P[2^p - 1] \geq Cp\log p,$$

and for the Fermat number $F_m = 2^{2^m} + 1$,

$$P[2^{2^m} + 1] \geq Cm \times 2^m,$$

but this estimate may also be obtained in a more direct way, as suggested by D. Knayswick.

Stewart obtained also sharper, more technical expressions for lower bounds of $P[\Phi_n(\alpha,\beta)]$, and he conjectured that

$$P[\Phi(\alpha,\beta)] > C[\varphi(n)]^2$$

for α, β real, for all $n > 3$, where $C > 0$ is an effectively computable number (depending on α, β). This statement is true if n is square-free.

Using a more refined form of Baker's lower bounds for linear forms in logarithms (as given by Waldschmidt (1980)), Stewart (1982) proved the following result, valid for all $n > C_0$ (an absolute constant):

(3.24) For every $(P,Q) \in \mathcal{S}$ there exists an effectively computable number $C_1 = C_1(P,Q) > 0$ such that if $n > C_0$, then $P[U_n]$, $P[V_n]$ are bounded below by

$$\max\left\{n-1, C_1 \frac{n \log n}{q(n)^{\frac{4}{3}}}\right\}.$$

The following result is non-effective, but gives sharper bounds on sets of asymptotic density 1 (STEWART (1982)):

(3.25) Let $f : \mathbb{N} \to \mathbb{R}_{>0}$ be any function such that $\lim f(n) = 0$. For each $(P,Q) \in \mathcal{S}$ there exists a set $T \subseteq \mathbb{N}$ of asymptotic density 1, such that if $n \in T$, then

$$P[U_n] \geq f(n) \frac{n(\log n)^2}{\log\log n}.$$

STEWART obtained further results about linear recurrence sequences other than Lucas sequences, and even for linear recurrence sequences of order greater than 2, but they fall beyond my scope. For a comprehensive survey, see STEWART (1985).

An interesting result related to these questions had already been obtained by MAHLER (1966):

(3.26) Let $Q \geq 2$, $D = P^2 - 4Q < 0$, and let E be a finite set of primes and denote by $E^{\times}[U_n]$ the largest factor of U_n, where prime factors all belong to E. If $0 < \epsilon < \frac{1}{2}$, there exists $n_0 > 1$ such that if $n > n_0$, then $\left|\frac{U_n}{E^{\times}[U_n]}\right| > Q^{(1/2-\epsilon)n}$. In particular, $\lim P[U_n] = \infty$.

The proof used p-adic methods.

4 Primes in Lucas sequences

Let U, V be the Lucas sequences with parameters $(P,Q) \in S$.

The main questions about primes in Lucas sequences are the following:

1. Does there exist $n > 1$ such that $U_n(P,Q)$, respectively $V_n(P,Q)$, is a prime?
2. Do there exist infinitely many $n > 1$ such that $U_n(P,Q)$, respectively $V_n(P,Q)$, is a prime?

I discuss the various possibilities, indicating what is known in the most important special cases.

The following is an example of a Lucas sequence with only one prime term, namely U_2:
$U(3,1)$: 0 1 3 8 21 55 144 377 987 ...

This was remarked after **(3.19)**. Similarly, if $a > b \geq 1$, with a, b odd, if $P = a + b$, $Q = ab$, then $V_n(P,Q) = a^n + b^n$ is even for every $n \geq 1$, so it is not a prime.

Applying CARMICHAEL's theorem **(3.11)** on the existence of primitive factors, it follows easily that:

(4.1) If $D > 0$ and $U_n(P,Q)$ is a prime, then $n = 2$, 4 or n is an odd prime. If $V_n(P,Q)$ is a prime, then n is a prime or a power of 2.

This result is not true if $D < 0$, as this example shows:

Let $(P,Q) = (1,2)$, so $D = -7$ and

$U(1,2)$: 0 1 1 −1 −3 −1 5 7 −3 −17 −11 23 45 −1 −91 −89 ...

In this example, U_6, U_8, U_9, U_{10}, U_{15}, ..., are primes.

Similarly, in $V(1,2)$, for example, the terms $|V_9|$, $|V_{10}|$ are primes.

Special Cases. In (1999), DUBNER and KELLER indicated all the indices $n < 50000$ for which the Fibonacci number U_n, or the Lucas number V_n, are known to be prime: U_n is known to be a prime for n = 3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, 131, 137, 359, 431, 433, 449, 509, 569, 571, $2971^{(W)}$, $4723^{(M)}$, $5387^{(M)}$, $9311^{(DK)}$ [W: discovered by H. C. WILLIAMS; M: discovered by F. Morain; DK: discovered by H. DUBNER and W. KELLER].

Moreover, for $n < 50000$, U_n is a probable prime for n = 9677, 14431, 25561, 30757, 35999, 37511 (and for no other $n < 50000$). This means that these numbers were submitted to tests indicating that they are composite.

For $n \leq 50000$, V_n is known to be a prime for n = 2, 4, 5, 7, 8, 11, 13, 16, 17, 19, 31, 37, 41, 47, 53, 61, 71, 79, 113, 313, 353, $503^{(W)}$, $613^{(W)}$, $617^{(W)}$, $863^{(W)}$, $1097^{(DK)}$, $1361^{(DK)}$, $4787^{(DK)}$, $4793^{(DK)}$, $5851^{(DK)}$, $7741^{(DK)}$, $10691^{(DK)}$, $14449^{(DK)}$ [W: discovered by H. C. WILLIAMS; DK: discovered by H. DUBNER and W. KELLER].

Moreover, V_n is a probable prime for n = 8467, 12251, 13963, 19469, 35449, 36779, 44507 (and for no other $n \leq 50000$).

Due to the size of the probable primes, an actual prime certification is required to be done.

The paper of DUBNER and KELLER contains a lot more factorizations; it is a continuation of previous work of numerous other mathematicians; we call attention to JARDEN (1958), the edition of JARDEN's book by BRILLHART (1973), and the paper by BRILLHART (1988) which contains complete factorizations of U_n (for $n \leq 1000$) and of V_n (for $n \leq 500$).

If $a = 2$, $b = 1$, the associated Lucas sequences are $U_n = 2^n - 1$ and $V_n = 2^n + 1$.

Now, if U_n is a prime, then $n = q$ is a prime, and $M_q = U_q = 2^q - 1$ is a prime Mersenne number. If V_n is a prime, then $n = 2^m$, and $F_m = 2^{2^m} + 1$ is a prime Fermat number.

Up to now, only 37 Mersenne primes are known, the largest one being M_{302137}, proved prime in 1999; it has more than 2 million digits. On the other hand, the largest known Fermat prime number is F_4. For a detailed discussion of Mersenne numbers and Fermat numbers, see my book *The Little Book of Big Primes* (1991a) or the up-to-date Brazilian edition (1994).

It is believed that there exist infinitely many Mersenne primes. Concerning Fermat primes, there is insufficient information to support any conjecture.

5 Powers and powerful numbers in Lucas sequences

In this section, I deal with the following questions. Let U, V be the Lucas sequences with parameters $(P, Q) \in \mathcal{S}$. Let $k \geq 1$, $h \geq 2$, and consider the set

$$\mathcal{C}_{U,k,h} = \{U_n \mid U_n = kx^h, \text{ with } |x| \geq 2\}.$$

Let $\mathcal{C}_{U,k} = \bigcup_{h \geq 2} \mathcal{C}_{U,k,h}$, so $\mathcal{C}_{U,k}$ consists of all U_n of the form $U_n = kx^h$ for some $|x| \geq 2$ and $h \geq 2$. If $k = 1$, one obtains the set of all U_n that are proper powers.

Similarly, let

$$\mathcal{C}^*_{U,k} = \{U_n \mid U_n = kt \text{ where } t \text{ is a powerful number}\}.$$

If $k = 1$, one obtains the set of all U_n which are powerful numbers.

Corresponding definitions are made for the sets $\mathcal{C}_{V,k,h}$ and $\mathcal{C}_{V,k}*$ associated to the sequence V.

The basic question is to find out if, and when, the above sets are empty, finite, or infinite, and, whenever possible, to determine the sets explicitly.

A related problem concerns the square-classes in the sequences U, V.

U_n, U_m are said to be *square-equivalent* if there exist integers $a, b \neq 0$ such that $U_m a^2 = U_n b^2$ or, equivalently, $U_m U_n$ is a square. This is clearly an equivalence relation on the set $\{U_n \mid n \geq 1\}$ whose classes are called the *square-classes of the sequence* U. If U_n, U_m are in the same square-class, and if $d = \gcd(U_n, U_m)$, then $U_m = dx^2$, $U_n = dy^2$, and conversely.

The square-classes of the sequence V are defined in a similar manner.

Concerning square-classes, the problems are the same: to determine if there are square-classes which are not trivial, that is, having more than one element; next, to ascertain if there are only finitely many nontrivial square-classes, if a square-class may be finite and, if possible, to determine explicitly the square-classes.

If $k \geq 1$, the notation $k\square$ indicates a number of the form kx^2, with $x \geq 2$; thus, $\square$ indicates a square greater than 1.

The first results on these questions were the determinations of those Fibonacci and Lucas numbers that are squares. This was achieved using rather elementary, but clever, arguments. In my presentation, I prefer to depart from the order in which the subject unfolded, and, instead, to give first the general theorems.

A. General theorems for powers

The general theorem of Shorey (1981, 1983) (valid for all non-degenerate binary recurrence sequences) was proved using sharp lower bounds for linear forms in logarithms by Baker (1973), plus a p-adic version by van der Poorten (1977), assisted by another result of Kotov (1976).

A result of Shorey (1977) may also be used, as suggested by Pethö.

(5.1) Let $(P, Q) \in \mathcal{S}$, $k \geq 1$. There exists an effectively computable number $C = C(P, Q, k) > 0$ such that if $n \geq 1$, $|x| \geq 2$, $h \geq 2$ and

$U_n = kx^h$, then n, $|x|$, $h < C$. A similar statement holds for the sequence V.

In particular, in a given Lucas sequence there are only finitely many terms which are powers.

STEWART's paper (1980) contains also the following result, suggested by MIGNOTTE and WALDSCHMIDT. For $h \geq 2$, $n \geq 1$, let $[n]^h$ denote the h-power closest to n.

(5.2) If $Q = \pm 1$, then

$$\lim_{n\to\infty} |U_n - [U_r]^h| = \infty.$$

This is achieved by showing that for every d, there exists an effectively computable number $C = C(P, d) > 0$ such that if $U_n = x^h + d$ with $|x| \geq 1$, $h \geq 2$, then n, $|x|$, $h < C$.

The above general results are not sufficient to determine explicitly all the terms U_n of the form kx^h, because the bounds indicated are too big.

PETHÖ (1982) gave the following extension of **(5.1)** (valid for all non-degenerate binary recurrences):

(5.3) Let E be a finite set of primes, $E^\times$ the set of integers all of whose prime factors belong to E. Given $(P, Q) \in \mathcal{S}$, there exists an effectively computable number $C > 0$, depending only on P, Q, and E, such that if $n \geq 1$, $|x| \geq 2$, $h \geq 2$, $k \in E^\times$, and $U_n = kx^h$, then n, $|x|$, h, $k \geq C$. A similar result holds for the sequence V.

B. Explicit determination in special sequences

Now I shall consider special sequences, namely, those with parameters $(1, -1)$ (the Fibonacci and Lucas numbers), those with parameters $(2, -1)$ (the Pell numbers), and those with parameters $(a + 1, a)$, where $a > 1$, in particular with parameters $(3, 2)$.

The questions to be discussed concern squares, double squares, other multiples of squares, square-classes, cubes, and higher powers.

The results will be displayed in a table (see page 35).

a Squares

The only squares in the sequence of Fibonacci numbers are $U_1 = U_2 = 1$ and $U_{12} = 144$. This result was proved independently in 1964 by COHN and WYLER.

The only square in the sequence of Lucas numbers is $V_3 = 4$, proved by Cohn (1964a).

One proof uses only divisibility properties and algebraic identities involving the Fibonacci and Lucas numbers. Another proof is based on the solution of the equations $X^2 - 5Y^4 = \pm 4$, $X^4 - 5Y^2 = \pm 4$.

For the parameters $(P, Q) = (2, -1)$, which give the sequences of Pell numbers, it is easy to see that V_n is never a square. The only U_n (with $n > 1$) which is a square is $U_7 = 169$. The proof follows from a study of the equation $X^2 - 2Y^4 = -1$, which was the object of a long paper by Ljunggren (1942c). Robbins reported this result in (1984) and it was again discovered by Pethö (1991) using a method of Diophantic approximation and computer calculations.

Let $a \geq 2$, $P = a + 1$, and $Q = a$. Nagell (1921a) (and Ljunggren (1942c), who completed the work) proved: If $\frac{a^n-1}{a-1}$ is a square, and $n > 1$, then $(a, n) = (3, 5)$ or $(7, 4)$.

Ko (1960, 1964) proved: If $a^n + 1$ is a square, then $(a, n) = (2, 3)$. This result answered a long-standing problem.

A short proof of Ko's theorem is due to Chein (1976); another one was given by Rotkiewicz (1983) involving the computation of Jacobi symbols.

Detailed proofs of the above results are given in my book *Catalan's Conjecture* (1994).

The special case of parameters $(3, 2)$ gives the numbers $U_n = 2^n - 1$, $V_n = 2^n + 1$, and it is very easy to see that $2^n - 1 = \square$ only for $n = 1$, and $2^n + 1 = \square$ only for $n = 3$.

b Double squares

Cohn (1964b) showed for Fibonacci numbers U_n and Lucas numbers V_n:

If $U_n = 2\square$, then $n = 3$ or 6, giving $U_3 = 2$, $U_6 = 8$.

If $V_n = 2\square$, then $n = 0$ or 6, giving $V_0 = 2$, $V_6 = 18$.

I have not found in the literature the determination of the Pell numbers $U_n(2, -1)$, $V_n(2, -1)$, $\frac{a^n-1}{a-1}$, $a^n + 1$ which are double squares (apart from the trivial cases).

c Square-classes

Cohn (1972) determined the square-classes of Fibonacci and Lucas numbers (and even of more general sequences). In (1989a), I used another method to solve this problem:

The square-classes of Fibonacci numbers consist all of one number, except $\{U_1, U_2, U_{12}\}$ and $\{U_3, U_6\}$.

The square-classes of Lucas numbers consist only of one number, except $\{V_1, V_3\}$, $\{V_0, V_6\}$.

The determination of the square-classes of sequences of Pell numbers remains to be done.

For the square-classes of the sequences $U_n = \frac{a^n-1}{a-1}$, $V_n = a^n + 1$ $(n \geq 1)$, see RIBENBOIM (1989b).

The square-classes of the sequence U consist all of only one number. If a is even, the square-classes of V are also reduced to one element. Furthermore, there is an effectively computable number $C > 0$ such that if

$$(a^n + 1)(a^m + 1) = \square$$

with $m \neq n$, a odd, then a, m, $n < C$. So, only finitely many square-classes are not trivial and they are all finite.

d Numbers of the form $k\square$ with $k \geq 3$

Let $k \geq 3$, assumed without loss of generality to be square-free. Often, k is taken to be an odd prime.

I have mentioned some papers concerning the special Lucas sequences with terms of the form $k\square$. On this matter, it is unavoidable to be incomplete and I wish to apologize to any author whose work I did not report.

On Fibonacci numbers, respectively Lucas numbers, of the form $p\square$ (where p is an odd prime) there are papers by STEINER (1980), ROBBINS (1983a), and GOLDMAN (1988).

STEINER showed that if $U_n = 3\square$, then $n = 4$. ROBBINS proved that if $U_n = p\square$, where p is a prime, $p \equiv 3 \pmod 4$ or $3 < p < 10000$, then $p = 3001$. GOLDMAN showed that if $p = 3$, 7, 47 or 2207, and the Lucas number $V_n = p\square$, then $V_n = p$; note that then $n = 2^e$ (with $e = 1, 2, 3, 4$).

For the sequence $\frac{a^n-1}{a-1}$, $(n \geq 0, a \geq 2)$, there is also a partial result by ROTKIEWICZ (1983): if $a \equiv 0$ or $3 \pmod 4$ and $n > 1$, n odd, then $\frac{a^n-1}{a-1} \neq n\square$. This is obtained using the calculation of Jacobi symbols.

e Cubes

LONDON and FINKELSTEIN (1969) showed that the only Fibonacci cubes are $U_1 = U_2 = 1$ and $U_6 = 8$, while the only Lucas number which is a cube is $V_1 = 1$. The proof by LONDON and FINKELSTEIN requires the explicit solution of the cubic diophantine equations $x^2 \pm 100 = y^3$, subject to certain conditions. The latter result was obtained by LAGARIAS (1981) as well as by PETHÖ (1983) with a different proof using WALDSCHMIDT's form (1980) of the lower bound for linear forms in logarithms, followed by computer calculations. PETHÖ also gave results about Fibonacci numbers of the form px^3 or p^2x^3. For Pell numbers, PETHÖ (1991) showed that for $n > 1$, $U_n(2,-1)$ is never a cube.

NAGELL (1920, 1921b) (work completed by LJUNGGREN (1942a, 1943)) showed that if $\frac{a^n-1}{a-1}$ is a cube, with $n = 3$, then $a = 18$; moreover, if $n > 3$, then $n \not\equiv -1 \pmod 6$, which is just a partial result.

The work of NAGELL and LJUNGGREN also showed that $a^n + 1$ is a cube only in trivial cases.

These results are of course trivial for the numbers $2^n - 1$, $2^n + 1$, which cannot be cubes. They were given by GÉRONO (1870).

f Higher powers

Nobody has as yet found any power higher than a cube among Fibonacci or Lucas numbers (except, trivially, 1).

In (1978) and (1983b), ROBBINS showed, if $q \geq 5$, q a prime, and if n is the smallest index such that the Fibonacci number U_n is a qth power, then n is a prime. Thus, if p is a prime dividing U_n, then $n = \rho_U(p)$, but also $p^q \mid U_n$, a fact which seems very unlikely to happen. The same result was also obtained in (1983) by PETHÖ.

PETHÖ (1991) showed also that a Pell number $U_n(2,-1)$ (with $n > 1$) is not a power (higher than a square).

The work of NAGELL and LJUNGGREN already quoted gives: If $\frac{a^n-1}{a-1} = y^m$ where $m > 3$, $n \geq 3$, then $n \neq 3$. Moreover, from NAGELL (1920) and LJUNGGREN (1943), necessarily 3 and 4 do not divide n when $m > 3$ (this is a partial result only).

INKERI communicated to me: If $\frac{a^n-1}{a-1}$ is a pth power (with $a > 1$, $n > 1$ and p a prime), then the p-adic value $v_p(a) \neq 1$ (see the proof in my book *Catalan's Conjecture* (1994), page 120).

The problem to determine if a^n+1 can be equal to a higher power, or the similar problem for a^n-1, amounts to the determination of all consecutive powers of integers. CATALAN (1844) conjectured that 8 and 9 are the only consecutive powers. This problem remains open, and my book *Catalan's Conjecture* (already quoted) is entirely devoted to this question. Let it be said here only that, with a clever use of BAKER's lower bounds for linear forms in logarithms, TIJDEMAN (1976) showed:

(5.4) There exists an effectively computable number $C > 0$ such that if $a^n + 1 = b^m$ with $a, b \geq 1$, $m \geq 2$, then $a, b, m, n < C$.

LANGEVIN (1976) calculated an upper bound for C:

$$C < e^{e^{e^{e^{730}}}}$$

which is beyond what imagination can dare.

It would be desirable to lower his bound so that numerical computer calculations may eventually confirm Catalan's conjecture.

Of course, it is easy to show for the special sequence of numbers $2^n - 1$, $2^n + 1$ that they are not higher powers (different from 1). This was done by GÉRONO (1870).

g Addendum on repunits

A number is called a *repunit* if all its digits in base 10 are equal to 1. Such numbers are of the form

$$\frac{10^n - 1}{10 - 1} = U_n(11, 10).$$

A repunit (different from 1) is not a square, nor a fifth power. This follows from INKERI's result, already quoted. An independent proof was given by BOND (see my book *Catalan's Conjecture* (1994), page 120).

INKERI (1972) showed that a repunit (different from 1) is not a cube. Another proof was given by ROTKIEWICZ (1981) (see *Catalan's Conjecture*, pages 119, 120).

The question of the determination of repunits which are powers has now been completely solved—only the trivial repunit 1 is a power. This result is in a reprint of BUGEAUD (1999). The proof requires bounds in linear forms in two p-adic logarithms plus extensive computations with modular techniques to solve Thue equations.

Sequences	Fibonacci	Lucas	$U_n(2,-1)$	$V_n(2,-1)$	$U_n(3,2)$	$V_n(3,2)$	$\frac{a^n-1}{a-1}$ $(a>2)$	a^n+1 $(a>2)$
□	! Cohn Wyler	! Cohn	! Ljungren	! Ljungren	! trivial	! Frénicle de Bessy	! Nagell Ljungren	! Ko
2□	! Cohn	! Cohn	?	?	! trivial	! trivial	?	?
Square classes	! Cohn Ribenboim	! Cohn Ribenboim	?	?	! trivial	! trivial	! Ribenboim	!? Ribenboim
Cubes	! London and Finkelstein	! London and Finkelstein	! Pethö	?	! Gérono	! Gérono	!? Nagell Ljungren	! Nagell Ljungren
Higher Powers	!? Shorey and Stewart or Pethö				! Gérono	! Gérono	!? Nagell	!? Tijdeman

h Recapitulation

It is perhaps a good idea to assemble in a table the various results about special Lucas sequences discussed about.

The sign (!) indicates that the problems has been solved; (?) means the problem is completely open, or that I could not find it treated in the literature; the sign (!?) means that only partial results are known, cases remaining still unsettled.

C. Uniform explicit determination of multiples, squares, and square-classes for certain families of Lucas sequences

It is an interesting and somewhat unexpected feature in the determination of squares, double-squares, and square-classes, that certain

infinite families of Lucas sequences can be treated at the same time, providing uniform results.

In a series of papers, COHN (1966, 1967, 1968, 1972) has linked this problem to the solution of certain quartic equations where he obtained results for all (non-degenerate) sequences with parameters $(P, \pm 1)$, where $P \geq 1$ is odd.

Some results are also valid for a certain infinite, but thin, set of even parameter P, as will be soon indicated.

MCDANIEL and I have devised a new method, involving the computation of Jacobi symbols, applicable to parameters (P, Q) with P, Q odd, $P \geq 1$, $\gcd(P, Q) = 1$, and $D > 0$.

These results were announced in (1992), and detailed proofs will soon appear.

a Squares and double squares

The next results are by MCDANIEL and RIBENBOIM .

It is assumed that $P \geq 1$, P, Q are odd, $\gcd(P, Q) = 1$, and $D = P^2 - 4Q > 0$.

(5.5)
1. If $U_n = \square$, then $n = 1$, 2, 3, 6, or 12.
2. $U_2 = \square$ if and only if $P = \square$.
3. $U_3 = \square$ if and only if $P^2 - Q = \square$.
4. $U_6 = \square$ if and only if $P = 3\square$, $P^2 - Q = 2\square$, $P^2 - 3Q = 6\square$.
5. $U_{12} = \square$ if and only if $P = \square$, $P^2 - Q = 2\square$, $P^2 - 2Q = 3\square$, $P^2 - 3Q = \square$, and $(P^2 - 2Q)^2 - 3Q^2 = 6\square$.

The determination of all allowable (P, Q) for which $U_3(P, Q) = \square$ is obvious, and clearly there are infinitely many such pairs (P, Q).

(5.6) The set of allowable parameters (P, Q) for which $U_6(P, Q) = \square$ is parameterized by the set $\{(s, t) \mid \gcd(s, t) = 1,\ s \text{ even},\ t \text{ odd},\ st \equiv 1 \pmod 3\}$ by putting

$$P = \frac{(s^2 - t^2)^2}{3}, \quad Q = (a^2 - b^2)^2 - \frac{8(a^2 + b^2 + ab)^2}{q}$$

with

$$a = \frac{2(s^2 + t^2 + st)}{3}, \quad b = \frac{s^2 + t^2 + st}{3},$$

and three other similar forms for P, Q (not listed here for brevity). In particular, there are infinitely many (P, Q) for which $U_6(P, Q) = \square$.

$(P, Q) = (1, -1)$ is the only known pair such that $U_{12}(P, Q) = \square$. It is not known if the system of equations given in **(5.5)** part (5) admits other nontrivial solution.

(5.7)
1. If $U_n = 2\square$, then $n = 3$ or 6.
2. $U_3 = 2\square$ if and only if $P^2 - Q = 2\square$.
3. $U_6 = 2\square$ if and only if $P = \square$, $P^2 - Q = 2\square$, and $P^2 - 3Q = \square$.

The set of allowable parameters (P, Q) for which $U_3(P, Q) = 2\square$ is clearly infinite and easily parameterized.

The set of allowable (P, Q) for which $U_6(P, Q) = 2\square$ is not completely known. However, the subset of all $(1, Q)$ for which $U_6(1, Q) = 2\square$ may be parameterized and shown to be infinite.

Concerning the sequence V, the results are the following:

(5.8)
1. If $V_n = \square$, then $n = 1$, 3, or 5.
2. $V_3 = \square$ if and only if $P = \square$.
3. $V_3 = \square$ if and only if both P and $P^2 - 3Q$ are squares, or both P and $P^2 - 3Q$ are $3\square$.
4. $V_5 = \square$ if and only if $P = 5\square$ and $P^4 - 5P^2Q + 5Q^2 = 5\square$.

(5.9) The set of all allowable (P, Q) for which $V_3(P, Q) = \square$ is infinite and parameterized as follows:

First type: $P = s^2$, $Q = \frac{s^4 - t^2}{3}$ where s is odd, t even, 3 does not divide st, $\gcd(s, t) = 1$, and $s^2 < 2t$;

Second type: $P = 3s^2$, $Q = 3s^4 - t^2$, where s is odd, t is even, 3 divides s, $\gcd(s, t) = 1$, and $\sqrt{3}s^2 < 2t$.

(5.10) The set of all allowable (P, Q) for which $V_5(P, Q) = \square$ is infinite and parameterized as follows:

First type: $P = 5s^2t^2$, $Q = -\frac{s^8 - 50s^4t^4 + 125t^8}{4}$ where s, t are odd, 5 does not divide s, $\gcd(s, t) = 1$, and $|s| > \left[\frac{25 + 5\sqrt{5}}{2}\right]^{\frac{1}{4}} t$.

Second type: $P = s^2t^2$, $Q = -\frac{5(s^8 - 10s^4t^4 + 5t^8)}{4}$ where s, t are odd, 5 does not divide s, $\gcd(s, t) = 1$, and $|s| > \left[\frac{49 + \sqrt{1901}}{10}\right]^{\frac{1}{4}} t$.

(5.11)
1. If $V_n = 2\square$, then $n = 3$ or 6.
2. $V_3 = 2\square$ if and only if either $P = \square$, $P^2 - 3Q = 2\square$, or $P = 3\square$, $P^2 - 3Q = 6\square$.

3. $V_6 = 2\square$ if and only if $P^2 - 2Q = 3\square$, and $(P^2 - 2Q)^2 - 3Q^2 = 6\square$.

(5.12) The set of all allowable (P, Q) for which $V_6(P, Q) = 2\square$ is infinite and parameterized as follows: $P = s^2$, $Q = 3s^4 - 2t^2$ where s is odd, $\gcd(s, t) = 1$, 3 does not divide s, and $\sqrt{6}s^2 < 4t$.

At my request, J. Top determined the pairs (P, Q) for which $V_6(P, Q) = 2\square$ (see the paper of McDaniel and Ribenboim already quoted):

(5.13) The allowable (P, Q) for which $V_6(P, Q) = 2\square$ correspond to the rational points of a certain elliptic curve with group of rational points isomorphic to $(\mathbb{Z}/2) \times \mathbb{Z}$. These points give rise to infinitely many pairs of allowable parameters. $(P, Q) = (1, -1)$ corresponds to the points of order 2; $(5, -1)$ corresponds to the generator of the subgroup of infinite order.

Other solutions may be calculated from the group law, that is, with the classical chord and tangent method. Thus

$$(P, Q) = (29, -4801), (4009, 3593279), (58585, -529351744321), \ldots$$

are also possible parameters.

It is much more difficult to deal with the case where P or Q is even. The first known results are due to Cohn (1972).

(5.14) Let $Q = -1$ and $P = V_m(A, -1)$, where A is odd, $m \equiv 3 \pmod 6$.

1. If $U_n(P, -1) = \square$, then $n = 1$ or $n = 2$, and $P = 4$ or 36.
2. If $U_n(P, -1) = 2\square$, then $n = 4$, $P = 4$.
3. If $V_n(P, -1) = \square$, then $n = 1$, $P = 4$ or 36.
4. If $U_n(P, -1) = 2\square$, then $n = 2$, and $P = 4$ or 140.

(5.15) Let $Q = 1$ and $P = V_m(A, 1)$ where A is odd and 3 divides m.

1. If $U_n(P, 1) = \square$, then $n = 1$.
2. If $U_n(P, 1) = 2\square$, then $n = 2$, and $P = 18$ or 19602.
3. $V_n(P, 1) = \square$ is impossible.
4. If $V_n(P, 1) = 2\square$, then $n = 1$, and $P = 18$ or 19602.

Note that there are infinitely many even $P = V_m(A, -1)$ with A odd, $m \equiv 3 \pmod 6$, but this set is thin.

For example, for $P < 6000$ the only possibilities are 4, 36, 76, 140, 364, 756, 1364, 2236, 3420, 4964. A similar remark applies to the numbers $P = V_n(A, 1)$, where A is odd and 3 divides m.

In 1983, ROTKIEWICZ published the following partial, but remarkable result:

(5.16) If P is even, $Q \equiv 1 \pmod 4$, $\gcd(P, Q) = 1$, and if $U_n(P, Q) = \square$, then either n is an odd square or n is an even integer, not a power of 2, whose largest prime factor divides the discriminant D.

MCDANIEL and RIBENBOIM (1998b) used the result of ROTKIEWICZ to show:

(5.17) Let P be positive and even, let $Q \equiv 1 \pmod 4$ with $D = P^2 - 4Q > 0$, $\gcd(P, Q) = 1$ and let $U_n(P, Q) = \square$. Then n is a square, or twice an odd square; all prime factors of n divide D; if $p^t > 2$ is a prime power dividing n, then for $1 \leq u < t$, $U_{p^u} = p\square$ when u is even, and $U_{p^U} = p\square$ when u is odd. If n is even and $U_n = \square$, then, in addition, $p = \square$ or $p = 2\square$.

b Square-classes

In (1992), together with MCDANIEL, I proved the following result was proved:

(5.18) Let $(P, Q) \in \mathcal{S}$. Then for every $n > 0$ there exists an effectively computable integer $C_n > 0$, depending on P, Q, n, such that if $n < m$ and $U_n(P, Q)U_m(P, Q) = \square$, or $V_n(P, Q)V_m(P, Q) = \square$, then $M < C_n$.

In particular, all square-classes in sequences U, V are finite.

For parameters $(P, 1)$, $(P, -1)$, with P odd, COHN (1972) used his results on certain quartic equations of type $X^4 - DY^2 = \pm 4, \pm 1$ or $X^2 - DY^4 = \pm 4, \pm -1$, to obtain results on square-classes:

(5.19) Let $P \geq 1$ be odd.

1. If $1 \leq n < m$ and $U_n(P, -1)U_m(P, -1) = \square$, then
   $n = 1, \quad m = 2, \quad P = \square, \quad$ or
   $n = 1, \quad m = 12, \quad P = 1, \quad$ or
   $n = 3, \quad m = 6, \quad P = 1, \quad$ or
   $n = 3, \quad m = 6, \quad P = 3.$

2. If $P \geq 3$, $1 \leq n \leq m$, and $U_n(P,1)U_m(P,1) = \square$, then
$n = 1, \quad m = 6, \quad P = 3, \quad$ or
$n = 1, \quad m = 2, \quad P = \square$.

(5.20) Let $P \geq 1$ be odd.

1. If $0 \leq n < m$ and $V_n(P,1)V_m(P,1) = \square$, then
$n = 0, \quad m = 6, \quad P = 1, \quad$ or
$n = 1, \quad m = 3, \quad P = 1, \quad$ or
$n = 0, \quad m = 6, \quad P = 5$.
2. If $P \geq 3$, $0 \leq n < m$, and $V_n(P,1)V_m(P,1) = \square$, then
$n = 0$, $m = 3$, $P = 3$ or 27.

A very special case, but with a more direct proof, was given later by André-Jeannin (1992).

The following theorem was proved by McDaniel (1998a):

(5.21) Let $P > 0$, $Q \neq 0$, $\gcd(P,Q) = 1$, $D = P^2 - 4Q > 0$. Assume that P, Q are odd.

1. (a) If $1 < m < n$ and $U_mU_n = \square$, then $(m,n) \in \{(2,3),(2,12),(3,6),(5,10)\}$ or $n = 3m$,
(b) If $1 < m$, $U_mU_{3m} = \square$, then m is odd, $3 \nmid m$, $Q \equiv 1 \pmod 4$, $\left(\frac{-Q}{P}\right) = +1$, and $P < |Q+1|$.
(c) If P, $m > 1$ are given, there exists an effectively computable constant $C > 0$ such that if Q is as in the hypotheses, and if $U_mU_{3m} = \square$, then $|Q| < C$.
(d) If P, Q are given as above, there exists an effectively computable $C > 0$ such that if $m > 1$ and $U_mU_{3m} = \square$, then $m < C$.
2. (a) If $1 < m < n$ and $V_mV_n = \square$, then $n = 3m$.
(b) If $1 < m$ and $V_mV_{3m} = \square$, then m is odd, $3 \nmid m$, $Q \equiv 3 \pmod 4$, $3 \nmid P$, $\left(\frac{-3Q}{P}\right) = +1$ and, $P < |\frac{Q}{k} + k|$, where $k = \sqrt[5]{0.6} \approx 0.9$.
(c) If $m > 1$ and P are given, there exists an effectively computable $C > 0$ such that if $Q \neq 0$ is as above and $V_mV_{3m} = \square$, then $|Q| < C$.
(d) If P, Q are given as above, there exists an effectively computable $C > 0$ such that if $1 < m$ and $V_mV_{3m} = \square$, then $m < C$.

c Multiples of squares

There are only a few systematic results, mainly due to Cohn (1972).

Let $k \geq 3$ be an odd square-free integer, let $P \geq 1$, with P odd. Cohn studied the equations $U_n(P,-1) = k\square$, $U_n(P,-1) = 2k\square$, but could not obtain complete results.

Clearly, there exists a smallest index $r > 0$ such that k divides $U_r(P,-1)$. Since the square-classes have at most two numbers, as indicated before in this case, there exist at most two indices n such that $U_n(P,-1) = k\square$, respectively $2k\square$.

(5.22) With the above hypotheses and notations:

1. If $r \not\equiv 0 \pmod 3$ and $U_n = k\square$, then $n = r$, while $U_n = 2k\square$ is impossible.
2. If $r \equiv 3 \pmod 6$, $U_n(P,-1) = k\square$ is impossible, however, no solution was obtained for $U_n(P,-1) = 2k\square$ in this case.
3. If $n \equiv 0 \pmod 6$, and if the 2-adic value $v_2(r)$ is even, then $U_n(P,-1) = 2k\square$ is impossible; if $v_2(r)$ is odd, then $U_n(P,-1) = k\square$ is impossible except if $P = 5$, $n = 12$, $k = 455$. The other cases are left open.

Cohn also stated that for $P \geq 3$, the equations $U_n(P,1) = k\square$, respectively $2k\square$, can be treated similarly, with partial results.

D. Powerful numbers in Lucas sequences

Let $(P,Q) \in \mathcal{S}$, and let U, respectively V, be the Lucas sequences with parameters (P,Q). If U_n is a powerful number, and if p is a primitive factor of U_n, then p^2 divides U_n. This suggests that the set of indices n such that U_n is powerful should be finite. A similar remark applies to the sequence V.

A proof of this fact, based on Masser's conjecture, is known for Fibonacci numbers and Lucas numbers.

Masser's conjecture (1985), also called the (ABC) conjecture, is the following statement (see also Oesterlé (1988)):

Given $\epsilon > 0$, there exists a positive number $C(\epsilon)$ such that if a, b, c are positive integers with $\gcd(a,b) = 1$, $a + b = c$, if $g = \prod_{p|abc} p$, then $c < C(\epsilon) g^{1+\epsilon}$. It is a great challenge for mathematicians to prove the (ABC) conjecture. A much weaker form of the tantalizing (ABC) conjecture was proved by Stewart (1986). Elkies (1991) showed that the (ABC) conjecture implies the famous theorem of

FALTINGS (establishing MORDELL's conjecture). It is also known that the (ABC) conjecture implies that there exist at most finitely many integers $n \geq 3$, x, y, $z \neq 0$, such that $x^n + y^n = z^n$. This is just short of proving Fermat's Last Theorem.

I learned the following from G. WALSH:

(5.23) If MASSER's conjecture is true, and if $k \geq 1$ is a given square-free integer, there exist only finitely many indices n such that the Fibonacci number U_n, or the Lucas number V_n, is of the form kt, where t is a powerful number.

The proof is short and simple.

For any integer $N = \prod_{i=1}^{r} p_i^{e_i}$ (where $p_1, \ldots, p_r$ are distinct primes and $e_1, \ldots, e_r \geq 1$), the *powerful part* of N is by definition

$$w(N) = \prod_{e_i > 1} p_i^{e_i}.$$

So, N is powerful exactly when $N = w(N)$.

In 1999, RIBENBOIM and WALSH proved, assuming the (ABC) conjecture to be true,

(5.24) Let U, V be Lucas sequences with positive discriminant. For every $\epsilon > 0$, the sets $\{n \mid w(U_n) > U_n^{\epsilon}\}$ and $\{n \mid w(V_n) > V_n^{\epsilon}\}$ are finite. In particular, each of the sequences U, V has only finitely many terms which are powerful.

Noteworthy special cases arise taking $P = 1$, $Q = -1$ (Fibonacci and Lucas numbers), $P = 2$, $Q = -1$ (Pell numbers), $P = 3$, $Q = 2$ and more generally $P = a + 1$ $Q = a$ (while $a > 1$). In particular, the (ABC) conjecture implies that there exist only finitely many Mersenne numbers M_q and Fermat numbers F_m which are powerful.

References

1202 Leonardo Pisano (Fibonacci). *Liber Abbaci (^{2}1228).* Tipografia delle Scienze Matematiche e Fisiche, Rome, 1857 edition. B. Boncompagni, editor.

1657 Frénicle de Bessy. Solutio duorum problematum circa numeros cubos et quadratos. Bibliothèque Nationale de Paris.

1843 J. P. M. Binet. Mémoire sur l'intrégation des équations linéaires aux différences finies, d'un ordre quelconque, á coefficients variables. *C. R. Acad. Sci. Paris*, 17:559–567.

1844 E. Catalan. Note extraite d'une lettre addressée á l'éditeur. *J. reine u. angew. Math.*, 27:192.

1870 G. C. Gérono. Note sur la résolution en nombres entiers et positifs de l'équation $x^m = y^n + 1$. *Nouv. Ann. de Math. (2)*, 9:469–471, and 10:204–206 (1871).

1878 E. Lucas. Théorie des fonctions numériques simplement périodiques. *Amer. J. of Math.*, 1:184–240 and 289–321.

1886 A. S. Bang. Taltheoretiske Untersogelser. *Tidskrift Math., Ser. 5*, 4:70–80 and 130–137.

1892 K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. f. Math.*, 3:265–284.

1904 G. D. Birkhoff and H. S. Vandiver. On the integral divisors of $a^n - b^n$. *Ann. Math. (2)*, 5:173–180.

1909 A. Wieferich. Zum letzten Fermatschen Theorem. *J. reine u. angew. Math.*, 136:293–302.

1913 R. D. Carmichael. On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math. (2)*, 15:30–70.

1920 T. Nagell. Note sur l'équation indéterminée $\frac{x^n-1}{x-1} = y^q$. *Norsk Mat. Tidsskr.*, 2:75–78.

1921a T. Nagell. Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$. *Norsk Mat. Forenings Skrifter, Ser. I*, 1921, No. 2, 14 pages.

1921b T. Nagell. Sur l'équation indéterminée $\frac{x^n-1}{x-1} = y^2$. *Norsk Mat. Forenings Skrifter, Ser. I*, 1921, No. 3, 17 pages.

1930 D. H Lehmer. An extended theory of Lucas' functions. *Ann. of Math.*, 31:419–448.

1935 K. Mahler. Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen. *Nederl. Akad. Wetensch. Amsterdam Proc.*, 38:50–60.

1938 G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Clarendon Press, Oxford, 5th (1979) edition.

1942a W. Ljunggren. Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante. *Acta Math.*, 75:1–21.

1942b W. Ljunggren. Über die Gleichung $x^4 - Dy^2 = 1$. *Arch. Math. Naturvid.*, 45(5):61–70.

1942c W. Ljunggren. Zur Theorie der Gleichung $x^2 + 1 = Dy^4$. *Avh. Norsk Vid. Akad. Oslo.*, 1(5):1–27.

1943 W. Ljunggren. New propositions about the indeterminate equation $\frac{x^n-1}{x-1} = y^q$. *Norsk Mat. Tidsskr.*, 25:17–20.

1950 H.-J. Kanold. Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme. *J. reine u. angew. Math.*, 187:355–366.

1953 C. G. Lekkerkerker. Prime factors of elements of certain sequences of integers. *Nederl. Akad. Wetensch. Proc. (A)*, 56:265–280.

1954 M. Ward. Prime divisors of second order recurring sequences. *Duke Math. J.*, 21:607–614.

1955 E. Artin. The order of the linear group. *Comm. Pure Appl. Math.*, 8:335–365.

1955 M. Ward. The intrinsic divisors of Lehmer numbers. *Ann. of Math. (2)*, 62:230–236.

1958 D. Jarden. *Recurring Sequences.* Riveon Lematematike, Jerusalem. ^{3}1973, revised and enlarged by J. Brillhart, Fibonacci Assoc., San Jose, CA.

1960 A. A. Brauer. Note on a number theoretical paper of Sierpiński. *Proc. Amer. Math. Soc.*, 11:406–409.

1960 Chao Ko. On the Diophantine equation $x^2 = y^n + 1$. *Acta Sci. Natur. Univ. Szechuan*, 2:57–64.

1961 L. K. Durst. Exceptional real Lucas sequences. *Pacific J. Math.*, 11:489–494.

1961 M. Ward. The prime divisors of Fibonacci numbers. *Pacific J. Math.*, 11:379–389.

1962 A. Rotkiewicz. On Lucas numbers with two intrinsic prime divisors. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astron. Phys.*, 10:229–232.

1962a A. Schinzel. The intrinsic divisions of Lehmer numbers in the case of negative discriminant. *Ark. Math.*, 4:413–416.

1962b A. Schinzel. On primitive prime factors of $a^n - b^n$. *Proc. Cambridge Phil. Soc.*, 58:555–562.

1963a A. Schinzel. On primitive prime factors of Lehmer numbers, I. *Acta Arith.*, 8:213–223.

1963b A. Schinzel. On primitive prime factors of Lehmer numbers, II. *Acta Arith.*, 8:251–257.

1963 N. N. Vorob'ev. *The Fibonacci Numbers.* D. C. Heath, Boston.

1964a J. H. E. Cohn. On square Fibonacci numbers. *J. London Math.Soc.*, 39:537–540.

1964b J. H. E. Cohn. Square Fibonacci numbers etc. *Fibonacci Q.*, 2:109–113.

1964 Chao Ko. On the Diophantine equation $x^2 = y^n + 1$. *Scientia Sinica (Notes)*, 14:457–460.

1964 O. Wyler. Squares in the Fibonacci series. *Amer. Math. Monthly*, 7:220–222.

1965 J. H. E. Cohn. Lucas and Fibonacci numbers and some Diophantine equations. *Proc. Glasgow Math. Assoc.*, 7:24–28.

1965 P. Erdös. Some recent advances and current problems in number theory. In *Lectures on Modern Mathematics, Vol. III*, edited by T. L. Saaty, 169–244. Wiley, New York.

1965 H. Hasse. Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteilbarer Ordnung mod p ist. *Math. Annalen*, 162:74–76.

1966 J. H. E. Cohn. Eight Diophantine equations. *Proc. London Math. Soc. (3)*, 16:153–166, and 17:381.

1966 H. Hasse. Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod p ist. *Math. Annalen*, 168:19–23.

1966 K. Mahler. A remark on recursive sequences. *J. Math. Sci.*, 1:12–17.

1966 E. Selmer. *Linear Recurrences over Finite Fields.* Lectures Notes, Department of Mathematics, University of Bergen.

1967 J. H. E. Cohn. Five Diophantine equations. *Math. Scand.*, 21:61–70.

1967 C. Hooley. On Artin's conjecture. *J. reine u. angew. Math.*, 225:209–220.

1968 J. H. E. Cohn. Some quartic Diophantine equations. *Pacific J. Math.*, 26:233–243.

1968 L. P. Postnikova and A. Schinzel. Primitive divisors of the expression $a^n - b^n$. *Math. USSR-Sb.*, 4:153–159.

1968 A. Schinzel. On primitive prime factors of Lehmer numbers, III. *Acta Arith.*, 15:49–70.

1969 V. E. Hoggatt. *Fibonacci and Lucas Numbers.* Houghton-Mifflin, Boston.

1969 R. R. Laxton. On groups of linear recurrences, I. *Duke Math. J.*, 36:721–736.

1969 H. London and R. Finkelstein (alias R. Steiner). On Fibonacci and Lucas numbers which are perfect powers. *Fibonacci Q.*, 7:476-481 and 487.

1972 J. H. E. Cohn. Squares in some recurrence sequences. *Pacific J. Math.*, 41:631–646.

1972 K. Inkeri. On the Diophantic equation $a\frac{x^n-1}{x-1} = y^m$. *Acta Arith.*, 21:299–311.

1973 A. Baker. A sharpening for the bounds of linear forms in logarithms, II. *Acta Arith.*, 24:33–36.

1973 H. London and R. Finkelstein (alias R. Steiner). *Mordell's Equation* $y^2 - k = x^3$. Bowling Green State University Press, Bowling Green, OH.

1974 A. Schinzel. Primitive divisions of the expression $A^n - B^n$ in algebraic number fields. *J. reine u. angew. Math.*, 268/269: 27–33.

1975 A. Baker. *Transcendental Number Theory.* Cambridge Univ. Press, Cambridge.

1975 C. L. Stewart. The greatest prime factor of $a^n - b^n$. *Acta Arith.*, 26:427–433.

1976 E. Z. Chein. A note on the equation $x^2 = y^n + 1$. *Proc. Amer. Math. Soc.*, 56:83–84.

1976 S. V. Kotov. Über die maximale Norm der Idealteiler des Polynoms $\alpha x^m + \beta y^n$ mit den algebraischen Koeffizenten. *Acta Arith.*, 31:210–230.

1976 M. Langevin. Quelques applications des nouveaux résultats de van der Poorten. *Sém. Delange-Pisot-Poitou,* 17^e *année*, 1976, No. G12, 1–11.

1976 P. J. Stephens. Prime divisors of second order linear recurrences, I. and II. *J. Nb. Th.*, 8:313–332 and 333–345.

1976 R. Tijdeman. On the equation of Catalan. *Acta Arith.*, 29: 197–209.

1977 A. Baker. The theory of linear forms in logarithms. In *Transcendence Theory: Advances and Applications (Proceedings*

of a conference held in Cambridge 1976), edited by A. Baker and D. W. Masser, 1–27. Academic Press, New York.

1977 T. N. Shorey, A. J. van der Porten, R. Tijdeman, and A. Schinzel. Applications of the Gel'fond-Baker method to Diophantine equations. In *Transcendence theory: Advances and Applications*, edited by A. Baker and D. W. Masser, 59–77. Academic Press, New York.

1977a C. L. Stewart. On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. *Proc. London Math. Soc.*, 35:425–447.

1977b C. L. Stewart. Primitive divisors of Lucas and Lehmer numbers. In *Trancendence Theory: Advances and Applications*, edited by A. Baker and D. W. Masser, 79–92. Academic Press, New York.

1977 A. J. van der Poorten. Linear forms in logarithms in p-adic case. In *Transcendence Theory: Advances and Applications*, edited by A. Baker and D. W. Masser, 29–57. Academic Press, New York.

1978 P. Kiss and B. M. Phong. On a function concerning second order recurrences. *Ann. Univ. Sci. Budapest. Eötvös Sect Math.*, 21:119–122.

1978 N. Robbins. On Fibonacci numbers which are powers. *Fibonacci Q.*, 16:515–517.

1980 R. Steiner. On Fibonacci numbers of the form $v^2 + 1$. In *A Collection of Manuscripts Related to the Fibonacci Sequence*, edited by W. E. Hogatt and M. Bicknell-Johnson, 208–210. The Fibonacci Association, Santa Clara, CA.

1980 C. L. Stewart. On some Diophantine equations and related recurrence sequences. In *Séminaire de Théorie des Nombres Paris 1980/81 (Séminare Delange-Pisot-Poitou), Progress in Math.,* 22:317–321 (1982). Birkhäuser, Boston.

1980 M. Waldschmidt. A lower bound for linear forms in logarithms. *Acta Arith.*, 37:257–283.

1981 K. Győry, P. Kiss, and A. Schinzel. On Lucas and Lehmer sequences and their applications to Diophantine equations. *Colloq. Math.*, 45:75–80.

1981 J. C. Lagarias and D. P. Weissel. Fibonacci and Lucas cubes. *Fibonacci Q.*, 19:39–43.

1981 H. Lüneburg. Ein einfacher Beweis für den Satz von Zsigdmondy über primitive Primteiler von $A^n - B^n$. In *Ge-*

ometries and Groups, Lect. Notes in Math., 893:219–222, edited by M. Aigner and D. Jungnickel. Springer-Verlag, New York.

1981 T. N. Shorey and C. L. Stewart. On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, II. *J. London Math. Soc.*, 23:17–23.

1982 K. Györy. On some arithmetical properties of Lucas and Lehmer numbers. *Acta Arith.*, 40:369–373.

1982 A. Pethö. Perfect powers in second order linear recurrences. *J. Nb. Th.*, 15:5–13.

1982 C. L. Stewart. On divisors of terms of linear recurrence sequences. *J. reine u. angew. Math.*, 333:12–31.

1983 A. Pethö. Full cubes in the Fibonacci sequence. *Publ. Math. Debrecen*, 30:117–127.

1983a N. Robbins. On Fibonacci numbers of the form px^2, where p is a prime. *Fibonacci Q.*, 21:266–271.

1983b N. Robbins. On Fibonacci numbers which are powers, II. *Fibonacci Q.*, 21:215–218.

1983 A. Rotkiewicz. Applications of Jacobi symbol to Lehmer's numbers. *Acta Arith.*, 42:163–187.

1983 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.*, 52:24–36.

1984 N. Robbins. On Pell numbers of the form px^2, where p is prime. *Fibonacci Q. (4)*, 22:340–348.

1985 J. C. Lagarias. The set of primes dividing the Lucas numbers has density 2/3. *Pacific J. Math.*, 118:19–23.

1985 D. W. Masser. Open problems. In *Proceedings Symposium Analytic Number Theory*, edited by W. W. L. Chen, London. Imperial College.

1985 C. L. Stewart. On the greatest prime factor of terms of a linear recurrence sequence. *Rocky Mountain J. Math.*, 15: 599–608.

1986 T. N. Shorey and R. Tijdeman. *Exponential Diophantine Equations.* Cambridge University Press, Cambridge.

1986 C. L. Stewart and R. Tijdeman. On the Oesterlé-Masser conjecture. *Monatshefte Math.*, 102:251–257.

1987 A. Rotkiewicz. Note on the Diophantine equation $1 + x + x^2 + \ldots + x^m = y^m$. *Elem. of Math.*, 42:76.

1988 J. Brillhart, P. L. Montgomery, and R. D. Silverman. Tables of Fibonacci and Lucas factorizations. *Math. of Comp.*, 50: 251–260.

1988 M. Goldman. Lucas numbers of the form px^2, where $p = 3$, 7, 47 or 2207. *C. R. Math. Rep. Acad. Sci. Canada*, 10: 139–141.

1988 J. Oesterlé. Nouvelles approches du "théorème" de Fermat. Séminaire Bourbaki, 40ème anée, 1987/8, No. 694, *Astérisque*, 161–162, 165–186.

1989a P. Ribenboim. Square-classes of Fibonacci numbers and Lucas numbers. *Portug. Math.*, 46:159–175.

1989b P. Ribenboim. Square-classes of $\frac{a^n-1}{a-1}$ and a^n+1. *J. Sichuan Univ. Nat. Sci. Ed.*, 26:196–199. Spec. Issue.

1989 N. Tzanakis and B. M. M. de Weger. On the practical solution of the Thue equation. *J. Nb. Th.*, 31:99–132.

1991 W. D. Elkies. *ABC* implies Mordell. *Internat. Math. Res. Notices (Duke Math. J.)*, 7:99–109.

1991 A. Pethö. The Pell sequence contains only trivial perfect powers. In *Colloquia on Sets, Graphs and Numbers, Soc. Math., János Bolyai*, 561–568. North-Holland, Amsterdam.

1991a P. Ribenboim. *The Little Book of Big Primes*. Springer-Verlag, New York.

1991b P. Ribenboim and W. L McDaniel. Square-classes of Lucas sequences. *Portug. Math.*, 48:469–473.

1992 R. André-Jeannin. On the equations $U_n = U_q x^2$, where q is odd and $V_n = V_q x^2$, where q is even. *Fibonacci Q.*, 30: 133–135.

1992 W. L. McDaniel and P. Ribenboim. Squares and double squares in Lucas sequences. *C. R. Math. Rep. Acad. Sci. Canada*, 14:104–108.

1994 P. Ribenboim. *Catalan's Conjecture*. Academic Press, Boston.

1995 P. M. Voutier. Primitive divisors of Lucas and Lehmer sequences. *Math. of Comp.*, 64:869–888.

1998a W. L. McDaniel and P. Ribenboim. Square classes in Lucas sequences having odd parameters. *J. Nb. Th.*, 73:14–23.

1998b W. L. McDaniel and P. Ribenboim. Squares in Lucas sequences having one even parameter. *Colloq. Math.*, 78: 29–34.

1999 Y. Bugeaud and M. Mignotte. On integers with identical digits. Preprint.

1999 H. Dubner and W. Keller. New Fibonacci and Lucas primes. *Math. of Comp.*, 68:417–427.

1999a P. Ribenboim. Números primos, Mistérios e Récordes. Instituto de Matématica Puru e Aplicado, Rio de Janeiro.

1999b P. Ribenboim and P. G. Walsh. The *ABC* conjecture and the powerful part of terms in binary recurring sequences. *J. Nb. Th.*, 74:134–147.