Seminaire Delange-Pisot-Poitou
(Theorie des Nombres)
1980-81

ON SOME DIOPHANTINE EQUATIONS AND RELATED LINEAR RECURRENCE SEQUENCES

C. L. Stewart

Recently Shorey and Stewart [10] proved the following result.

Theorem 1. Let a, b, c and d be integers with b^2-4ac and acd non-zero. If x, y and t are integers with $|x|$ and t larger than one satisfying

$$ax^{2t} + bx^t y + cy^2 = d , \tag{1}$$

then the maximum of $|x|$, $|y|$ and t is less than C, a number which is effectively computable in terms of a, b, c and d.

One feature of the above result is that the exponent t is a variable. The proof depends in part upon a precise lower estimate for linear forms in the logarithms of algebraic numbers due to Baker [1]. This estimate is essentially best possible in terms of the height of one of the algebraic numbers. R. Tijdeman [12] made use of a similar estimate for his proof that there are only finitely many solutions of Catalan's equation $x^m-y^n = 1$, in integers x, y, m and n all larger than one. Tijdeman's advance initiated much work on exponential Diophantine equations, and in [13] he has chronicled progress in this area. If t is equal to one in (1) and a, b, c, d are integers with d non-zero and b^2-4ac positive and not a perfect square then Gauss proved, in contrast to Theorem 1, that if

$$ax^2 + bxy + cy^2 = d ,$$

has one solution in integers x and y then the equation has infinitely many solutions in integers x and y.

As an intermediate step in the proof of Theorem 1 we show that a certain binary recurrence sequence is a pure power only finitely many times. In fact we are able to prove such a result in general. Let r and s be integers with r^2+4s non-zero. Let u_0 and u_1 be integers and put

$$u_n = ru_{n-1} + su_{n-2} ,$$

for $n = 2, 3, \ldots$. Then for $n \geq 0$ we have

$$u_n = a\alpha^n + b\beta^n , \tag{2}$$

where α and β are the two roots of X^2-rX-s and

$$a = \frac{u_0\beta-u_1}{\beta-\alpha} , \quad b = \frac{u_1-u_0\alpha}{\beta-\alpha} ,$$

whenever $\alpha \neq \beta$. The sequence of integers $(u_n)_{n=0}^{\infty}$ is a binary recurrence sequence. It is said to be non-degenerate if $ab\alpha\beta$ is non-zero and α/β is not a root of unity. We proved with T. N. Shorey [10]:

Theorem 2. Let d be a non-zero integer and let u_n, defined as in (2), be the n-th term of a non-degenerate binary recurrence sequence. If

$$dx^q = u_n ,$$

for integers x and q larger than one, then the maximum of x, q and n is less than C, a number which is effectively computable in terms of a, α, b, β and d.

If $(u_n)_{n=0}^{\infty}$ is a non-degenerate binary recurrence sequence then $|u_n|$ tends to infinity with n hence u_n is a pure power for only finitely many integers n. For the proof we first show that q is bounded and to this end we employ the estimate of Baker [1] referred to above when α and β are real, while if α and β are not real we appeal to a p-adic analogue of Baker's result due to van der Poorten [8]. We next bound x by means of a result of Kotov [4]. Let K be an algebraic number field, let m and n be distinct integers with $m \geq 2$ and $n \geq 3$, and let α, β, x and y be non-zero algebraic integers from K with x and y coprime. In 1976 Kotov proved that the greatest prime factor of $\mathrm{Norm}_{K/Q}(\alpha x^m+\beta y^n)$ tends to infinity with $\max\{|\mathrm{Norm}_{K/Q}(x)|, |\mathrm{Norm}_{K/Q}(y)|\}$ and this is useful for us here. To conclude we use the fact that $|u_n|$ tends to infinity with n to bound n.

Petho [6] has obtained a similar result to Theorem 2. He proved that if we suppose, in addition to the hypotheses of Theorem 2, that r and s are coprime then the maximum of x, q and n is less than a number which is effectively computable in terms of a, α, b, β and the greatest prime factor of d. Petho observed that for $n \geq 0$

$$u_{n+1}^2 - ru_{n+1}u_n - su_n^2 = t(\alpha\beta)^n , \tag{3}$$

where $t = u_1^2 - ru_0u_1 - su_0^2$. Since (3) is solvable in terms of u_{n+1} there exists an integer z such that

$$(r^2+4s)u_n^2 = z^2 - 4t(\alpha\beta)^n \quad . \tag{4}$$

To conclude, Petho replaces u_n by dx^q in the above equation and employs a result of Shorey, van der Poorten, Tijdeman and Schinzel [9]. They proved that if $f \in Q[z, y]$ is a binary form with $f(1, 0) \neq 0$ such that $f(z, 1)$ has $k(\geq 2)$ distinct roots and if for non-zero integers, w, x, $q(\geq 2)$, z and y

$$wx^q = f(z, y) \quad ,$$

with z and y coprime, $|z|>1$ and $qk \geq 6$ then

$$\max \{|w|, |x|, |q|, |z|, |y|\} < C \quad ,$$

where C is a positive number which is effectively computable in terms of f and the greatest prime factor of wy.

For the Fibonacci sequence $(t_n)_{n=0}^{\infty}$ Cohn [3] proved that t_n is a square or twice a square only when n is 0, 1, 2, 3, 6 or 12. Petho [7] has shown that t_n is a perfect cube only when n is 0, 1, 2 or 6. At Oberwolfach in April of this year Mignotte and Waldschmidt remarked that indeed the distance from t_n to the closest square tends to infinity with n. If $t_n = (\alpha^n-\beta^n)/(\alpha-\beta)$ and $v_n = \alpha^n+\beta^n$ for $n > 0$ then we have

$$v_n^2 - (\alpha-\beta)^2\, t_n^2 = 4(\alpha\beta)^n = \pm 4 \quad . \tag{5}$$

Let x and c be integers and assume $t_n = x^2+c$. Since $(\alpha-\beta)^2 = 5$

$$v_n^2 = 5x^4 + 10cx^2 + 5c^2 \pm 4 \quad . \tag{6}$$

Since $5X^4 + 10cX^2 + 5c^2 \pm 4$ has distinct roots it follows from Siegel's theorem [11] on the finiteness of the number of solutions of the hyper-elliptic equation that all the integers v_n which are solutions of (6) are less than some fixed positive number in absolute value hence, since $|v_n|$ tends to infinity with n, n is bounded. The result now follows. Combining the argument of Mignotte and Waldschmidt with that of Petho and [10] we see that the distance between u_n and the closest pure power tends to infinity with n whenever u_n is the n-th term of a non-degenerate binary recurrence sequence for which $\alpha\beta = \pm 1$. In particular, it suffices to show that if x, q, c and n are integers with $x^q + c = u_n$ and $q \geq 2$ then n is bounded in terms of a, α, b, β and c. If $|x|$ is larger than one then by Lemma 6 of [10], q is so bounded. We now argue as above with (4) in place of (5). Note that t is not zero since $\alpha\beta = \pm 1$ and the sequence is non-degenerate.

For linear recurrence sequences of order larger than two not much is known. Let u_n be the n-th term of a general linear recurrence sequence whose associated characteristic polynomial has one root of largest absolute value. In this case Shorey and Stewart [10] have proved, subject to some hypotheses to avoid degeneracy, that u_n is not a q-th power for q larger than C, where C is an effectively computable positive number which does not depend on n. In fact we use a result of this sort together with a generalization to algebraic number fields of Baker's theorem [2] on solutions of the hyperelliptic equation to prove the following theorem concerning simultaneous quadratic equations.

Theorem 3. *Let* $a, b, c, d, a_1, b_1, c_1$ *and* d_1 *be integers with* a, c, d, a_1, c_1 *and* d_1 *non-zero. Assume the simultaneous equations*

$$a_1x^2+b_1xy+c_1y^2 = d_1 \quad , \tag{7}$$

$$ax^2+bxy+cy^2 = dz^q \quad , \tag{8}$$

have solutions in integers $x, y, z,$ *and* q *with* $|z|$ *and* q *larger than one. Let* α_1 *and* α_2 *be the roots of* $a_1x^2+b_1x+c_1$. *If* α_1 *and* α_2 *are not roots of* ax^2+bx+c, $b_1^2 \neq 4a_1c_1$ and $b^2 \neq 4ac$ *then the maximum of* $|x|, |y|, |z|,$ *and* q *is less than* C, *a number which is effectively computable in terms of* $a, b, c, d, a_1, b_1, c_1$ *and* d_1.

Mordell, p. 59 of [5], showed that if $q = 2$ then the simultaneous equations (7) and (8) have only finitely many solutions in integers x, y and z since they correspond to solutions of a finite number of equations involving binary quartic forms and by a result of Thue they are finite in number.

REFERENCES

[1] A. Baker, A sharpening of the bounds for linear forms in logarithms II, Acta Arith. 24 (1973), 33-36.

[2] A. Baker, Bounds for the solutions of the hyperelliptic equation, Proc. Camb. Philos. Soc. 65 (1969), 439-444.

[3] J.H.E. Cohn, On square Fibonacci numbers, J. Lond. Math. Soc., 39 (1964), 537-540.

[4] S.V. Kotov, Uber die maximale Norm der Idealteiler des Polynoms $\alpha x^m+\beta y^n$ mit den algebraischen Koeffizienten, Acta Arith. 31 (1976), 219-230.

[5] L.J. Mordell, Diophantine equations, Academic Press, London and New York, 1969.

[6] A. Petho, Perfect powers in second order linear recurrences, J. Number Theory, to appear.

[7] A. Petho, private letter, January 9, 1980.

[8] A.J. van der Poorten, Linear forms in logarithms in the p-adic case, Transcendence theory: advances and applications, Academic Press, London and New York, 1977.

[9] T.N. Shorey, A.J. van der Poorten, R. Tijdeman and A. Schinzel, Applications of the Gel'fond-Baker method to Diophantine equations, Transcendence Theory: Advances and Applications, Academic Press, 1977.

[10] T.N. Shorey and C.L. Stewart, On the Diophantine equation $ax^{2t} + bx^ty + cy^2 = d$ and pure powers in recurrence sequences, Math. Scand., to appear.

[11] C.L. Siegel, The integer solutions of the equation $y^2 = ax^n+bx^{n-1}+\ldots+k$ (under the pseudonym X), J. London Math. Soc. 1 (1926), 66-68.

[12] R. Tijdeman, On the equation of Catalan, Acta Arith. 29 (1976), 197-209.

[13] R. Tijdeman, Exponential Diophantine equations, Proc. Intern. Congress Math. Helsinki (1978), Helsinki (1979), 381-387.

C.L. Stewart

University of Waterloo

Waterloo, Ontario, Canada