Binomial Coefficients and Lucas Sequences

Achim Flammenkamp
Fakultät für Mathematik, Universität Bielefeld, Postfach 10 01 31, 33 501 Bielefeld, Germany
E-mail: achim@uni-bielefeld.de

and

Florian Luca
Instituto de Matemáticas de la UNAM, Campus Morelia, Apartado Postal 61-3 (Xangari),
CP 58 089, Morelia, Michoacán, Mexico
E-mail: fluca@matmor.unam.mx

Communicated by A. Granville
Received October 30, 2000

1. INTRODUCTION

Throughout this paper, \( a \) and \( b \) are integers such that \( a > |b| \). For any non-negative integer \( n \) let

\[
\begin{align*}
    u_n &= \frac{a^n - b^n}{a - b} \\
    v_n &= a^n + b^n.
\end{align*}
\]

The sequences \((u_n)_{n \geq 0}\) and \((v_n)_{n \geq 0}\) are particular instances of the so-called Lucas sequences of first and second kind, respectively. These sequences enjoy very nice arithmetic properties and diophantine equations involving members of such sequences often arise in the study of exponential diophantine equations.

In this paper, we investigate the occurrence of binomial coefficients in sequences whose general term is given by formula (1) or (2). That is, we look at the solutions of the diophantine equations

\[
\begin{align*}
    u_n &= \binom{m}{k} \\
    &\quad \text{for } m \geq 2k > 2
\end{align*}
\]
and

\[ v_n = \binom{m}{k} \quad \text{for} \quad m \geq 2k > 2. \]  \tag{4}

Notice that since \( \binom{m}{1} = m \) and \( \binom{m}{k} = \binom{m-1}{m-k} \) hold for all \( m \geq 1 \) and for all \( 1 \leq k \leq m-1 \), the assumption \( m \geq 2k > 2 \) imposes no restriction at all on the non-trivial solutions of the equations (3) and (4). We will also assume that \( n \geq 2 \).

We recall that various equations involving powers, products of consecutive integers, and binomial coefficients have been previously investigated. Erdős and Selfridge (see [20]) have shown that a product of consecutive integers is never a perfect power. Erdős [19] has investigated the problem of determining all binomial coefficients which are perfect powers. He showed that the equation

\[ x^n = \binom{m}{k} \quad \text{for} \quad x \in \mathbb{N}, \quad n > 1 \quad \text{and} \quad m \geq 2k > 2 \]  \tag{5}

has no solutions for \( k \geq 4 \). The remaining cases of equation (5) have been solved by Györy (see [21, 22]) using a result of Darmon and Merel (see [15]). There are many papers in the literature treating extensions of equation (5) to problems involving perfect powers in products of consecutive terms from an arithmetical progression as well as equal products of consecutive terms in arithmetical progressions (see, for example, [3, 6, 8, 40]).

In [28], Maohua Le treated the equation

\[ \binom{m}{2} - 1 = q^n + 1 \quad \text{for} \quad m \geq 2, \quad q \geq 2 \quad \text{and} \quad n \geq 3, \]  \tag{6}

and showed that it has only finitely many effectively computable solutions \((m, n, q)\). Here, \( q \) was assumed to be a prime power. Some equations similar to (6) have been also considered by Cameron (see [24]). All solutions of equation (3) for \((a, b, k) = (2, 1, 2)\) have been found by Browkin and Schinzel in [10]. In fact, as Schinzel pointed out to us, in this case equation (3) can be rewritten, after some linear substitutions, as \( y^2 = 2^t - 7 \) with positive integers \( y \) and \( t \), which is the famous diophantine equation of Ramanujan first solved by Nagell. In [29], one of us determined all the binomial coefficients which can be the number of sides or regular polygons constructible with ruler and compass.
By the results of Erdős and Győry on Eq. (5), we may assume that \( b \neq 0 \) in both equations (3) and (4).

We first investigate equations (3) and (4) when the parameter \( k \) is fixed. Our result is the following.

**Theorem 1.** Assume that \( a > |b| > 0 \) are fixed and that \( k \geq 2 \) is fixed as well. Then, equation (4) has only finitely many solutions \((n, m)\). Moreover, equation (3) has also only finitely many solutions \((n, m)\) except for the cases when \((a, b) = (8, 2)\) and \( k = 3 \) or \((a, b) = (4, 2), (9, 1), (7, -1) \) and \( k = 2 \).

We are also interested in the solutions \((n, m, k)\) of equations (3) and (4) when \( k \) varies.

The easiest case is when the two integers \( a \) and \( b \) are not coprime. In this case, we have the following result.

**Theorem 2.** Assume that \( a > |b| > 0 \) are fixed with \( \gcd(a, b) \neq 1 \). Then, equation (4) has only finitely many solutions \((n, m, k)\). Moreover, equation (3) has also only finitely many solutions \((n, m, k)\) except for the cases in which \((a, b) \in \{(8, 2), (4, 2)\}\). When \((a, b) = (8, 2)\) the only solutions of equations (3) are \((n, m, k) = (2, 5, 2)\) and \((n, 2^n+1, 3)_{n \geq 3}\) and when \((a, b) = (4, 2)\) the only solutions of equation (3) are \((n, m, k) = (n, 2^n, 2)_{n \geq 2}\) and \((4, 10, 3)\).

We have been unable to prove a result as general as Theorem 2 for the situation in which \( a \) and \( b \) are coprime. However, in some situations, we were still able to conclude that equations (3) or (4) have only finitely many solutions \((n, m, k)\) for which the parameter \( n \) is either prime, or a power of 2. That is, we have the following results.

**Theorem 3.** Assume that \( 2 \mid ab \). Then, equation (3) has only finitely many solutions \((n, m, k)\) for which \( n \) is prime.

**Theorem 4.** Assume that \( b = 1 \). Then, equation (4) has finitely solutions \((n, m, k)\) for which \( n \) is a power of 2. Moreover, all these solutions can be effectively computed.

Recall that if \( a \) is fixed and \( n \geq 0 \) the number \( F_n(a) = a^{2^n} + 1 \) is called a **generalized Fermat number**. When \( a = 2 \) this is simply refereed to as a **Fermat number**. Ever since 1640 when Fermat conjectured that all Fermat numbers are prime (which, as we all know, has turned out to be a very unfortunate claim) a lot interest has been expressed in the prime factor decomposition of Fermat and generalized Fermat numbers (see [9, 18]).
and there is even a book in progress about what we know and don’t know about the Fermat numbers (see [26]). Theorem 4 above tells us that if \( a \) is fixed, then there are only finitely many effectively computable indices \( n \) for which \( F_\nu(a) \) can be a non-trivial binomial coefficient. When \( a = 2 \) there is none (see Corollary 2 below).

Notice that Theorem 4 above is effective while Theorems 1, 2 and 3 are not. The reason for the ineffectiveness of Theorems 1, 2 and 3 will become apparent from their proofs.

Finally, we present some computational applications of Theorems 2 and 3.

**Corollary 1.** Assume that \( a > |b| \) and that \(|ab|\) is an even divisor of 30 with \((a, b) \neq (5, \pm 2)\). Then, the only solutions \((n, m, k)\) of equation (3) with \( n \) prime occur when \( k = 2 \) and

\[
(a, b, n, m) \in \{(3, -2, 5, 11), (6, 5, 3, 14), (10, -1, 3, 14)\}.
\]

We would have liked to treat the cases \((a, b) = (5, \pm 2)\) as well. In this case, we can show that the only solutions \((n, m, k)\) with \( n \) prime of equation (3) are the ones for which \( k = 2 \). Unfortunately, we have not been able to solve these last two equations.

Notice that Corollary 1 tells us, in particular, that a Mersenne number is never a non-trivial binomial coefficient, and that no repunit with a prime number of digits (that is, a number of the form

\[
111 \cdots 1 = \frac{10^p - 1}{9}
\]

with \( p \) prime) is a non-trivial binomial coefficient. We recall that the Mersenne numbers are never perfect powers. Indeed, this follows easily from what is known about the Catalan equation (see, for example, [34]). Recall also that Bugeaud and Mignotte (see [12]) showed that the repunits are never perfect powers either.

**Corollary 2.** When \( a \leq 30 \) and \( b = 1 \) the only solutions of equation (4) with \( n = 2^s \) for some \( s \in \mathbb{N} \) are

\[
(a, n, m, k) \in \{(3, 2, 5, 2), (18, 2, 26, 2)\}.
\]

We recall that in [30] it is shown that no Fermat number is a non-trivial binomial coefficient. This result is now just a particular instance of Corollary 2.
2. THE PROOF OF THEOREM 1

Throughout this section, we assume that $a$ and $b$ are fixed integers with $a > |b| > 0$ and that $k \geq 2$ is also a fixed integer. We look at the solutions $(n, m)$ of the equations

$$u_n = \binom{m}{k}$$

and

$$v_n = \binom{m}{k},$$

where $u_n$ and $v_n$ are given by formulae (1) and (2). The main goal of this section is to show that equation (8) has only finitely many solutions $(n, m)$ and that equation (7) has also only finitely many solutions $(n, m)$ except for the cases in which $k = 2$ and $(a, b) \in \{(9, 1), (7, -1), (4, 2)\}$, or $k = 3$ and $(a, b) = (8, 2)$.

We distinguish the following cases.

Case 1. Assume that $a$ and $b$ are multiplicatively independent.

At this stage, we recall that a Universal Hilbert set $U \subset \mathbb{Q}$ is a set $U$ having the property that whenever $F \in \mathbb{Q}[x, y]$ is irreducible, the polynomial $F(u, y) \in \mathbb{Q}[y]$ remains irreducible for all but finitely many values $u \in U$. In particular, it follows right away that if $U$ is a Universal Hilbert set and if $f \in \mathbb{Q}[y]$ is a polynomial of degree greater than 1, then the equation $u = f(y)$ has only finitely many solutions $(u, y)$ with $u \in U$ and $y \in \mathbb{Q}$. In 1998, Corvaja and Zannier (see [14]) proved that if $a > |b| > 1$ are two integers such that $a$ and $b$ are multiplicatively independent, then, whenever $c$ and $d$ are two non-zero rational numbers, the terms of the sequence $(w_n)_{n \geq 0}$ with $w_n = ca^n + db^n$ for $n \geq 0$, form a Universal Hilbert set. In particular, if $f \in \mathbb{Q}[y]$ is a polynomial of degree greater than 1, then the equation $w_n = f(y)$ has only finitely many integer solutions $(n, y)$. This shows that both equations (7) and (8) have only finitely many solutions $(n, m)$. The arguments of Corvaja and Zannier from [14] use a version of Schmidt’s Subspace Theorem due to Schlickweil from [37, 38], therefore their proofs are ineffective. Thus, our finiteness result for the solutions of equations (7) and (8) is ineffective in this instance as well.

Case 2. Assume $a$ and $b$ are multiplicatively dependent.

It follows that there exist a positive integer $\theta > 1$ and two integers $r > s \geq 0$ such that $a = \theta^r$ and $b = \epsilon \theta^s$, where $\epsilon \in \{\pm 1\}$. The results of
Corvaja and Zannier from [14] no longer apply in this instance but we shall show that some variations of them can be employed in order to conclude that if either one of the equation (3) or (4) has infinitely many solutions \((m, n)\), then all three parameters \(k, r\) and \(s\) must be small. We are grateful to the referee who supplied the following result.

**Proposition 1.** Let \(\theta \neq 0, \pm 1\) and \(r > s \geq 0\) be integers, and set \(a = \theta'\) and \(b = \theta'\). Assume that \(a \neq 0\) and \(b\) are rational numbers and that \(P(x) \in \mathbb{Q}[x]\) is a polynomial of degree \(k \geq 2\). If the equation

\[
P(x) = ax^r + bx^s \tag{9}
\]

has infinitely many solutions \((x, n) \in \mathbb{Z}\), then \(r | s k\), and there exist an integer \(m \in \{0, 1, \ldots, k-1\}\) and a linear polynomial \(l(x) \in \mathbb{Z}[x]\) such that

\[
P(l(x)) = ax^m x^r + bx^m x^s \tag{10}
\]

where \(s' = sk/r\).

**Proof of Proposition 1.** Since equation (9) has infinitely many integer solutions \((x, n)\), we get that (9) has infinitely many integer solutions for which \(n > 0\). Of course, there exist infinitely many such solutions \((x, n)\) for which \(n\) is in the same congruence class modulo \(k\), call it \(\mu \pmod k\). This implies infinitely many integer solutions \((x, n_1)\) with \(n_1 > 0\) for the equation

\[
P(x) = a_n x^n + b_n x^n, \tag{11}
\]

where \(a_n = \theta^n, b_n = \theta'^n, a = \theta^n, b = \theta'^n\) with \(r_1 = kr\) and \(s_1 = ks\). Via this transformation, we may assume that \(k | r\) in the hypothesis of Proposition 1 above. Notice that \(s_1/k/r_1 = sk/r = s'\), therefore neither the conclusion that \(r | sk\), nor the value of \(sk/r\) will be affected by the replacement of the pair \((r, s)\) with the pair \((r_1, s_1)\).

From now on, we assume that \(k | r\), therefore that \(\mu = 0\), and we have to show that \(r | sk\) and that there exists a linear polynomial \(l(x) \in \mathbb{Z}[x]\) such that

\[
P(x) = ax^k + bx^s \tag{12}
\]

Put \(F(x, t) := P(x) - at^r - bt^s\). Since \(k | r\), we have \(F(x, t) = c(x - X_1(t)) \cdots (x - X_d(t))\), where \(c\) is the leading coefficient of \(P(x)\) and \(X_1(t), \ldots, X_d(t) \in \mathbb{Q}((t^{-1}))\) are the Puiseux expansions of \(x\) at \(t = \infty\). Indeed, the condition that \(k | r\) implies that the Puiseux series \(X_1(t), \ldots, X_d(t)\) are unramified (in general, one would have that \(X_1(t), \ldots, X_d(t) \in \mathbb{Q}((t^{-1}))\), where \(e = k/gcd(k, r)\).
Now let $x_0$ and $t_0$ be complex numbers satisfying $F(x_0, t_0) = 0$. When $|t_0|$ is large enough, the power series $X_1(t), \ldots, X_d(t)$ converge at $t = t_0$, with one of the sums $X_1(t_0), \ldots, X_d(t_0)$ equal to $x_0$. Hence, since the equation

$$F(x, \theta^n) = P(x) - (a^n + b^n) = 0$$

(13)

has infinitely many integer solutions $(x, n)$ with $n > 0$, it follows that there exist an index $j \in \{1, \ldots, k\}$ such that $X_j(\theta^n) \in \mathbb{Z}$ for infinitely many positive integers $n$. Let’s call such an $n$ interesting.

In the sequel, we write $X(t)$ instead of $X_j(t)$. Let $Y(t) = \sum b[t]$ be the sum of the terms of $X(t)$ of non-negative degree. That is,

$$X(t) = Y(t) + \text{the terms of negative degree.}$$

(14)

Then,

$$|X(t_0) - Y(t_0)| \ll |t_0|^{-1}$$

(15)

holds whenever $X(t)$ converges at $t_0 \in \mathbb{C}^*$. Thus, for every interesting $n$, there exists a rational integer $x_n = X(\theta^n)$ such that

$$|x_n - Y(\theta^n)| \ll |\theta|^{-n}.$$  

(16)

Now Lemma 2 of Corvaja and Zannier [14] implies the existence of a polynomial $Q(t) \in \mathbb{Z}[t]$ such that $x_n = Q(\theta^n)$ holds for all but finitely many interesting $n$’s.

Since $X(t)$ and $Q(t)$ coincide in infinitely many distinct points, they must coincide identically. Thus, $X(t) = Q(t)$, which means that $R(t) = P(Q(t))$, where we put $R(t) = a(t) + b(t)$. We now show that the polynomial $Q(t)$ is of the form $l(t^q)$, where $q$ is the degree of $Q$ and $l(x) \in \mathbb{Z}[x]$ is a linear polynomial. Of course, it suffices to show that $Q(t) = l(t^q)$ for some linear polynomial $l(x) \in \mathbb{Q}[x]$, because the fact that the coefficients of $l(x)$ are integers will follow from the fact that the coefficients of $Q(t)$ are integers.

Assume first that $s \beta = 0$. Then $Q'(t)$ divides $R'(t) = r x t^{-1}$ in the ring $\mathbb{Q}[t]$, which immediately implies that $Q(t) = l(t^q)$ with a linear polynomial $l(x) \in \mathbb{Q}[x]$.

Assume now that $s \beta \neq 0$. Put $d_1 = \gcd(r, s)$ and let $v = (r - s)/d_1$. Let $\gamma_1, \ldots, \gamma_v$ be all the roots of order $v$ of $s \beta/(r x)$. Then we may factorize $R'(t)$ as

$$R'(t) = \phi_0(t) \phi_1(t) \cdots \phi_v(t),$$

(17)

where $\phi_0(t) = r x t^{-1}$ and $\phi_j(t) = t^{\delta_j} - \gamma_j$ for $j = 1, \ldots, v$. Factorization (17) has the following property: if $\delta_1$ and $\delta_2$ are two roots of $R'(t)$, then $R(\delta_1) = R(\delta_2)$ if and only if $\delta_1$ and $\delta_2$ are both roots of the same $\phi_j(t)$. 

252 FLAMMENKAMP AND LUCA
On the other hand, we also have the following factorization of $R'(t)$,

$$R'(t) = P'(Q(t)) \cdot Q'(t) = c_1(Q(t) - e_1) \cdots (Q(t) - e_{k-1}) \cdot Q'(t), \quad (18)$$

where $c_1$ is the leading coefficient of $R'(t)$ and $e_1, \ldots, e_{k-1}$ are all the roots of $P'(t)$ (recall that $k \geq 2$, therefore $k-1 \geq 1$). Since $R(t)$ has the same value at all the roots of $Q(t) - e_i$, namely $P(e_i)$, by the preceding remarks we get that each of the polynomials $Q(t) - e_i$ divides some $\phi_j(t)$ in the ring $\overline{Q}[t]$. If some $Q(t) - e_i$ divides $\phi_0(t)$, then it is immediate that $Q(t) = l(t^s)$ for some linear polynomial $l(x) \in \overline{Q}[x]$.

Now assume that every $Q(t) - e_i$ divides $\phi_j(t)$ for some $j \in \{1, \ldots, n\}$. In this case, $q = \deg(Q) \leq \deg(\phi) = d_1$. It also follows that $P'(Q(t))$ divides $\phi_1(t) \cdots \phi_n(t)$, which implies that $r - q \leq r - s$, whence $q \geq s$. Since $d_1 \leq s$, we get that $q = d_1 = s$; that is, $Q(t) - e_i$ is a constant multiple of $\phi_j(t)$. This again implies that $Q(t) = l(t^s)$ for a linear polynomial $l(x) \in \overline{Q}[x]$. This shows that indeed $Q(t) = l(t^s)$ for some linear polynomial $l(x) \in \overline{Q}[x]$. Finally, the equality

$$\alpha t^r + \beta t^s = R(t) = P(Q(t)) = P(l(t^s)) \quad (19)$$

implies that $q | s$, $r = qk$, and by replacing now $t^s$ by $t$ in formula (19) we get

$$P(l(t)) = \alpha t^k + \beta t^s, \quad (20)$$

where $s' = s/q = sk/r$ is an integer. This concludes the proof of Proposition 1.

For the remainder of the proof of Theorem 1 we shall apply Proposition 1 above with $a_i = \theta'$, $b_i = \theta^r$ and $P(x) = \binom{x}{s}$. The polynomial $P(x)$ has the property that all its roots are simple and real; in particular, if $l(x) \in \overline{Z}[x]$ is any linear polynomial, then all the roots of $P(l(x))$ are simple and real as well. We distinguish the following subcases.

**Subcase 1.** $s = 0$. In this case, $b = \epsilon \in \{\pm 1\}$ and one can take $r = 1$. Let $a_i = a = \theta$ and $b_i = 1 = \theta^0$. Assume that either equation (3) or equation (4) has infinitely many integer solutions $(m, n)$. It then follows that one of the equations

$$P(x) = \alpha \beta^s + \beta b^s \quad (21)$$

has infinitely many solutions integer solutions $(x, n)$ where $(\alpha, \beta)$ is one of the pairs $\left(\frac{1}{\sqrt{2}}, \frac{\sqrt{2}}{2}\right)$ or $\left(1, \pm 1\right)$. Proposition 1 above now tells us that there exist a pair of non-zero rational numbers $(\alpha_i, \beta_i)$ and a linear polynomial $l(x) \in \overline{Z}[x]$ such that

$$P(l(x)) = \alpha_i x^k + \beta_1. \quad (22)$$
The polynomial appearing in the right hand side of formula (22) has complex non-real roots when \( k \geq 3 \). Thus, the only case left to investigate is when \( k = 2 \).

We first treat equation (3). Equation (3) is

\[
\frac{m(m-1)}{2} = \frac{a^n - e^n}{a - e}, \tag{23}
\]

which can be rewritten as

\[
(a - e) m^2 - (a - e) m + 2e^n = 2a^n. \tag{24}
\]

Let

\[
f(x) = (a - e) x^2 - (a - e) x + 2e^n \in \mathbb{Z}[x]. \tag{25}
\]

By a well-known result of Thue (see [39]), we know that if \( F(X) \in \mathbb{Z}[X] \) is a polynomial having at least two distinct roots, then the largest prime factor of \( F(x) \), denoted by \( P(F(x)) \), tends to infinity with \( x \) when \( |x| \) tends to infinity through natural numbers. In fact, using a \( p \)-adic version of Baker’s method, one can show that \( P(F(x)) \to \infty \) in an effective way when \( |x| \) tends to infinity through natural numbers. Thus, equation (24) can have infinitely many integer solutions \((m, n)\) only when the discriminant of the quadratic polynomial \( f(x) \) is zero. But this discriminant is

\[
(a - e)(a - e - 8e^n), \tag{26}
\]

and this is zero only when \( e = 1 \) and \( a = 9 \), or when \( e = 1 \), \( a = 7 \) and \( n \) is even. This gives the two infinite families of solutions

\[
\frac{9^n - 1}{8} = \left( \frac{3^n + 1}{2} \right), \quad \text{for all} \quad n \geq 1, \tag{27}
\]

and

\[
\frac{7^n - (-1)^n}{8} = \left( \frac{7^{n/2} + 1}{2} \right) \quad \text{for} \quad n \geq 2 \text{ even}, \tag{28}
\]

of equation (3).
A similar analysis shows that the only instance in which equation (4) can have infinitely many solutions occurs when \( k = 2 \). In this case, equation (4) can be rewritten as

\[
m^2 - m - 2e^n = 2a^n
\]

and the quadratic polynomial appearing in the left hand side of (29) has discriminant \( 1 + 8e^n \neq 0 \). This completes the analysis for this subcase. We remark as well that by the previous arguments, all the solutions of equations (3) and (4) can be effectively computed.

**Subcase 2.** \( s > 0 \). We may of course assume that \( r \) and \( s \) are coprime. If one of the equations (3) or (4) has infinitely many solutions \((m, n)\), we then get infinitely many integer solutions \((x, n)\) of an equation of the form

\[
P(x) = a_1 a^n + b_1 b^n,
\]

where \( a_i = a = \theta^i, b_i = \theta^i \) and \((a_1, b_1)\) one of the pairs of non-zero rational numbers \((\frac{1}{\theta^3}, \frac{\pm 1}{\theta^3})\) or \((1, \pm 1)\). Proposition 1 now tells us that there exist a pair of non-zero rational numbers \((a_1, b_1)\) and a linear polynomial \(l(x) \in \mathbb{Z}[x]\) such that

\[
P(l(x)) = a_1 x^k + b_1 x^s,
\]

where \( s' = sk/r \) is an integer. Since \( r \) and \( s \) are coprime and \( r | sk \), we get that \( r | k \). Since the polynomial appearing in the right hand side of (31) has 0 as a multiple root when \( s' > 1 \), it follows that \( s' = 1 \). Thus, \( s = 1 \) and \( r = k \). Finally, when \( k - s' = k - 1 \geq 3 \), the polynomial appearing in the right hand side of (31) has complex non-real roots; therefore \( k = r \leq 3 \).

We first treat the case \( r = k = 3 \).

We begin with equation (3) and rewrite it as

\[
\frac{m(m-1)(m-2)}{6} = w^3 - \varepsilon w^c = w^3 \pm \varepsilon w^c,
\]

where \( w = \theta^s \) and \( c = a - b = \theta^3 - \varepsilon \theta \). It is now easily checked that any curve \( \mathcal{C} \) given by

\[
F(x, y) := \frac{x(x-1)(x-2)}{6} - \varepsilon' y^3 = 0,
\]

where \( \varepsilon' \in \{\pm 1\} \) is irreducible over the field of complex numbers \( \mathbb{C} \), and that it has no multiple points for any rational value of \( c \neq 6 \). In particular, its genus is positive in this instance, and by a famous result of Siegel (see [42]), we get that the curve \( \mathcal{C} \) given by (33) can contain only finitely many
integer points \((x, y)\) when \(c \neq 6\). Thus, the only possibility is \(c = \theta^3 - e\theta = 6\), and the only acceptable solution of this last equation is \(e = 1\) and \(\theta = 2\), which gives \(a = 8, b = 2\) and the infinite family of solutions

\[
\frac{8^n - 2^n}{8 - 2} = \binom{2^n + 1}{3}, \quad \text{for all } n \geq 3. \tag{34}
\]

We now look at equation (4) by rewriting it as

\[
\frac{m(m-1)(m-2)}{6} = w^3 + e^3 w, \tag{35}
\]

where again \(w = \theta^n\). Notice that the curve

\[
F_1(x, y) := \frac{x(x-1)(x-2)}{6} - (y^3 + e'y) = 0, \tag{36}
\]

with \(e' \in \{\pm 1\}\) is a particular case of a curve given by formula (33) (take \(c = 1\) in (33)), therefore by the preceding analysis we conclude that equation (4) will always have only finitely many solutions in this instance.

Finally, assume that \(r = k = 2\). In this case, \(b = e\theta\) and \(a = \theta^2 = (e\theta)^2\). We may therefore assume that \(e = 1\). We will treat only equation (3) since the arguments for equation (4) are entirely similar. We denote \(m\) by \(y\) in equation (3) and rewrite it as

\[
\frac{w(w-1)}{\theta(\theta-1)} = \frac{y(y-1)}{2}, \tag{37}
\]

where \(w = \theta^n\) for some \(n \geq 1\), or, equivalently

\[
(4w - 2)^2 - 2\theta(\theta - 1)(2y - 1)^2 = -2(\theta - 2)(\theta + 1). \tag{38}
\]

Let \(A = -2(\theta - 2)(\theta + 1)\) and \(B = 2\theta(\theta - 1)\). The case \(\theta = 2\) gives \((a, b) = (4, 2)\) which leads to the infinite family of solutions

\[
\frac{4^n - 2^n}{2} = \binom{2^n}{2}, \quad \text{for all } n \geq 2.
\]

From now on, we assume that \(\theta \neq 2\). Hence, \(A \neq 0\). Equation (38) becomes

\[
X^2 - BY^2 = A, \tag{39}
\]

where \(X = 4w - 2 = 4\theta^n - 2\). Notice that \(B > 0\). We distinguish two situations according to whether \(B\) is a perfect square or not. If \(B\) is a perfect
square, then equation (39) has only finitely many integer solutions \((X, Y)\). Indeed, equation (39) can be rewritten as

\[
(X - \sqrt{B}Y)(X + \sqrt{B}Y) = A,
\]

which implies that

\[
\begin{cases}
X - \sqrt{B}Y = e'd_i, \\
X + \sqrt{B}Y = e' \frac{A}{d_i},
\end{cases}
\]

for some positive divisor \(d_i\) of \(A\) and some \(e' \in \{\pm 1\}\).

Notice that \(X\) and \(Y\) are determined uniquely by the values of \(d_i | A\) and \(e' \in \{\pm 1\}\). Assume now that \(B\) is not a perfect square. In this case, the general theory of Pell equations tells us that equation (39) has infinitely many positive solutions \((X, Y)\) once it has at least one such solution (notice that \((X, Y) = (2, 1)\) is a positive solution of equation (39)). However, it is well-known that in this case, (see [33, 43]) there exist finitely many binary recurrent sequences \((W^{(1)}_m)_{m \geq 0}, (W^{(2)}_m)_{m \geq 0}, \ldots, (W^{(k)}_m)_{m \geq 0}\) such that if \((X, Y)\) is a solution of equation (39), then \(X = W^{(i)}_m\) for some \(i = 1, 2, \ldots, k\) and some \(m \geq 0, k\). More precisely, let \((U_1, V_1)\) be the minimal positive solution of the Pell equation

\[
U^2 - BV^2 = 1,
\]

and let \(\zeta = U_1 + \sqrt{B}V_1\). Then, there exist finitely many pairs \((a_i, b_i)\), say \(k\) of them, of non-zero algebraic numbers, such that if \((X, Y)\) is a solution of equation (39), then

\[
X = a_i \zeta^m + b_i \zeta^{-m}, \quad \text{for some } i = 1, 2, \ldots, k \text{ and some } m \geq 0. \quad (40)
\]

Since \(X = 4\theta^n + 2\), it follows that it is enough to show that if \(a_i\) and \(b_i\) are some fixed non-zero algebraic numbers the equation

\[
4\theta^n - 2 = a_i \zeta^m + b_i \zeta^{-m}, \quad (41)
\]

has only finitely many positive integer solutions \((n, m)\). However, from a result from [39], we know that if \((W'_m)_{m \geq 0}\) and \((T_n)_{n \geq 0}\) are two binary recurrent sequences having the property that the two roots of maximal absolute values of the characteristic equations of \((W'_m)_{m \geq 0}\) and \((T_n)_{n \geq 0}\), respectively, are multiplicatively independent, then the equation \(W'_m = T_n\) has only finitely many effectively computable solutions \((n, m)\). All that is left to notice is that if one sets \(T_n = 4\theta^n - 2\) for \(n \geq 0\) and \(W'_m = a_i \zeta^m + b_i \zeta^{-m}\) for \(m \geq 0\), then the roots of maximal absolute values of the characteristic equations of \((T_n)_{n \geq 0}\) and \((W'_m)_{m \geq 0}\) are \(\theta\) and \(\zeta\), respectively. They are certainly multiplicatively independent (because \(\zeta\) is a unit and \(|\theta| > 1\) is an
3. THE PROOF OF THEOREM 2

In this section, we show that if \( a > |b| > 0 \) and \( \gcd(a, b) \neq 1 \), then equation (4) has only finitely many solutions \((n, m, k)\) and equation (3) has only finitely many solutions \((n, m, k)\) except for the cases when \( (a, b) = (8, 2) \) and \( (a, b) = (4, 2) \). Suppose that \((n, m, k)\) is a solution of either (3) or (4). In this case, we show that there exists two computable functions \( g_1(a) \) and \( g_2(a) \) such that if \( n > g_1(a) \) then \( k < g_2(a) \).

We start with a prime number \( p \) dividing \( \gcd(a, b) \). From equation (3) or (4), it follows that \( p^{n-1} \mid \binom{m}{k} \). We now recall a result due to Kummer (see [27]).

**Proposition 2 (Kummer’s Theorem).** Let \( m > k \geq 1 \) be positive integers and let \( p \) be a prime number. Then, the order \( a_p \) at which \( p \) divides the binomial coefficient \( \binom{m}{k} \) is equal to the number of carries which occur when adding \( k \) with \( m-k \) in base \( p \). In particular, \( p^{a_p} \leq m \).

Since \( p^{n-1} \mid \binom{m}{k} \) it follows, by Kummer’s theorem above, that \( p^{n-1} \leq m \). Hence, \( m \geq 2^{n-1} \). To get an upper bound for \( k \) when \( n \) is large, notice that

\[
\left( \frac{m}{k} \right) \leq \max(|u|, |v|) < 2a^{\frac{2a}{\log 2}}.
\]

(42)

Now, if \( k \geq \sqrt{m} \) then, assuming \( m \geq 9 \), we obtain

\[
\left( \frac{m}{k} \right) > \left( \frac{m}{\sqrt{m}} \right) > \left( \frac{m - \sqrt{m}}{\sqrt{m}} \right) \geq 2^{\sqrt{m}},
\]

which, combined with (42), gives an upper bound for \( m \) depending only on \( a \), and a fortiori for \( k \). If \( k < \sqrt{m} \) then, assuming that \( m \geq 4 \), we obtain

\[
\left( \frac{m}{k} \right) > \left( \frac{m-k}{k} \right) > \left( \frac{\sqrt{m}}{2} \right)^k,
\]

which, combined with (42), bounds \( k \) in terms of \( a \).

A somewhat finer (and somewhat longer) analysis can be done to show that the function \( g_2(a) \) can be taken to be \( \max(10, 2 \log a / \log 2) \).
What the above arguments show, in particular, is that if either equation (3) or equation (4) has infinitely many positive integer solutions \((m, n, k)\), then there exists a fixed value of \(k\), let’s call it \(k_0\), for which there exist infinitely many solutions \((n, m, k)\) with \(k = k_0\). However, according to Theorem 1, this can never happen for equation (4), and it can happen for equation (3) only when \((a, b) = (8, 2)\) and \(k_0 = 3\) or \((a, b) = (4, 2), (9, 1), (7, -1)\) and \(k_0 = 2\). Since \(\gcd(a, b) \neq 1\), it follows that either \((a, b) = (8, 2)\) or \((a, b) = (4, 2)\).

We will now completely solve equation (3) when \((a, b) = (4, 2)\) or \((8, 2)\). Let \((a, b) = (4, 2)\) and assume that

\[
\binom{m}{2} = 2^{n-1}(2^n - 1) = \binom{m}{k},
\]

for some \(k \geq 3\). Clearly, \(2^{n-1} \leq m\). Since

\[
\binom{m}{k} \geq \binom{m}{3} \geq \binom{2^{n-1}}{3},
\]

we get that

\[
2^{n-1}(2^n - 1) \geq \frac{2^{n-1}(2^{n-1} - 1)(2^{n-1} - 2)}{6},
\]

which is impossible for \(n \geq 5\). Thus, one simply has to check the values of \(n \leq 4\). The only non-trivial solution is \((n, m, k) = (4, 10, 3)\).

Assume now that \((a, b) = (8, 2)\). We first treat the case

\[
\binom{m}{2}.
\]

Notice that when \(n = 2\), one gets

\[
\binom{2^{n-1} + 1}{3} = \binom{5}{3} = \binom{5}{2}.
\]

Assume now that \(n \geq 3\). Since

\[
\binom{2^{n-1} + 1}{3},
\]

it follows that equation (44) is a particular case of the diophantine equation

\[
\binom{w}{3} = \binom{m}{2}.
\]
The only solutions of equation (45) with \( w \geq 6 \) and \( m \geq 4 \) are \((w, m) = (10, 16), (22, 56)\) and \((36, 120)\). Equation (45) was first solved by Avanesov (see [1]) and later on de Weger and Stroeker (see [44]) solved a few other diophantine equations involving equal binomial coefficients (see also [23] for a different approach). At any rate, it is easy to see that equation (44) has no solution simply because all \( w \)'s which appear as solutions of equation (45) are even, therefore they cannot be of the form \( 2^n + 1 \). Assume now that

\[
u_n = \binom{m}{k},
\]

(46)

for some \( m \geq 2k \geq 8 \). Since \( m \geq 2^{n-1} \) and

\[
\binom{m}{k} > \binom{m}{4} > \binom{2^{n-1}}{4},
\]

it follows that

\[
u_n = \left(\frac{2^n + 1}{3}\right) > \binom{2^{n-1}}{4}.
\]

(47)

Inequality (47) forces \( n \leq 6 \) and one checks that equation (46) has no non-trivial solutions in the range \( 3 \leq n \leq 6 \).

Theorem 2 is therefore proved.

4. THE PROOFS OF THEOREMS 3 AND 4

The proofs of Theorems 3 and 4 are so similar that we will deal with them in the same time. In general, we will treat equation (3) in more detail and we shall only sketch the analyze for equation (4).

Assume that \((n, m, k)\) is either a solution of (3) with \( n \) prime, or a solution of (4) with \( n \) a power of 2. At the beginning, we make no restrictions on the parameters \( a \) and \( b \) except for the fact that \( a > |b| > 0 \) and \( a \) and \( b \) are coprime. We distinguish two cases, according to whether the parameter \( k \) is large or small with respect to \( n \).

Case 1. (i) Assume that \( n \nmid (a - b) \) and that \( n \geq 32 \). If \( k \geq n \) in equation (3), then \( a \neq 2 \) and

\[
n - 2 < \frac{2n \left(1 + \frac{a}{2.5}\right)}{(n - 1) \log(2.5) \log \left(1 + \frac{a}{2.5}\right)} \log \left(n \frac{\log a}{\log 2.5 \left(1 + \frac{a}{2.5}\right)}\right).
\]

(48)
Assume that \( n \geq 64 \) and that \( k > n/2 \) in equation (4). Then, \( a \neq 2 \) and

\[
n \log a - \log 2 < \frac{2(n+1) \log(a) \left(1 + \frac{a^2}{2.5}\right)}{n \log(2.5) \log \left(\frac{1}{4} + \frac{a^2}{10}\right)} \log \left(\frac{n+1}{\log 2.5} \left(1 + \frac{a^2}{2.5}\right)\right).
\]

Before proving inequality (48) and its analogue (49), let us first notice that if \( n \) satisfies inequality (48) (or (49)), then \( n \leq N_1(a) \) (respectively \( n \leq N_2(a) \)), where \( N_1(a) \) and \( N_2(a) \) are maximum values of \( n \) for which (48) and respectively (49) hold. Let \( m_1(a, b) = \max(32, P(a-b), N_1(a)) \) and \( m_2(a) = \max(64, N_2(a)) \). It follows that if \((n, m, k)\) is a solution of (3) with \( n \) prime, or a solution of (4) with \( n \) a power of 2 such that \( n > m_1(a, b) \) (respectively \( n > m_2(a) \)), then \( k < n \) (respectively \( k \leq n/2 \)). In particular, except for finitely many computable values of \( n \), every solution of (3) or (4) with \( n \) prime or \( n \) a power of 2, respectively, will satisfy \( k < n \) or \( k \leq n/2 \), respectively.

We now prove inequality (48). Since \( k \geq 32 \), it follows that

\[
k! < \left(\frac{k}{2.5}\right)^k.
\]

Indeed, inequality (50) follows from Stirling’s formula. Hence, equation (3) implies that

\[
a^n > \frac{a^n - b^n}{a - b} = \binom{m}{k} = \frac{m(m-1) \cdots (m-k+1)}{k!} > 2.5^k \left(\frac{m-k}{k}\right)^k,
\]

or

\[
\frac{m-k}{k} < \frac{a^{n/k}}{2.5}.
\]

Since \( m \geq 2k \), we get that

\[
1 < \frac{a^{n/k}}{2.5}
\]

or

\[
k < n \frac{\log a}{\log 2.5}.
\]
Notice that inequality (52) together with the fact that \( k \geq n \) shows that \( a \neq 2 \). Moreover, inequality (51) together with the fact that \( k \geq n \) imply also that

\[
m < k \left( 1 + \frac{a^{n/k}}{2.5} \right) < k \left( 1 + \frac{a}{2.5} \right). \tag{53}
\]

We now use the fact that every prime divisor of \( u_n \) is congruent to 1 modulo \( n \). Indeed, it is well-known that if \( n > a - b \) is a prime, then every prime divisor of \( u_n \) is indeed congruent to 1 modulo \( n \). This follows either from the theory of primitive divisors of Lucas sequences (see [13], for example), or can be immediately proved using Fermat’s little theorem. For any positive integer \( t > 1 \) and any real number \( y > t \) let \( \pi(y; t, 1) \) denote the number of primes less than or equal to \( y \) which are congruent to 1 modulo \( t \). From a result of Montgomery and Vaughan (see [32]), we know that

\[
\pi(y; t, 1) < \frac{2y}{\phi(t) \log(y/t)}. \tag{54}
\]

In particular,

\[
\pi(y; n, 1) < \frac{2y}{\phi(n) \log(y/n)} = \frac{2y}{(n-1) \log(y/n)}. \tag{54}
\]

Notice that since \( a \geq 3 \) and \( k \geq n \), the upper bound on \( m \) given by formula (53) is larger than \( n \). Thus, one may now use inequalities (53) and (54) to get

\[
\pi(m; n, 1) < \frac{2k \left( 1 + \frac{a}{2.5} \right)}{(n-1) \log \left( \frac{k}{n} \left( 1 + \frac{a}{2.5} \right) \right)}. \tag{55}
\]

One may now combine inequalities (52), (55) and the fact that \( k \geq n \) to get

\[
\pi(m; n, 1) < 2n \log(a) \cdot \frac{2n \log(a)}{(n-1) \log(2.5)} \cdot \frac{1}{\log \left( 1 + \frac{a}{2.5} \right)} \tag{56}
\]
Denote by \( f(a, n) \) the function appearing in the right hand side of inequality (56). Now let \( q \) be any prime number less than or equal to \( m \) which is congruent to 1 modulo \( n \). Assume that \( q^n \| (\frac{m}{k}) \). By Proposition 2, it follows that \( q^n \leq m \). Hence,

\[
  u_n = \binom{m}{k} = \prod_{q \leq m} q^n \leq m^{x(m/k, 1)} < m^{f(a, n)}. \tag{57}
\]

Since certainly \( u_n > a^{n-2} \), it follows that

\[
  a^{n-2} < m^{f(a, n)},
\]

or

\[
  n - 2 < \frac{f(a, n)}{\log a} \log(m) < \frac{f(a, n)}{\log a} \log \left( n \frac{\log a}{\log 2.5} \left( 1 + \frac{a}{2.5} \right) \right). \tag{58}
\]

Inequality (58) is exactly inequality (48).

The proof of inequality (49) follows the same pattern. First of all, since \( k \geq n/2 + 1 > 32 \), we get

\[
  a^{n+1} \geq 2a^n > a^n + b^n = \binom{m}{k} > 2.5^k \left( \frac{m-k}{k} \right)^k,
\]

therefore,

\[
  \frac{m-k}{k} < \frac{a^{(n+1)/k}}{2.5}. \tag{59}
\]

Since \( m \geq 2k \), we get

\[
  k < (n+1) \frac{\log a}{\log 2.5} \tag{60}
\]

(compare with (52)). Moreover, from inequality (6), we also get that

\[
  m < k \left( 1 + \frac{a^{(n+1)/k}}{2.5} \right) < k \left( 1 + \frac{a^2}{2.5} \right), \tag{61}
\]

because \( k \geq n/2 + 1 \) (compare (61) with (53)).
One now uses that fact that the only prime divisors of $v_n$ are either 2 (which occurs when both $a$ and $b$ are odd, but in this case $4 \nmid v_n$) or are congruent to 1 modulo $2n$ (this follows again either from the theory of primitive divisors for Lucas sequences, or from Fermat’s little theorem). One can now use the inequality from [32] to count how many prime numbers which are congruent to 1 modulo $2n$ are less than $m$. Notice that if $a \geq 3$, then the upper bound on $m$ given by formula (61) is larger than $2n$, because

$$k \left(1 + \frac{a^2}{2.5}\right) > \frac{n}{2} \left(1 + \frac{9}{2.5}\right) > 2n.$$  

Hence, one can indeed apply the inequality from [32] in this case and get that

$$\pi(m; 2n, 1) \leq \frac{2m}{\phi(2n) \log(m/2n)} < \frac{2k \left(1 + \frac{a^2}{2.5}\right)}{n \log \left(\frac{k \left(1 + \frac{a^2}{2.5}\right)}{2n}\right)}, \quad \text{(62)}$$

Combining the above inequality (62) with inequality (60) and with the fact that $k > n/2$, we get

$$\pi(m; n, 1) < \frac{2(n+1) \log(a) \left(1 + \frac{a^2}{2.5}\right)}{n \log(2.5) \log \left(\frac{1}{4} + \frac{a^2}{10}\right)}. \quad \text{(63)}$$

One can now proceed as before to get to inequality (49). The only case left is the case in which $a = 2$. But this is easily seen to be impossible. Indeed, inequality (60) implies that

$$k < (n+1) \frac{\log 2}{\log 2.5} \leq n$$

(because $n \geq 64$), therefore inequality (61) implies that

$$m < n \left(1 + \frac{4}{2.5}\right) < 3n. \quad \text{(64)}$$
However, since every prime divisor of \( v_n \) (hence, of \( \binom{n}{k} \)) in this case is congruent to 1 modulo \( 2n \), it follows that \( \binom{n}{k} \) can be divisible with at most one such prime, which is necessarily less than \( 3n \) but larger than \( 2n \). Thus, \( v_n = 2^{2n} + 1 = \binom{3n}{n} < 3n \), which is absurd.

This case is therefore completely settled.

Remark 1. The referee observed that if one only wants simply an upper bound for \( n \) in terms of \( a \), then one does not need the full force of the classical result of Montgomery and Vaughan on \( \pi(y; n, 1) \) (formulae (54) and (62)), but one may instead use the fact that there are at most \( (y-1)/n+1 \) positive integers not exceeding \( y \) which are congruent to 1 modulo \( n \). With \( y = m \) satisfying inequalities (53) and (52), we get that there are at most \( O(a \log a) \) such integers, where the implied constant is absolute. We have however preferred to use the result of Montgomery and Vaughan since otherwise the upper bounds on \( n \) in terms of \( a \) would’ve been larger and the computations required to prove Corollaries 1 and 2 (which used the upper bounds (48) and (49) on \( n \)) would have taken longer to complete.

We now treat the cases \( n > m_1(a, b) \) or \( n > m_2(a) \), respectively.

Case 2. (i) Assume that \( 2 \nmid ab \) and that \((n, m, k)\) is a solution of equation (3) with \( n \) prime and \( n > m_1(a, b) \). Then, \( k < P(ab) \).

(ii) Assume that \( b = 1 \) and that \((n, m, k)\) is a solution of equation (4) with \( n > m_2(a) \). Then \( a \) is even and \( k < \log a/\text{ord}_q(a) \log 2 \).

Here, for a positive integer \( u \) and a prime number \( q \) we used \( \text{ord}_q(u) \) for the exponent at which \( q \) appears in the prime factor decomposition of \( u \).

We treat first equation (3). To avoid confusion, we denote \( n \) by \( p \) in what follows, thus emphasizing also the fact that it is a prime. Assume that claim (i) above does not hold and let \((p, m, k)\) be a solution of (3) with \( P(ab) \leq k < p \). We use again the fact that every prime divisor of \( u_p \) is congruent to 1 modulo \( p \). Write

\[
m = \prod_{q | m} q^{s_q}
\]

and let

\[
A = \{ q \mid q \equiv 1 \pmod{p} \}.
\]

Let

\[
d = \prod_{q \in A} q^{s_q}.
\]
The next step is to show that \( d = k \). For this, we first show that \( d \mid k \). To this end, we first recall the following result due to Lucas. Assume that \( r \) is a prime and write
\[
m = m_0 + m_1 r + \cdots + m_r r^t \quad \text{for some } m_i \in \{0, 1, \ldots, r-1\} \text{ with } m_t \neq 0,
\]
(68)
and
\[
k = k_0 + k_1 r + \cdots + k_r r^t \quad \text{for some } k_i \in \{0, 1, \ldots, r-1\}.
\]
(69)

Then, Lucas’s theorem (see [31]) says the following.

**Proposition 3 (Lucas’s Theorem).** Assume that \( m > k \geq 1 \) are positive integers and that \( r \) is a prime. Assume moreover that the base \( r \) representations of \( m \) and \( k \) are given by formulae (68) and (69). Then,
\[
\binom{m}{k} \equiv \left( \binom{m_0}{k_0} \right) \left( \binom{m_1}{k_1} \right) \cdots \left( \binom{m_t}{k_t} \right) \pmod{r}.
\]
(70)

Let us go back to the claim that \( d \mid k \). This is clear if \( d = 1 \). Assume that \( d > 1 \) and choose a prime number \( q \mid d \). Since all the prime divisors of \( u_p \) are congruent to \( 1 \) modulo \( p \), it follows that \( q \nmid u_p \). But since \( q \mid d \mid m \), it follows that if one writes \( m \) in base \( q \) according to formula (68), then one gets that \( m_0 = 0 \). If \( q \nmid k \), then \( k_0 > 0 \) and now formula (70) would imply that
\[
u_p \equiv \binom{m}{k} \equiv \left( \binom{0}{k_0} \right) \left( \binom{m_1}{k_1} \right) \cdots \left( \binom{m_t}{k_t} \right) \pmod{q},
\]
which is impossible because \( q \) does not divide \( u_p \). Hence, every prime divisor of \( d \) divides \( k \) as well. To show that \( d \mid k \), we need to show that if \( q^a \mid d \), then \( q^a \mid k \). Assuming that this were not so, it follows that \( q^b \mid k \) for some \( b < a_p \). But in this case, \( m_b = 0 \) and \( k_b \neq 0 \) which, via formula (70), would imply again that \( q \) divides \( u_p \), which is impossible.

Hence, \( d \mid k \). In particular, since \( k < p \), it follows that \( d < p \) as well. We now notice that \( m \equiv d \pmod{p} \). Moreover, since \( d \leq k < p \), it follows that if one writes both \( m \) and \( k \) in base \( p \) one gets \( m_0 = d \) and \( k_0 = k \). Now Lucas’s theorem for the prime \( p \) implies that
\[
u_p \equiv \binom{m}{k} \pmod{p} \equiv \binom{d}{k} \pmod{p}.
\]
(71)
Since \( p \mid u_p \) for \( p \mid (a-b) \), congruence (71) together with the fact that \( 1 \leq d \leq k \) imply that \( d = k \). Thus, \( k \mid m \). We may now write equation (3) as

\[
 u_p = \frac{m}{k} \binom{m-1}{k-1}. \tag{72}
\]

where \( \frac{m}{k} \) is an integer. At this point, one should notice that the relevant feature of the proceeding argument was based only on the shape of the prime divisors of \( u_p \). Hence, one can iterate the above argument to get that \( (k-i) \mid (m-i) \) for all \( i \in \{0, 1, \ldots, k-1\} \). This is equivalent to

\[
 m \equiv i \pmod{k-i} \equiv k \pmod{k-i}, \quad \text{for all } i \in \{0, 1, \ldots, k-1\}. \tag{73}
\]

Let

\[
 N = \text{lcm}(1, 2, \ldots, k) = [1, 2, \ldots, k]. \tag{74}
\]

From formula (73), we get that \( m \equiv k \pmod{N} \). Write \( m = k + \lambda N \) for some positive integer \( \lambda \). Now equation (3) implies that

\[
 u_p = \binom{m}{k} = \frac{m}{k} \frac{m-1}{k-1} \cdots \frac{m-k+1}{1} = \prod_{i=0}^{k-1} \left( 1 + \frac{\lambda N}{k-i} \right). \tag{75}
\]

Let \( N_i = \frac{N}{k-i} \) and \( M_i = 1 + \lambda N_i \) for \( i \in \{0, 1, \ldots, k-1\} \). Equation (75) can rewritten as

\[
 u_p = \prod_{i=1}^{k} M_i. \tag{76}
\]

We now finally start exploiting the fact that \( 2 \parallel ab \). We first notice that \( u_p \equiv 3 \pmod{4} \). Indeed, to see why this is so, one may assume that \( a \) is odd and that \( 2 \parallel b \) and notice that

\[
 u_p \equiv \frac{a^p - b^p}{a - b} \pmod{4}
\]

or

\[
 u_p \equiv a^{p-1} + a^{p-2}b + \cdots + b^{p-1} \pmod{4} \equiv a^{p-1} + a^{p-2}b \pmod{4} \equiv 3 \pmod{4}.
\]

The case in which \( 2 \parallel a \) is odd can be dealt with similarly.
Now denote by \( \mu \) the largest integer such that \( 2^\mu \leq k \). We notice that exactly one of the numbers \( N_i \) is odd and all the other ones are even. Indeed, the only odd number \( N_i \) is precisely the one for which \( i = k - 2^\nu \).

Since all the numbers \( M_j \) are odd for \( j \in \{0, 1, \ldots, k-1\} \) (in particular, \( M_j \) as well), it follows that \( 2 \downarrow \lambda \). Moreover, since \( u_0 \equiv 3 \pmod{4} \), it follows that \( 2 \parallel \lambda \). Let \( j = k - 2^{\nu-1} \). Notice that \( \mu \geq 1 \) because \( k \geq 2 \). Then,

\[
N_j = N_{2^\mu-1} \equiv 2 \pmod{4}.
\]  (77)

Moreover, since \( k \geq P(ab) \), it follows that every odd prime dividing \( ab \) divides \( N_j \) as well. Since \( 2 \parallel \lambda \), it follows that \( M_j = 1 + \lambda N_j \equiv 5 \pmod{8} \) and \( M_j \equiv 1 \pmod{r} \) for all odd primes \( r \mid ab \). Reducing equation (76) modulo \( M_j \), we get

\[
a^p \equiv b^p \pmod{M_j},
\]
or

\[
(ab)^p \equiv b^{2^p} \pmod{M_j}.
\]  (78)

Equation (78) together with the fact that \( p \) is odd imply that \( (ab/M_j) = 1 \) (notice that \( ab \) and \( M_j \) are coprime). Here, we used \( (\cdot) \) to denote the Jacobi symbol. Write now \( ab = 2e\nu^2 \) where \( \nu \) is positive odd and squarefree and \( e \in \{\pm1\} \). The above Jacobi symbol equality becomes

\[
1 = (ab/M_j) = (2e\nu^2/M_j) = (2e\nu/M_j) = (\nu/M_j) \prod_{r \mid \nu} (r/M_j).
\]  (79)

Since

\[
\left( \frac{M_j}{r} \right) = 1,
\]

for all odd primes \( r \mid ab \) and since \( M_j \equiv 1 \pmod{4} \), the quadratic reciprocity law implies that

\[
\left( \frac{r}{M_j} \right) = 1 \quad \text{for all primes } r \mid \nu.
\]  (80)

Since \( M_j \equiv 5 \pmod{8} \), it follows that

\[
\left( \frac{\nu}{M_j} \right) = 1 \quad \text{and} \quad \left( \frac{2}{M_j} \right) = -1.
\]  (81)
But now notice that by multiplying all relations (80) and (81) we get a relation contradicting (79). This disposes of (i) of the above claim.

**Remark 2.** Incidentally, in the previous argument we have proved, among other things, the following statement which might be of independent interest.

**Proposition 4.** Assume that \(a\) and \(b\) are two integers with \(a > |b| > 0\) and that \(p\) is a prime number not dividing \(a - b\). Suppose moreover that \(m\) and \(k\) are two positive integers with \(k < \min(p, m/2)\). If \((\frac{m}{k})u_p\), then \(k | m\).

Assume now that \((n, m, k)\) is a solution of equation (4) with \(n = 2^r > m_2(a)\). In this case, \(k \leq n/2 \leq 2^{r-1}\). We assume again that the prime factor decomposition of \(m\) is given by formula (65) and we set

\[ A_1 = \{q | m, q \text{ odd and } q \not\equiv 1 \pmod{2^{s+1}}\} \tag{82} \]

Let

\[ d_1 = \prod_{q \in A_1} q^{x_q} \tag{83} \]

and

\[ d_2 = 2^{x_2}d_1. \tag{84} \]

We now want to show again that \(k | n\). If the number \(a\) is even, it follows that all prime divisors of \(v_{x_2}\) are odd and congruent to 1 modulo \(2^{s+1}\) and one can apply the above argument to conclude that \(d_2 = k\), therefore \(k | n\). The situation is slightly more complicated if \(a\) is odd. In this case one can still conclude right away that \(d_1 | k\). Moreover, since \(2 \| v_{x_2} = \binom{n}{r}\) one can use Proposition 2 again to conclude that exactly one “carry” occurs when adding \(k\) with \(m - k\) binary. It now follows that \(2^{x_2-1} | k\) whenever \(x_2 \geq 1\). Hence, \(2^{x_2-1}d_1 | k\) when \(x_2 \geq 1\) and \(d_2 = 2^{x_2}d_1 \leq 2k \leq 2^r\) in this case, while \(d_2 = d_1 | k\) when \(x_2 = 0\). Since every odd prime divisor of \(m\) which is not in \(A_2\) is congruent to 1 modulo \(2^{s+1}\), it follows that \(m \equiv d_2 \pmod{2^{s+1}}\). In particular, the last \(s+1\) binary digits of \(m\) are exactly the ones occurring in \(d_2\). If \(d_2 = k\) or \(2^{x_2-1}d_1 = k\) (when \(x_2 \geq 1\)), it follows that \(k | n\) and we are done. Assume therefore that \(2^{x_2-1}d_1\) is a divisor of \(k\) strictly less than \(k/2\) when \(x_2 \geq 1\) or \(d_1\) is a divisor of \(k\) strictly less than \(k\) when \(x_2 = 0\). We show that this is impossible. Indeed, if so, it then follows that \([\log_2(d_2)] < [\log_2(k)]\). Here, we used \(\log_2\) to denote the base 2 logarithm. But since \(k \leq 2^{r-1}\) and \(m \equiv d_2 \pmod{2^{r+1}}\), it follows easily that when adding \(k\) with \(m - k\) in base 2, at least 2 “carries” will occur (at the positions \(2^r\) and \(2^{r-1}\)).
The above arguments show that indeed \( k \mid m \). Proceeding inductively, we conclude again that \((k - i) \mid (m - i)\) for all \( i = 0, 1, \ldots, k - 1 \). Hence, one can again write

\[
v_{v'} = \prod_{i=0}^{k} M_i,
\]

(85)

where \( M_i \) where defined previously. As we have seen, there exists exactly one index \( i \), namely \( i = k - 2^a \) for which \( N_i \) is odd. If \( \lambda \) is odd, then one may choose \( j = k - 2^{a-1} \) and conclude that \( M_j = 1 + \lambda N_j \equiv 3 \pmod{4} \) which is impossible because \( v_{v'} \) cannot have divisors which are congruent to 3 modulo 4 (because \( v_{v'} \) is a sum of two coprime squares). Thus, \( \lambda \) is even, which implies that every factor \( M_i = 1 + \lambda N_i \) appearing in the right hand side of formula (85) is odd. Hence, \( a \) is even. We now use the fact that \( b = 1 \) and rewrite formula (85) as

\[
a^{2^a} + 1 = \lambda \left( \sum_{i=0}^{k-1} N_i \right) + \lambda^2 \left( \sum_{0 \leq i < j \leq k-1} N_i N_j \right) + \cdots + \lambda^{k-1} \prod_{i=0}^{k-1} N_i,
\]

or

\[
a^{2^a} = \lambda \left( \sum_{i=1}^{k} S_i \lambda^{i-1} \right),
\]

(86)

where we denoted by \( S_i \) the \( i \)th fundamental symmetric polynomial in the variables \( N_0, \ldots, N_{k-1} \). Since exactly one of the numbers \( N_i \) is odd and all the other ones are even, it follows that \( S_1 \) is odd and \( S_i \) is even for \( i \geq 2 \). In particular, the factor \( \sum_{i=1}^{k} S_i \lambda^{i-1} \) appearing in the right hand side of formula (86) is odd. From formula (86), we conclude that if \( \alpha = \text{ord}_{2}(a) \), then \( 2^{\alpha} = \text{ord}_{2}(\lambda) \). In particular, \( \lambda \geq 2^{2^\alpha} = 2^{m} \). We now return to formula (85) and use the fact that \( k \geq 2 \), to get that

\[
v_{a} = a^{n} + 1 > (1 + \lambda)^k > \lambda^k + 1 > 2^{mk} + 1,
\]

or

\[
2^{sk} < a,
\]

or

\[
k < \frac{\log a}{\alpha \log 2} = \frac{\log a}{\text{ord}_{2}(a) \log 2},
\]

which is exactly the claim made at (ii) above.
These arguments settle both claims made at Case 2.

The proofs of the Theorems 3 and 4 follow now at once. Indeed, assume that \((n, m, k)\) is a solution of equation (3) with \(n\) prime when \(a\) and \(b\) are coprime and \(2 \parallel ab\). By the previous arguments, it follows that if \(n > m_1(a, b)\), then \(k < P(ab)\). There are only finitely many such \(k\)'s and for each fixed one, equation (3) has only finitely many solutions by Theorem 1 (notice that the cases \((a, b) = (4, 2), (9, 1), (7, -1)\) and \((8, 2)\) are excluded). A similar argument applies for finishing the proof of Theorem 4.

Hence, both Theorems 3 and 4 are proved.

5. APPLICATIONS

In this Section, we prove Corollaries 1 and 2. For such applications, one first computes \(m_1(a, b)\) and \(m_2(a)\) (see Section 4) and tests \(u_n\) and \(v_n\) against being a binomial coefficient for all primes \(n \leq m_1(a, b)\) and respectively for all \(n\)'s which are powers of 2 and less than or equal to \(m_2(a)\). After this has been achieved, one still has to find all solutions \((n, m, k)\) of equation (3) with \(n > m_1(a, b)\) prime and \(k < P(ab)\) or of equation (4) with \(n > m_2(a)\) a power of 2 and \(k < \log a/\log_2(a)\) log 2. Since \(b = 1\) in equation (4), this equation is, in general, very easy to solve for small values of \(k\) but not the same is true for equation (3). However, in some cases, one can employ congruence arguments or linear forms in logarithms and solve equation (3) for some choices of \(a\) and \(b\).

Proof of Corollary 1. For small values of \(a\), the function \(\max\{m_1(a, b) \mid 0 < |b| < a\}\) is increasing and almost linear in \(a\) and \(\max\{m_1(a, b) \mid 0 < |b| < a \leq 30\} = 96\). Just in an attempt to produce more solutions for either (3) or (4), we ran a computer program which found all the solutions of (3) and (4) for \(0 < |b| < a \leq 30\) and \(n \leq 102\). From now on, we assume that we are in the hypotheses of Corollary 1 and that \((n, m, k)\) is a solution of equation (3) with \(n > 100\) prime. In particular, \(k < P(ab)\).

This shows that equation (3) has no such solutions for \((a, b) = (2, \pm 1)\). Assume now that \(P(ab) = 3\). In this case, any solution of equation (3) must have \(k = 2\). Equation (76) becomes

\[u_n = (1 + \lambda)(1 + 2\lambda),\]

where \(2 \parallel \lambda\). Since \(3 \parallel \lambda\) and \(n\) is odd, it follows that \(u_n \equiv 1 \pmod{3}\). From equation (87), it follows right away that \(3 \mid \lambda\). In particular, the factor \(1 + 2\lambda\) from the right hand side of equation (87) is congruent to 5 modulo 8 and is congruent to 1 modulo 3. The arguments from the preceding Section

\(^1\) These data are available upon request.
based on the Jacobi symbol show that equation (87) is impossible. This takes care of the cases \((a, b) = (3, \pm 2), (6, \pm 1)\). Assume now that \(5 = P(ab)\). It now follows that \(5 | ab\) and that \(k \leq 4\). If \(k = 4\), equation (76) becomes

\[ u_n = (1 + 3\lambda)(1 + 4\lambda)(1 + 6\lambda)(1 + 12\lambda), \]

where \(2 \parallel \lambda\). Since \(5 | ab\) and \(n\) is odd, it follows right away that \(u_n \equiv \pm 1 \pmod{5}\). Now equation (88) implies that \(5 | \lambda\). It now follows that the factor \(1 + 6\lambda\) is congruent to \(5\) modulo \(8\) and to \(1\) both modulo \(5\) and modulo \(3\). Now the argument from the preceding Section based on Jacobi symbol shows that equation (88) is impossible. Assume now that \(k = 3\). Equation (76) becomes

\[ u_n = (1 + 2\lambda)(1 + 3\lambda)(1 + 6\lambda), \]

where \(2 \parallel \lambda\). As we have seen, \(u_n \equiv \pm 1 \pmod{5}\). If \(u_n \equiv 1 \pmod{5}\), then equation (88) implies that \(5 | \lambda\). In this case, the factor \(1 + 6\lambda\) from the right hand side of equation (89) is congruent to \(5\) modulo \(8\) and to \(1\) both modulo \(3\) and modulo \(5\). The preceding arguments show that equation (89) is impossible. Hence, the only possibility is when \(u_n \equiv -1 \pmod{5}\). This occurs only when \((a, b) = (5, \pm 2), (10, \pm 3), (15, \pm 2)\) and \(n \equiv 3 \pmod{4}\).

We wrote a computer program which checked that equation (89) has no such solutions. The computations were done simply by testing for solutions of \(n\) coprime to 75600. That is, assume that \(n\) is a prime which is congruent to \(3\) modulo \(4\) and such that equation (89) has an integer solution \(\lambda\). This number \(n\) will belong to a certain class modulo 75600 which is coprime to 75600 and which is also 3 modulo 4. Pick now \(q\) a prime number such that \(q - 1 \mid 75600\). Now Fermat’s little theorem will tell us that equation (89) should have a solution modulo \(q\). Since 75600 has relatively many divisors of the form \(q - 1\) with \(q\) prime, we succeeded in showing that for every congruence class which is coprime to 75600 and which is congruent to \(3\) modulo \(4\), there exists at least one such prime \(q\) such that (89) is insolvable modulo \(q\). This takes care of the case \(k = 3\). Finally, assume now that \(k = 2\). Equation (76) becomes

\[ u_n = (1 + \lambda)(1 + 2\lambda), \]

where \(2 \parallel \lambda\). Equation (89) can be rewritten as

\[ 8(a^n - b^n) + (a - b) = (a - b)(4\lambda + 3)^2. \]

We first treat the case \(3 | ab\). In this case, since \(n\) is odd, it follows easily that \(3\) divides the right hand side of equation (91), and since \(3 \nmid (a - b)\), it
follows that $3 \mid (4\lambda + 3)^2$. In particular, 9 divides the left hand side of equation (91). One obtains now easily a contradiction modulo 9 in most cases. Indeed, the only instances to consider are $(a, b) = (6, \pm 5), (10, \pm 3), (15, \pm 2), (30, \pm 1)$.

If $(a, b) = (30, 1)$, then equation (91) modulo 9 is

$$8(30^n - 1) + 30 - 1 \equiv 0 \pmod{9},$$

or

$$8 \cdot 30^n + 21 \equiv 0 \pmod{9},$$

which is obviously impossible for $n \geq 2$. Similar arguments apply to $(a, b) = (30, -1), (10, \pm 3)$. Assume now that $(a, b) = (6, \pm 5)$. When $(a, b) = (6, 5)$, then equation (91) modulo 9 is

$$8(6^n - 5^n) + 1 \equiv 0 \pmod{9},$$

or

$$5^n \equiv -1 \pmod{9},$$

which forces $3 \mid n$ contradicting the fact that $n > 100$ is prime. When $(a, b) = (6, -5)$, equation (91) modulo 9 is

$$8(6^n + 5^n) + 11 \equiv 0 \pmod{9},$$

or

$$5^n \equiv 2 \pmod{9}.$$

It now follows that $n \equiv 5 \pmod{6}$. However, if one reduces equation (91) modulo 7, one gets

$$8(6^2 + 5^2) + 11 \equiv 11(4\lambda + 3)^2 \equiv 4(4\lambda + 3)^2 \pmod{7},$$

or

$$6 \equiv (8\lambda + 6)^2 \pmod{7},$$

which is impossible because $6 \equiv -1 \pmod{7}$ is not a quadratic residue modulo 7.

Assume now that $(a, b) = (15, -2)$. In this case, reducing equation (91) modulo 9 we get

$$8(15^n + 2^n) + 17 \equiv 0 \pmod{9},$$

or

$$15^n + 2^n \equiv -1 \pmod{9}. $$

This is impossible because $15^n$ and $2^n$ are not congruent to $-1 \pmod{9}$ for any $n$. Hence, we have a contradiction, and so equation (91) has no solutions in integers.
or

\[ 2^n \equiv -1 \pmod{9}, \]

which implies that \(3 \mid n\) contradicting the fact that \(n\) is a prime. Finally, when \((a, b) = (15, 2)\), one may reduce equation (91) modulo 9 to get that

\[ 8(15^n - 2^n) + 13 \equiv 0 \pmod{9}, \]

or

\[ 2^n \equiv 5 \pmod{9}, \]

which forces \(n \equiv 5 \pmod{6}\). If one reduces now (91) modulo 5 one gets

\[ 8(15^n - 2^n) + 13 \equiv 13(4\lambda + 3)^2 \pmod{5}, \]

or

\[ 2(2^{n+2} + 1) \equiv 2(4\lambda + 3)^2 \pmod{5}. \]

Since \((2^{n+2} + 1)\) is a quadratic residue modulo 5, one gets that \(n \equiv 1 \pmod{4}\). Hence, \(n \equiv 5 \pmod{12}\), which implies that \(n \equiv 17, 29, 41, 53 \pmod{60}\). Reducing now equation (91) modulo 31, one gets that the only two acceptable values of \(n\) are \(n \equiv 29, 41 \pmod{60}\), but one can also check that for \(n \equiv 41 \pmod{60}\) equation (91) has no solution modulo 61. Now \(n \equiv 29 \pmod{60}\) leads to \(n \equiv 29, 89, 149 \pmod{180}\). Finally, by reducing equation (91) modulo 181 it follows that the only acceptable value of \(n\) is \(n \equiv 89 \pmod{180}\) but for this value of \(n\) modulo 180 equation (91) has no solution modulo 19. This takes care of the situation \(|ab| = 30\).

The situation is much harder when \(|ab| = 10\). The easiest case is \((a, b) = (10, 1)\). In this case, equation (3) is simply

\[ \frac{10^n - 1}{9} = \frac{m(m - 1)}{2}, \]

or

\[ 8 \cdot 10^n + 1 = (6m - 3)^2, \]

or

\[ (6m - 3)^2 - 5(2^{(n+3)/2} \cdot 5^{(n-1)/2})^2 = 1. \quad (92) \]
In particular, the pair \((X, Y) = (6m - 3, 2^{(n+3)/2} \cdot 5^{(n-1)/2})\) is a solution of the Pell equation

\[
X^2 - 5Y^2 = 1. \tag{93}
\]

The smallest positive solution of equation (93) is \((X_1, Y_1) = (9, 4)\) and if \((X, Y)\) is any positive solution of equation (93), then \((X, Y) = (X_t, Y_t)\) for some positive integer \(t\) where

\[
X_t + \sqrt{5} Y_t = (9 + 4 \sqrt{5})^t \quad \text{for any } t \geq 1.
\]

The sequence \((Y_t)_{t \geq 0}\) is a binary recurrent sequence with \(Y_1 = 4, Y_2 = 72\) and

\[
Y_{t+2} = 18Y_{t+1} - Y_t \quad \text{for all } t \geq 1. \tag{94}
\]

It is well-known that a sequence such as \((Y_t)_{t \geq 1}\) has primitive divisors for all \(t \geq 1\), except maybe for \(t = 1, 2, 3, 6, 12\) (see [13]). Recall that a primitive divisor \(p\) of \(Y_t\) is a prime number \(p | Y_t\) such that \(p \nmid Y_s\) for any \(s < t\). In particular, every primitive divisor of \(p\) of \(Y_t\) satisfies \(p \geq t-1\). Since we are searching for solutions of the equation \(Y_t = 2^{(n+3)/2} \cdot 5^{(n-1)/2}\), it follows that \(t \leq 6\) or \(t = 12\). One can check these remaining values of \(t\) and convince oneself that equation (92) has no other solutions.

Finally, we look at the case \((a, b) = (10, -1)\). In this instance, equation (3) is simply

\[
\frac{10^n + 1}{11} = \frac{m(m-1)}{2},
\]

or

\[
8 \cdot 10^n + 19 = 11(2m - 1)^2. \tag{95}
\]

Reducing equation (95) modulo 3, we get that

\[
11(2m - 1)^2 \equiv 8 \cdot 10^n + 19 \pmod{3} \equiv 8 + 19 \pmod{3} \equiv 0 \pmod{3}. \tag{96}
\]

It now follows that \(3 | (2m - 1)\). Write \(2m - 1 = 3x\) and \(10^{(n-1)/2} = y\). Equation (95) can now be rewritten as

\[
99x^2 - 80y^2 = 19. \tag{97}
\]

Equation (97) implies that

\[
\frac{x}{y} = \sqrt{\frac{80}{99}} = \frac{19}{99} \cdot \frac{1}{\sqrt{80 \cdot 99}} \leq \frac{19}{\sqrt{80} \cdot 99} \cdot \frac{1}{2y^2}. \tag{98}
\]
From Theorem 7.2 on page 262 in [25], it follows that \( x/y \) is a convergent of \( \sqrt{80/99} \). The continued fraction expansion of \( \sqrt{80/99} \) is [0, 1, 8, 1, 8, 2, 8, 1, 8, 2, 8, 1, 8, 2, ...]. That is, if one denotes the continued fraction expansion of \( \sqrt{80/99} \) by \([a_0, a_1, ..., a_k, ...]\), then \( a_0 = 0, a_1 = 1 \) and \( a_{2k} = 8, a_{2k+1} = 2 \) and \( a_{4k-1} = 1 \) for \( k \geq 1 \). For any \( k \geq 0 \) let \( p_k/q_k \) be the \( k \)th convergent of \( \sqrt{80/99} \). It is easy to check that if \( x = p_k, y = q_k \) satisfy equation (97), then \( k \) is odd. Thus, the problem is equivalent to determining the odd values of \( k \geq 1 \) for which \( q_k = 10^{(a-1)/2} \). It is easy to see that \( q_1 = 1, q_3 = 10, q_5 = 188, q_7 = 1781 \). Moreover, by using the fact that 

\[
q_{k+2} = a_{k+2}q_{k+1} + q_k \quad \text{for all} \quad k \geq 0,
\]

one can easily show that both \((q_{4k+1})_{k \geq 0}\) and \((q_{4k+3})_{k \geq 0}\) are binary recurrent and they satisfy the same recurrence relation, namely 

\[
q_{4(k+2)+1} = 178q_{4(k+1)+1} - q_{4k+1}, \quad \text{for all} \quad k \geq 0,
\]

\[
q_{4(k+2)+3} = 178q_{4(k+1)+3} - q_{4k+3}, \quad \text{for all} \quad k \geq 0.
\]

The roots of the common characteristic equation 

\[
\lambda^2 - 178\lambda + 1 = 0,
\]

are 

\[
\lambda_{1,2} = 89 \pm 12\sqrt{55},
\]

and now one can easily check that the general formulae of the \( k \)th term of the sequences \((q_{4k+1})_{k \geq 0}\) and \((q_{4k+3})_{k \geq 0}\) are 

\[
q_{4k+1} = \left(\frac{20 + 3\sqrt{55}}{40}\right)(89 + 12\sqrt{55})^k + \left(\frac{20 - 3\sqrt{55}}{40}\right)(89 - 12\sqrt{55})^k, \quad \text{for all} \quad k \geq 0, \quad (99)
\]

and 

\[
q_{4k+3} = \left(\frac{200 + 27\sqrt{55}}{40}\right)(89 + 12\sqrt{55})^k + \left(\frac{200 - 27\sqrt{55}}{40}\right)(89 - 12\sqrt{55})^k, \quad \text{for all} \quad k \geq 0, \quad (100)
\]
Based on either formulae (99) or (100), one can easily see that $q_{4k+r} > 10^k$ for all $k \geq 1$ and $r \in \{1, 3\}$. Assume now that $10^{(n-1)/2} = q_{4k+r}$ for some $k \geq 1$ and $r \in \{1, 3\}$. On the one hand, from the preceding inequality, we get that $n-1 > 2k$. This gives us a lower bound on $n$ with respect to $k$. We now find an upper bound on $n$ with respect to $k$. In order to do this, we use a lower bound for a linear form in two $p$-adic logarithms. There are many lower bounds for linear forms in both complex and $p$-adic logarithms in the literature. We picked the following one due to Bugeaud and Laurent (see [11]).

**Theorem BL.** Let $a_1$ and $a_2$ be two algebraic numbers and let $p$ be a prime ideal of norm $p$ in $\mathbb{Q}(a_1, a_2)$. Let $f$ be the residual degree of $p$, $D = \mathbb{Q}[a_1, a_2]/f$ and $g$ be the smallest positive integer such that $a_i^g - 1 \in p$. Finally, let $A_1, A_2$ be real numbers such that $\log A_i > \max(h(a_i), \log p)$ for $i = 1, 2$. Here, we used $h(a_i)$ to denote the logarithmic heights of the algebraic numbers $a_i$ for $i = 1$ or $2$. Let $b_1, b_2$ be two positive integers and put

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}. \quad (101)$$

Finally, set

$$A = a_1^{b_1} a_2^{b_2} - 1 \quad (102)$$

and assume that $A \neq 0$. Then, the order at which the ideal $p$ divides $A$ is bounded above by

$$\text{ord}_p(A) < \frac{24pg}{(p-1)(\log p)^2} D^4 \left( \max \left\{ \log b' + \log \log p + 0.4, \frac{10 \log p}{D}, 10 \right\} \right)^2 \times \log A_1 \log A_2. \quad (103)$$

We now rewrite the equations $10^{(n-1)/2} = q_{4k+r}$, for some $k \geq 1$ and $r \in \{1, 3\}$ as

$$10^{(n-1)/2} = \left( \frac{20 - 3\sqrt{55}}{40} \right)^{89} \left( 89 - 12\sqrt{55} \right)^k$$

$$\times \left( \frac{179 + 24\sqrt{55}}{19} \right)^{89} \left( 89 + 12\sqrt{55} \right)^{2k-1} \left( 89 + 12\sqrt{55} \right). \quad (104)$$
and
\[
10^{(n-1)/2} = -\left(\frac{200-27\sqrt{55}}{40}\right)(89-12\sqrt{55})^k \\
\times \left(\left(\frac{16019+2160\sqrt{55}}{19}\right)(89+12\sqrt{55})^{2k}-1\right),
\] (105)
respectively. Notice that in \(\mathbb{Q}((\sqrt{55})\) the number 5 is a square. More precisely, \(p = 15+2\sqrt{55}\) is a prime and \(p^2\) is associated to 5. For equation (104), we choose \(\alpha_1 = (179+24\sqrt{55})/19, \alpha_2 = 89+12\sqrt{55}, b_1 = 1\) and \(b_2 = 2k\). One notices easily that \(D = 2, f = 1\) and \(g = 2\). Moreover, an immediate computation shows that one can take \(A_1 = 362\) and \(A_2 = 179\). Since equation (104) tells us that the power at which \(p\) divides \(A\) is at least \(n-1\), it follows that
\[
n-1 \leq \text{ord}_p(A) < \frac{960}{\log 5} \left(\max\{\log b' + \log \log 5 + 0.4, 5 \log 5, 10\}\right)^2 \log 362 \log 179,
\] (106)
where
\[
b' = \frac{1}{2 \log 179} + \frac{k}{\log 362} \leq \frac{1}{2 \log 179} + \frac{n-1}{2 \log 362}.
\] (107)
Inequalities (106) and (107) imply that \(n < 10^6\). An identical argument can be applied to deal with equation (105) and infer that \(n < 1.3 \cdot 10^6\) in this case.

To finish, we simply checked computationally that equation (95) has no solutions with \(n\) prime and \(100 < n < 1.5 \cdot 10^6\). Of course, we did not compute \(8 \cdot 10^n + 19\) but instead we checked that for every \(n\) prime in the range \(100 < n < 1.5 \cdot 10^6\), there exists at least one prime number \(q \leq 107\) such that
\[
\left(\frac{11(8 \cdot 10^n + 19)}{q}\right) = -1.
\]
This takes care of the situation \((a, b) = (10, -1)\).
As we mentioned in the Introduction, we have been unable to treat equation (3) for \((a, b) = (5, \pm 2)\) and \(k = 2\). At any rate, if \((a, b) = (5, 2)\) then one can rewrite equation (3) as
\[
8(5^n - 2^n) + 3 = 3(2m - 1)^2.
\]
Now one can conclude easily that if one sets \(x = 6m - 3\), then
\[
|2 \cdot 5^{(n-1)/2} \cdot \sqrt{30} - x| < \frac{24}{\sqrt{30}} \cdot \frac{1}{(1.25)^{(n-1)/2}}.
\]
In particular,
\[
\|5^{(n-1)/2} \sqrt{120}\| < \frac{24}{\sqrt{30}} \cdot \frac{1}{(1.25)^{(n-1)/2}}.
\]
Here, we used \(\|\cdot\|\) to denote the distance to the nearest integer. However, from the work of Ridout [35] on Roth’s theorem [36], we know that if \(a > 1\) is a positive integer and \(b\) is a positive integer which is not a square, then for any \(\epsilon > 0\) the diophantine inequality
\[
\|a^\epsilon \sqrt{b}\| < \frac{1}{a^{\epsilon}},
\]
has only finitely many solutions \(n\). Thus, even without the use of the results of Corvaja and Zannier from [14], it follows that equation (3) has only finitely many solutions in this case. In practice, hypergeometric methods à la Beukers [5], Bennet [4], and Dubickas [17] can be employed to effectively solve equations of the type (110) when both \(a\) and \(\epsilon\) are not too small but we got nowhere with applying this method for our particular inequality (109). Similar arguments apply for the case \((a, b) = (5, -2)\) and \(k = 2\).

Proof of Corollary 2. We used inequality (49) to compute \(m_2(a)\) for \(a \leq 30\). Clearly, \(m_2(2) = 64\). The function \(m_2(a)\) is increasing for \(a \geq 5\) and \(\max(m_2(a) | a \leq 30) < 3000\). Thus, since we are looking only for solutions of (4) for which \(n\) is a power of 2, it suffices to check for all solutions of equation (4) with \(k \geq n/2\) and \(n = 2^s\) for some \(s \leq 11\). We checked computationally for the solutions of equation (4) in this range and the only solutions found are the ones given in the statement of Corollary 2.

From now on, we assume that \(s \geq 12\). In this case, we know that \(a\) is even and that
\[
k \leq \frac{\log a}{\text{ord}_2(a) \log 2}.
\]
In particular, $k \leq 4$. Assume that $k = 4$. In this case, since $a \leq 30$, it follows, by inequality (111) that $2 \parallel a$ and that $a > 16$. With the notations from Section 4, equation (85) can be written as

$$a^2 + 1 = (1 + 3\lambda)(1 + 4\lambda)(1 + 6\lambda)(1 + 12\lambda). \quad (112)$$

Reducing equation (112) modulo 5, it follows easily that $5 \parallel a$ and that $5 \parallel \lambda$. Hence, $10 \parallel a$. Since $16 < a \leq 30$ and $4 \nmid a$, it follows that $a = 30$. Reducing now equation (112) modulo 3, we get that $3 \parallel \lambda$. From the arguments from Section 4, we know that $2^* \parallel \lambda$. One may now rewrite equation (111) as

$$a^n = \lambda(25 + 210\lambda + 720\lambda^2 + 864\lambda^3). \quad (113)$$

Since the factor in the parenthesis from the right hand side of formula (113) is not a multiple of 3, it follows that $3^* \parallel \lambda$. Hence, $6^* \parallel \lambda$. Now equation (112) implies that

$$30^* + 1 > (1 + \lambda)^4 > \lambda^2 + 1 > 6^*+1 = 1296^* + 1,$$

which is obviously impossible. Hence, $k < 4$.

Assume now that $k = 3$. Equation (85) can now be written as

$$a^2 + 1 = (1 + 2\lambda)(1 + 3\lambda)(1 + 6\lambda). \quad (114)$$

Since $2 \parallel a$ and $a \leq 30$, it follows that $17 \nmid a$. By reducing equation (114) modulo 17 we get

$$2 \equiv (1 + 2\lambda)(1 + 3\lambda)(1 + 6\lambda) \pmod{17},$$

which has no solution. Thus, $k < 3$.

Finally, assume that $k = 2$. Equation (4) becomes

$$8a^2 + 9 = (2m - 1)^2, \quad (115)$$

which forces $3 \parallel a$ and $3 \parallel (2m - 1)$. Write $a = 6d$, $y = 2^{2t-1} + 1_2^{2t-1} - 1d^{2t-1}$ and $2m - 1 = 3x$. Equation (115) becomes

$$x^2 - 2y^2 = 1, \quad (116)$$

where $2^{2t-1} \parallel y$. Equation (116) is a Pell equation whose minimal solution is $(X_1, Y_1) = (3, 2)$. Hence, by the general theory of the Pell equations, we know that $(x, y) = (X_k, Y_k)$ for some positive integer $t$ where

$$X_k + \sqrt{2}Y_k = (3 + 2\sqrt{2})^k \quad \text{for all} \quad k \geq 1.$$
Moreover, since \(2^{2s-1+1} \mid Y_i\), it follows that \(2^{2s-1} \mid t\). In particular, by the theory of the primitive divisor, it follows that \(y = Y_i\) has a prime divisor larger than \(2^{2s-1} - 1 > 2^{21} - 1 > 30\), which is impossible because \(P(y) < 30\). This disposes of the proof of Corollary 2.

6. COMMENTS AND REMARKS

In this paper, we fixed \(a, b \in \mathbb{Z}\) and looked for solutions of equations (3) and (4) in \(n, m, k \in \mathbb{N}\). Looking at the resulting data, we noticed that only solutions with both \(n\) and \(k\) small were found—except for the four infinite families with \(a, b, k \in \{(4, 2, 2), (7, -1, 2), (8, 2, 3), (9, 1, 2)\}\), of course. Furthermore, the upper limit 30 = \(2\cdot3\cdot5\) on \(a\) is rather artificial, but we extended the search limit up to \(a \leq 200\) and \(n \leq 102\) and all further solutions found had \(n \leq 6\) too. A new search up to \(a \leq 5031\) and \(n \leq 6\) produced a total of 5069 solutions for equation (4). We also searched for solutions of equation (3) in the range \(a \leq 4509\) and \(n \leq 7\) and, excluding the four infinite families given by Theorem 1, we found a total of 7555 solutions.

Next we counted both such solutions corresponding to fixed values of \(n\) and \(k\).

All solutions found, except for the four parametric families given by Theorem 1, have \(\min\{n, k\} \leq 4\) and very few solutions have \(\min\{n, k\} = 4\).

Thus, more interesting, but certainly more difficult problem, would be to investigate the equations

\[
\frac{x^n - y^n}{x - y} = \binom{m}{k},
\]

(117)

and

\[
x^n + y^n = \binom{m}{k},
\]

(118)

for fixed \(n\) and \(k\) and variable \(x, y, m\). Notice that equation (117) is interesting only for \(n \geq 3\). In light of our computer experiment, the following question seems of interest:

**Open Question.** (i) **Do equations (117) and (118) have only finitely many solutions when \(\min\{n, k\} \geq 4\)?**

(ii) **Do these equations maybe have only finitely many solutions of the above type all together (that is, when \(n\) and \(k\) are treated as unknowns as well)?**

\(^2\) These data are available upon request as well.
Equation (117) has infinitely many solutions when \((n, k) = (3, 2)\) and equation (118) has infinitely many solutions when \((n, k) = (2, 2)\). Such solutions can be found by using Pell equations. Indeed, for (117), let us take \(y = 1\). Then, equation (117) can be rewritten as

\[
2(2x + 1)^2 + 7 = (2m - 1)^2.
\] (119)

Equation (119) has the solutions \((x, m) = (0, 2)\), therefore it has in finitely many solutions. For equation (118) when \((n, k) = (2, 2)\), notice that the by taking \(m = t^2 + 1\), one gets

\[
\frac{m}{2} = \frac{t^2(t^2+1)}{2} = \left(\frac{t(t+1)}{2}\right)^2 + \left(\frac{t(t-1)}{2}\right)^2.
\] (120)

Notice that identity (120) provides a parametric family of solutions of triangular numbers which are sums of squares of two other triangular numbers. Questions of this type have been previously investigated. For example, Sierpiński (see [41]) found infinitely many triangular numbers which can be expressed simultaneously as a sum, a difference and a product of two other triangular numbers. Equation (117) can probably be solved when \((n, k) \in \{(4, 2), (3, 3)\}\). In these cases, by taking \(y = t\) as a parameter and by making some substitutions one can reduce equation (117) to an equation of the type

\[
v^2 = f(u),
\] (121)

where \(f\) is a monic polynomial of degree 3 with coefficients in \(\mathbb{Q}[t]\). For example, when \((n, k) = (4, 2)\) then, via the substitution \(v = 2m - 1, u = 2x + 2y/3\) and \(t = y/3\), equation (121) becomes

\[
v^2 = u^3 + 24t^2u + 160t^3 + 1.
\] (122)

Computational packages available nowadays can be employed, in some cases, to find all solutions over \(\mathbb{Q}(t)\) of equation (121). This approach was taken by Bremner in [7] who found all solutions in \(\mathbb{Q}(t)\) of the equation

\[
v^2 = u^3 - t^2u + 1,
\] (123)

and maybe this approach can be used to treat equations (117) in this context as well.

Similar arguments apply to equation (118) when \((n, k) \in \{(2, 3), (3, 2)\}\).

We have no idea how to attack equations (117) and (118) for other values of \(n\) and \(k\).
ACKNOWLEDGMENTS

We first thank the referee for providing several useful comments on a previous version of the manuscript, as well as for supplying Proposition 1 together with its proof. In a preliminary version of this manuscript, we have used a criterion of Davenport, Lewis and Schinzel (see [16]) for the irreducibility of a polynomial of the form \( f(x) - g(y) \in \mathbb{Q}[x, y] \) to treat the Case 2 of Theorem 1, approach which was a lot more tedious. We also thank Y. Bugeaud and A. Dubickas for helpful advice and A. Pintér, A. Schinzel, P. G. Walsh for pointing out some useful references. Finally, we thank Professor A. Dress and his research group in Bielefeld for their hospitality while this work was done. The second author was supported by the Alexander von Humboldt Foundation.

REFERENCES

8. B. Brindza, L. Hajdu, and I. Z. Ruzsa, On the equation \( x(x + d) \cdots (x + (k - 1) d) = by^l \), \textit{Glasgow Math. J.} \textbf{42} (2000), 255–262.
13. R. D. Carmichael, On the numerical factors of arithmetic forms \( a^* \pm \beta^* \), \textit{Ann. of Math.} (2) \textbf{15} (1913), 30–70.
22. K. Györy, On the diophantine equation \(n(n+1)\cdots(n+k−1) = bx^k\), *Acta Arith.* 83 (1998), 87–92.