[5] B. J. Birch and D. J. Lewis, *p-adic forms*, J. Indian Math. Soc. 23 (1959), S. 11–32.
[6] E. Bombieri, *On the large sieve*, Mathematika 12 (1965), S. 201–225.
[7] H. Davenport and H. Halberstam, *Primes in arithmetic progressions*, Michigan Math. J. 13 (1966), S. 485–489.
[8] G. Greaves, *An application of the theorem of Barban, Davenport and Halberstam*, Bull. London Math. Soc. 6 (1974), S. 1–9.
[9] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, London – New York – San Francisco 1974.
[10] H. Hasse, *Zahlentheorie*, Akademie-Verlag, Berlin 1963.
[11] E. Hecke, *Algebraische Zahlen*, Chelsea Publishing Company, New York 1970.
[12] J. G. Hinz, *On the theorem of Barban and Davenport-Halberstam in algebraic number fields*, Journal of Number Theory 13(1981).
[13] E. Landau, *Über die zu einem algebraischen Zahlkörper gehörige Zetafunktion und die Ausdehnung der Tschebyschefschen Primzahlentheorie auf das Problem der Verteilung der Primideale*, J. Reine Angew. Math. 125 (1903), S. 64–188.
[14] — *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, B. G. Teubner Verlag, 1918.
[15] T. Mitsui, *On the Goldbach problem in an algebraic number field I, II*, J. Math. Soc. Japan 12 (1960), S. 290–372.
[16] O. Perron, *Algebra I*, de Gruyter, Berlin 1951.
[17] H.-E. Richert, *Selberg's sieve with weights*, Mathematika 16 (1969), S. 1–22.
[18] G. J. Rieger, *Verallgemeinerung der Siebmethode von A. Selberg auf algebraische Zahlkörper III*, J. Reine Angew. Math. 208 (1961), S. 79–90.
[19] H. Sarges, *Eine Anwendung des Selbergschen Siebes auf algebraische Zahlkörper*, Acta Arith. 28 (1976), S. 433–455.
[20] W. Schaal, *Obere und untere Abschätzungen in algebraischen Zahlkörpern mit Hilfe des linearen Selbergschen Siebes*, ibid. 13 (1968), S. 267–313.
[21] W. M. Schmidt, *Equations over finite fields*, Lecture Notes in Mathematics 536, Springer Verlag, Berlin–Heidelberg–New York 1976.
[22] C. L. Siegel, *Additive Theorie der Zahlkörper II*, Math. Ann. 88 (1923), S. 184–210.
[23] T. Tatuzawa, *On the number of integral ideals in algebraic number fields, whose norms not exceeding x*, Sci. Pap. Coll. Gen. Educ., Univ. Tokyo, 23 (1973), S. 73–86.

FACHBEREICH MATHEMATIK
UNIVERSITÄT MARBURG
Marburg/Lahn

Eingegangen am 9. 1. 1980 (1195)

ACTA ARITHMETICA
XLI (1982)

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

by

T. N. Shorey (Bombay, India)

1. For non-zero integers a, b, k and non-negative integers m, x, y with $\max(x, y) > 1$, Tijdeman [12] proved that the equation

$$ax^m+by^m = k \tag{1}$$

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 $a \neq 0$, $b \neq 0$, c and d be integers. Suppose that x, y are distinct positive integers and m, n with $n < m$ 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*

$$ax^m+by^m = cx^n+dy^n \tag{2}$$

with

$$ax^m \neq cx^n \tag{3}$$

implies that $m \leqslant N$.

If (1) holds for $m = m_1$ 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 $a \neq 0$, $b \neq 0$ and k be integers. Suppose that x and y are distinct positive integers. Then there exists an effectively computable number $N_1 > 0$ depending only on a and b such that the equation* (1) *has at most one solution in non-negative integers m with $m \geqslant N_1$.*

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 [12] mentioned above. Compare also with Kubota [3]. See also Parnami 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 $x > 0$, $y > 0$, $m > 2$, $n \geqslant 0$ with $x \neq y$, $n < m$, $ax^m \neq cx^n$ such that the binary form $aX^m + bY^m$ is irreducible over the rationals.*

In case $aX^m + bY^m$ 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 $x > 0$, $y > 0$, $m > 2$, $n \geqslant 0$ with $x \neq y$, $n < m-2$, $ax^m \neq cx^n$ and $ax^m + by^m \neq 0$.*

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 $P \geqslant 2$ 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 $x \in S$, $y \in S$, $x \neq y$, $n \geqslant 0$, $n < m$, $ax^m \neq cx^n$ and $ax^m + by^m \neq 0$, satisfy*

$$\max(x, y, m, n) \leqslant N_2$$

for a certain effectively computable number $N_2 > 0$ 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 R. 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 $\alpha_1, \ldots, \alpha_n$ be non-zero rational numbers of heights not exceeding $A_1, \ldots, A_n$ respectively, where we assume that $A_j \geqslant 3$ for $1 \leqslant j \leqslant n$. (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*

$$0 < |\alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1| < \exp\left(-(c_1 n)^{c_2 n} \Omega \log \Omega' \log B\right)$$

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

We shall apply Theorem A with $n, A_1, \ldots, A_{n-1}$ fixed. The theorem is best possible in its dependance 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 $P(x, y)$ is a polynomial (fixed) with integer coefficients of total degree n. Assume that $n < m$. Then the equation*

$$f(x, y) = P(x, y)$$

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 $d \geqslant 3$ with rational coefficients and without multiple factors. Then for given $\nu < d-2$ there are only finitely many integers x, y with*

$$0 < |F(x, y)| < \left(\max(|x|, |y|)\right)^{\nu}.$$

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 $m \geqslant u_1$ with u_1 sufficiently large. Then we have:

LEMMA 1. $ax^m + by^m \neq 0$.

Proof. Suppose that

$$ax^m + by^m = 0. \tag{4}$$

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

$$\mathrm{ord}_p(x) > \mathrm{ord}_p(y). \tag{5}$$

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

$$m \leqslant m\left(\mathrm{ord}_p(x) - \mathrm{ord}_p(y)\right) = \mathrm{ord}_p(b) - \mathrm{ord}_p(a),$$

which is not possible if u_1 is sufficiently large. This completes the proof of Lemma 1.

LEMMA 2. $m-n \leqslant u_2 \log m$.

Proof. We have

(6) $$|cx^n + dy^n| \leqslant u_3 x^n$$

and

(7) $$|ax^m + by^m| \geqslant |a| x^{m-u_4 \log m}.$$

The inequality (7) follows from Lemma 1 and Theorem A with $n = 2$, $B = m$, $A_1 = 3\max(|a|, |b|)$ 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

(8) $$n \leqslant u_5 (\log m)^3.$$

Now we proceed to prove (8). We can assume that n exceeds a sufficiently large number u_6. Then we have:

LEMMA 3. $x - y \leqslant x/3$.

Proof. From (2), we obtain

$$\left(\frac{x}{y}\right)^n = \frac{d - by^{m-n}}{ax^{m-n} - c} \leqslant u_7.$$

Now the lemma follows immediately.

Denote by r the greatest common divisor of x and y. Put $\theta = (\log m)^{-2}$. Then we prove:

LEMMA 4. $r \leqslant x^{1-\theta}$.

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

(9) $$\log x > \theta^{-1}.$$

Now apply Lemma 1 and Theorem A with $n = 2$, $B = m$, $A_1 = 3\max(|a|, |b|)$ and $A_2 = x^\theta > \max\left(\frac{x}{r}, \frac{y}{r}\right)$ to obtain

(10) $$|ax^m + by^m| \geqslant |a| x^{m - u_8 \theta \log m}.$$

Now combining (2), (10), (6), (9) and $n < m$, we find that

$$1 \leqslant m - n \leqslant u_9 \theta \log m,$$

which is not possible if u_6 is large enough. This completes the proof of Lemma 4.

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

$$x^n (ax^{m-n} - c) = y^n (d - by^{m-n}).$$

Observe that $(x/r)^n$ divides $d - by^{m-n} \neq 0$ and so

(11) $$(x/r)^n \leqslant |d - by^{m-n}| \leqslant u_{10} x^{m-n}.$$

By Lemma 4,

(12) $$(x/r)^n \geqslant x^{n\theta}.$$

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 $m \leqslant N$. It is no loss of generality to assume that y is less than x (> 2). Denote by v_1, v_2, v_3 effectively computable positive constants depending only on a, b, c, d and P. Write

$$x = p_1^{a_1} \ldots p_s^{a_s} \quad \text{and} \quad y = p_1^{b_1} \ldots p_s^{b_s}$$

where $p_1, \ldots, p_s$ are primes $\leqslant P$ and $a_1, \ldots, a_s$, $b_1, \ldots, b_s$ are non-negative integers $\leqslant 2\log x$. Apply Theorem A with $n = s+1 \leqslant P+1$, $A_1 = A_2 = \ldots \ldots = A_s = 2P$, $A_{s+1} = 3\max(|a|, |b|)$ and $B = 2m\log x \leqslant 2N\log x$ to conclude that

(13) $$|ax^m + by^m| \geqslant |a| x^m (\log x)^{-v_1}.$$

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

$$x \leqslant x^{m-n} \leqslant (\log x)^{v_2},$$

which implies that $x \leqslant v_3$. This completes the proof of Theorem 4.

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

$$0 < |ax^m + by^m| < \left(\max(x, y)\right)^{m - (\log m)^2 - 1}$$

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 C.

(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

(14) $$by^m = cx^n + dy^n$$

has only finitely many solutions in integers $x > 1$, $y > 1$, $n > 1$, m with $y \nmid x$, $m - n \geqslant 2$ and $n(m-n) \geqslant 6$.

Re-writing (14), we have

$$y^n (by^{m-n} - d) = cx.$$

Since $y^n \mid cx^n$ and $y \nmid x$, we find that n is bounded. Further there exist non-zero integers w and x_1 such that $|w|$ bounded and

(15) $$by^{m-n} - d = w x_1^n.$$

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 $x > 1$, $y > 1$, $n > 1$, m with $x \neq y$, y/x, $m-n \geqslant 2$ and $n(m-n) \geqslant 6$ 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 $mn \geqslant 6$ 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 $x > 1$, $y > 1$, $n > 1$, m with $x \neq y$ and $m-n \geqslant 2$.

References

[1] A. Baker, *Bounds for the solutions of the hyper-elliptic equation*, Proc. Camb. Philos. Soc. 65 (1969), pp. 439–444.
[2] —, *The Theory of Linear Forms in Logarithms*, Transcendence Theory: Advances and Applications, Academic Press, London and New York 1977, pp. 1–27.
[3] K. K. Kubota, *On a conjecture of Morgan Ward II*, Acta Arith. 33 (1977), pp. 29–48.
[4] K. Mahler, *Zur Approximation algebraischer Zahlen*, Math. Ann. 107 (1933), pp. 691–730 and 108 (1933), pp. 37–55.
[5] J. C. Parnami and T. N. Shorey, *Subsequences of binary recursive sequences*, Acta Arith. 40(1982), pp. 193–196.
[6] S. S. Pillai, *On the inequality* $0 < a^x - b^y \leqslant n$, J. Indian Math. Soc. 19 (1931), pp. 1–11.
[7] — *On the equation* $2^x - 3^y = 2^X + 3^Y$, Bull. Calcutta Math. Soc. 37 (1945), pp. 15–20.
[8] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), pp. 1–20.
[9] A. Schinzel, *An improvement of Runge's theorem on Diophantine equations*, Commentarii Pontif. Acad. Sci. 2, No 20 (1968).
[10] A. Schinzel and R. Tijdeman, *On the equation* $y^m = P(x)$, Acta Arith. 31 (1976), pp. 199–204.
[11] W. M. Schmidt, *Diophantine Approximation*, Lecture Notes in Mathematics, No. 785, Springer, Berlin 1980.
[12] R. Tijdeman, *Some applications of Baker's sharpened bounds to Diophantine equations*, Séminaire Delange–Pisot–Poitou, 16, No. 24 (1975).
[13] — *On the equation of Catalan*, Acta Arith. 29 (1976), pp. 197–209.
[14] — *Diophantine Equations (Approximation methods)*, Studieweek getaltheorie en computers, Mathematical Centre, Amsterdam 1980, pp. 261–277.

SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
Bombay, India

Received on 2. 5. 1980
and in revised form on 15. 10. 1980 (1206)

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 $k \geqslant 2$ 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

$$(1.1)\qquad \Phi_k(D) = \sum_{x=1}^{p-1} \left(\frac{x(x^k+D)}{p}\right),$$

where D is an integer not divisible by p and $\left(\frac{}{p}\right)$ is the Legendre symbol. When $k=2$, Jacobsthal ([5], pp. 240–241) evaluated $\Phi_2(D)$ when D is a quadratic residue (mod p) but left a sign ambiguity in its evaluation when D is a quadratic non-residue (mod 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 Schrutka ([9], p. 258) evaluated $\Phi_3(D)$ when D is a cubic residue (mod p) but left an ambiguity in its evaluation when D is a cubic non-residue (mod 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 [6].

When $k=4$, Whiteman [12], [13] has shown that

$$(1.2)\qquad \Phi_4(D) = \begin{cases} -4(-1)^{(p-1)/8}c, & \text{if } D \text{ is an octic residue } (\text{mod } p),\\ +4(-1)^{(p-1)/8}c, & \text{if } D \text{ is a quartic but not an octic residue } (\text{mod } p),\\ 0, & \text{if } D \text{ is a quadratic but not a quartic residue } (\text{mod } p),\\ \pm 4d, & \text{if } D \text{ is a quadratic non-residue } (\text{mod } p),\end{cases}$$

where $p = c^2 + 2d^2 \equiv 1 \pmod 8$, $c \equiv 1 \pmod 4$.

* Research supported by Natural Sciences and Engineering Research Council Canada grant A-7233.