The equation $ax^m + by^m = cx^n + dy^n$ implies that $m$ is bounded by an effectively computable number depending only on $a$, $b$, and $k$. In § 3, we shall generalize this as follows:

**Theorem 1.** Let $a 
eq 0$, $b 
eq 0$, $c$ and $d$ be integers. Suppose that $x$, $y$ are distinct positive integers and $m$, $n$ with $m < n$ are non-negative integers. Then there exists an effectively computable number $N > 0$ depending only on $a$, $b$, $c$ and $d$ such that the equation

$$ax^m + by^m = cx^n + dy^n$$

implies that $m \leq N$.

If (1) holds for $m = m_0$ and for $m = m_2$, then (2) is valid with $c = a$, $d = b$, $m = m_1$, $n = m_2$. Theorem 1, therefore, implies the following result.

**Corollary.** Let $a 
eq 0$, $b 
eq 0$ and $k$ be integers. Suppose that $x$ and $y$ are distinct positive integers. Then there exists an effectively computable number $N > 0$ depending only on $a$ and $b$ such that the equation (1) has at most one solution in non-negative integers $m$ with $m \geq N$.

The interest of the corollary lies in the fact that $N_1$ is independent not only of $x$ and $y$ but also of $k$. Compare this with the theorem of Tijdeman [22] mentioned above. Compare also with Kubota [3]. See also Farmani and Shorey [5].

Combining Theorem 1 and Theorem B (see § 2) of Schinzel [9], we have:
Theorem 2. Let \( a, b, c \) and \( d \) be fixed integers. Then the equation (2) has only finitely many solutions in integers \( x > 0, y > 0, m > 2, n > 0 \) with \( x \neq y, n < m, ax^n \neq cx^m \) such that the binary form \( ax^m + by^n \) is irreducible over the rationals.

In case \( ax^n + by^n \) is reducible over the rationals, we can combine Theorem 1 with Theorem C (see §2) due to Roth [8]. This gives immediately the following result.

Theorem 3. Let \( a \neq 0, b \neq 0, c \) and \( d \) be fixed integers. Then the equation (2) has only finitely many solutions in integers \( x > 0, y > 0, m > 2, n > 0 \) with \( x \neq y, n < m - 2, ax^n \neq cx^m \) and \( ax^n + by^n \neq 0 \).

In Theorems 2 and 3, we obtain effective bounds only for \( m \) and \( n \).

If \( x \) and \( y \) are composed of fixed primes, it is possible to give effective bounds for \( x \) and \( y \) too. Let \( P > 2 \) and denote by \( S \) the set of all positive integers composed of primes not exceeding \( P \). In §4, we shall prove:

Theorem 4. Let \( a \neq 0, b \neq 0, c \) and \( d \) be integers. Then all the solutions of (2), in integers \( x, y, m, n \) with \( x \in S, y \in S, x \neq y, n > 0, n < m, ax^n \neq cx^m \) and \( ax^n + by^n \neq 0 \), satisfy

\[
\max(x, y, m, n) \leq N_s
\]

for a certain effectively computable number \( N_s > 0 \) depending only on \( a, b, c, d \) and \( P \).

We shall use Theorem 1 for the proof of Theorem 3. For related work in the direction of Theorem 4, see Pillai [6], Mahler [4] and Tijdeman [14]. The equation (2) with \( ab = 0 \) is considered in Remarks (ii) and (iii).

I express my thanks to Professor B. Tijdeman for his valuable comments and for suggesting me improvements on an earlier draft of this paper.

2. In this section, we state the results that we use from other sources. The notations of this section are independent of the notations of the remaining paper. The proofs of Theorems 1 and 3 depend on the following result of Baker [2] on linear forms in logarithms.

Let \( a_1, \ldots, a_n \) be non-zero rational numbers of heights not exceeding \( A_1, \ldots, A_n \) respectively, where we assume that \( A_j \geq 3 \) for \( 1 \leq j \leq n \). The height of a rational number \( m/n \) with \( (m, n) = 1 \) is defined as \( \max(|m|, |n|) \).

Write

\[
\Omega' = \prod_{j=1}^{n-1} \log A_j \quad \text{and} \quad \Omega = \Omega' \log A_n.
\]

Theorem A. There exist effectively computable absolute constants \( c_1 > 0 \) and \( c_2 > 0 \) such that the inequalities

\[
0 \leq |a_1 \cdots a_n - 1| < \exp\{-(c_1 n)^{c_2} \Omega \log \Omega' \log B}\]

have no solution in rational integers \( b_1, \ldots, b_n \) with absolute values at most \( B \) (\( B \geq 2 \)).

We shall apply Theorem A with \( n, A_1, \ldots, A_n = 1 \), fixed. The theorem is best possible in its dependence on \( A_n \) and this is crucial for the proof of Theorem 1. Now we state a result of Schinzel [9] that we have applied in §1 to derive Theorem 2 from Theorem 1.

Theorem B. Let \( f(x, y) \) be an irreducible binary form (fixed) with integer coefficients of degree \( m > 2 \). Suppose that \( F(x, y) \) is a polynomial (fixed) with integer coefficients of total degree \( m \). Assume that \( n < m \). Then the equation

\[
f(x, y) = F(x, y)
\]

has only finitely many solutions in integers \( x \) and \( y \).

We remark that the method of proof of Theorem B is not effective.

Now we state a result of Roth that we have already applied in §1 to derive Theorem 3 from Theorem 1.

Theorem C. Suppose that \( F(x, y) \) is a binary form (fixed) of degree \( d \geq 3 \) with rational coefficients and without multiple factors. Then for given \( \nu < d - 2 \) there are only finitely many integers \( x, y \) with

\[
0 < |F(x, y)| < (\max(|x|, |y|))^{\nu}.
\]

We remark that the method of proof of Theorem C is not effective. Theorem C is an immediate consequence of Roth's theorem [8] on the approximations of algebraic numbers by rationals. The formulation of this theorem is taken from Schmidt ([11], p. 120).

3. In this section, we shall give a proof of Theorem 1. We remark that we shall use Theorem A thrice for the proof of Theorem 1. Denote by \( u_1, u_2, \ldots \) effectively computable positive numbers depending only on \( a, b, c \) and \( d \). Let \( x, y, m, n \) be as in Theorem 1 and suppose that they satisfy (2) and (3). It is no loss of generality to assume that \( x > y \). We can assume that \( m \geq n, n \geq u_1 \) sufficiently large. Then we have:

Lemma 1. \( ax^n + by^m \neq 0 \).

Proof. Suppose that

\[
ax^n + by^m = 0.
\]

If \( u_1 \) is large enough, we find that \( y \geq 2 \). Further \( x \) and \( y \) are composed of same primes. Since \( x > y \), there exists a prime \( p \) dividing \( x \) and \( y \) such that

\[
\operatorname{ord}_p(x) > \operatorname{ord}_p(y).
\]

Now it follows from (5) and (4) that

\[
m \leq m(\operatorname{ord}_p(x) - \operatorname{ord}_p(y)) = \operatorname{ord}_p(b) - \operatorname{ord}_p(a),
\]
which is not possible if \( u_4 \) is sufficiently large. This completes the proof of Lemma 1.

**Lemma 2.** \( m - n < u_4 \log m \).

**Proof.** We have

\[
|ax^n + dy^n| \leq u_2 x^n
\]

and

\[
|ax^n + by^n| \geq |a|x^{n-\log m}.
\]

The inequality (7) follows from Lemma 1 and Theorem A with \( n = 2 \), \( B = m \), \( A = 3\max(|a|, |b|) \) and \( A_2 = 3x \). Now the lemma follows immediately by combining (2), (7), (6) and \( x > 1 \).

In view of Lemma 2, it is sufficient to show that

\[
1 < u_3 (\log m) x^n.
\]

Now we proceed to prove (8). We can assume that \( u \) exceeds a sufficiently large number \( u_4 \). Then we have:

**Lemma 3.** \( x - y < x/3 \).

**Proof.** From (2), we obtain

\[
\left( \frac{x}{y} \right)^n = \frac{x^n - y^n}{x^n - y^n} < u_7.
\]

Now the lemma follows immediately.

Denote by \( r \) the greatest common divisor of \( x \) and \( y \). Put \( \theta = (\log m)^{-1} \).

Then we prove:

**Lemma 4.** \( r < x^{1-\theta} \).

**Proof.** Assume that \( r > x^{1-\theta} \). Then, by Lemma 3, we find that \( x^n > 3 \). Thus

\[
\log x > \theta^{-1}.
\]

Now apply Lemma 1 and Theorem A with \( n = 2 \), \( B = m \), \( A = 3\max(|a|, |b|) \) and \( A_2 = x/3 \) to obtain

\[
|ax^n + by^n| \geq |a|x^{n-\log m}.
\]

Now combining (2), (10), (6), (9) and \( n < u_4 \), we find that

\[
1 \leq m - n < u_4 \log m,
\]

which is not possible if \( u_4 \) is large enough. This completes the proof of Lemma 4.

**Proof of inequality (8).** Re-writing (2), we have

\[
ax^n(ax^n - n) = y^n(ax^n - n).
\]

Observe that \( (x/r)^n \) divides \( x - by^{m-n} \) and so

\[
(x/r)^n \leq |a|x^{n-\log m}.
\]

By Lemma 4, \( (x/r)^n \geq x/3 \).

By (12), (11) and Lemma 2, we obtain (8). As observed earlier, the proof of Theorem 1 is now complete.

**4. Proof of Theorem 4.** Let \( x, y, m, n \) be as in Theorem 4. Suppose that they satisfy (2). By Theorem 1, we conclude that \( m < N \). It is no loss of generality to assume that \( y \) is less than \( x (\geq 2) \). Denote by \( v_1, v_2, v_3 \) effectively computable positive constants depending only on \( a, b, c, d \) and \( P \). Write

\[
x = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \quad \text{and} \quad y = p_1^{\beta_1} \cdots p_k^{\beta_k},
\]

where \( p_1, \ldots, p_k \) are primes \( \leq P \) and \( \alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k \) are non-negative integers \( \leq 2 \log x \). Apply Theorem A with \( n = s + 1 \leq P + 1 \), \( A_1 = A_2 = \ldots = A_s = 2P \), \( A_{s+1} = 3\max(|a|, |b|) \) and \( B = 2m \log x \leq 2N \log x \) to conclude that

\[
|ax^n + by^n| \geq |a|x^{n-\log m}.
\]

Combining (2), (13) and (6), we find that

\[
x < x^{m-n} < (\log x)^n,
\]

which implies that \( x < v_4 \). This completes the proof of Theorem 4.

**Remarks.** (i) Let \( a \) and \( b \) be non-zero fixed integers. Then the inequality

\[
0 < |ax^n + by^n| < (\max(x, y))^{m-\log m - 1}
\]

has only finitely many solutions in positive integers \( x, y, m \) with \( \max(x, y) > 1 \) and \( m > 2 \). This follows from (7) and Theorem 0.

(ii) So far we have considered equation (2) with \( ab \neq 0 \). The case \( a = b = 0 \) is trivial. Without loss of generality, we may assume that \( a = 0 \) and \( b \neq 0 \). Suppose that \( b, c \) and \( d \) are non-zero fixed integers. Then we claim that the equation

\[
by^n = ax^n + dy^n
\]

has only finitely many solutions in integers \( x > 1, y > 1, n > 1, m > 2 \) with \( y|a \), \( m - n \geq 2 \) and \( n(n - m) \geq 6 \).

Re-writing (14), we have

\[
y^n(by^n - d) = ax^n.
\]

Since \( y^n | ax^n \) and \( y | ax^n \), we find that \( n \) is bounded. Further there exist non-zero integers \( w \) and \( x, y \) such that \( |w| \) bounded and

\[
by^n - d = wx^n.
\]
Now in view of the work of Schinzel and Tijdeman [10] and Baker [1] on the equation (15), the assertion follows immediately.

(iii) It is easy to see that the equation (14) has only finitely many solutions in integers \( x > 0, y > 0, n > 1, m \) with \( x \neq y \), \( y/m \), \( m-n \geq 2 \) and \( m(m-n) \geq 6 \) if and only if the conjecture of Pillai [7] that (1) has only finitely many solutions in integers \( m > 1, n > 1, x > 1, y > 1 \) with \( mn \geq 6 \) is correct. This conjecture of Pillai is still open. If \( b = c = d = 1 \), Tijdeman [13] proved that (14) has only finitely many solutions in integers \( x > 0, y > 0, n > 1, m \) with \( x \neq y \) and \( m-n \geq 2 \).

References


SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
Bombay, India

Received on 25.5.1980
and in revised form on 15.10.1980 (2206)

ACTA ARITHMETICA
XLI (1982)

An application of a formula of Western to the evaluation of certain Jacobsthal sums

by

R. H. Hudson (Columbia, S. C.) and K. S. Williams* (Ottawa, Ontario)

1. Introduction and summary. Let \( k \geq 2 \) be a positive integer and let \( p \) be a prime such that \( p \equiv 1 \pmod{2k} \). The Jacobsthal sum \( \Phi_k(D) \) is defined by

\[
\Phi_k(D) = \sum_{s=1}^{p-1} \frac{\mu(s^k + D)}{p},
\]

where \( D \) is an integer not divisible by \( p \) and \( \left( \frac{-1}{p} \right) \) is the Legendre symbol.

When \( k = 2 \), Jacobsthal ([5]), pp. 240–241, evaluated \( \Phi_2(D) \) when \( D \) is a quadratic residue \( \pmod{p} \) but left a sign ambiguity in its evaluation when \( D \) is a quadratic non-residue \( \pmod{p} \). Recently, the authors [3] have shown how to remove this ambiguity by using the law of quartic reciprocity. In a form given by Gosset [2]. When \( k = 3 \), von Schurks [9], p. 258, evaluated \( \Phi_3(D) \) when \( D \) is a cubic residue \( \pmod{p} \) but left an ambiguity in its evaluation when \( D \) is a cubic non-residue \( \pmod{p} \), and the authors [3] have shown how to remove this ambiguity by using a form of the law of cubic reciprocity given by Emma Lehmer [8].

When \( k = 4 \), Whiteman [12], [13] has shown that

\[
\Phi_4(D) = \begin{cases} 
-4(-1)^{\frac{p-1}{2}}c, & \text{if } D \text{ is an octic residue } \pmod{p}, \\
+4(-1)^{\frac{p-1}{2}}c, & \text{if } D \text{ is a quartic but not an octic residue } \pmod{p}, \\
\pm 4d, & \text{if } D \text{ is a quartic non-residue } \pmod{p}, \\
0, & \text{if } D \text{ is a quadratic residue } \pmod{p}, \\
\end{cases}
\]

where \( p \equiv c^3 + 2d^2 \equiv 1 \pmod{8} \) and \( c \equiv 1 \pmod{4} \).

* Research supported by Natural Sciences and Engineering Research Council Canada grant A-7293.

4 — Acta Arithmetica XLI.3