# Second thoughts on some topics from Diophantine approximation and analytic number theory

**C. L. Stewart**[1]

## 1 Introduction

I would like to thank the editors for asking me to contribute an article to this volume on the occasion of the Canadian Mathematical Society's fiftieth anniversary. I am honoured to do so. My intention in this paper is to highlight some of the problems which have occupied my attention over the past twenty years.

## 2 Polynomial congruences

Perhaps the most elementary problem which I have worked on is that of estimating the number of solutions of polynomial congruences in one variable. I was led to study this problem because I needed precise estimates for application in the study of Thue equations, see §9.

Let $f$ be a polynomial of degree $r \geq 2$ with integer coefficients, say

$$f(x) = a_r x^r + a_{r-1}x^{r-1} + \cdots + a_0 \ ,$$

and suppose that $f$ factors over the complex numbers as

$$f(x) = a_r(x - \alpha_1)\cdots(x - \alpha_r) \ .$$

The discriminant $D$ of $f$ is defined by

$$D = a_r^{2r-2}\prod_{i<j}(\alpha_i - \alpha_j)^2 \ .$$

Let $m$ be a positive integer. A natural question to ask is the following. How many solutions modulo $m$ does the congruence

$$f(x) \equiv 0 \pmod{m}$$

have? By the Chinese Remainder Theorem it suffices to establish an upper bound for the case when $m$ is a power of a prime, say $p^k$. Let us denote the number of solutions by $N = N(f, p, k)$. Let $l = l(p, D)$ be defined by $l = \mathrm{ord}_p D$, in other words $p^l | D$ and $p^{l+1} \not| D$. We shall assume henceforth that $p$ does not divide the content of $f$.

If $p$ does not divide $D$ then $N$ is at most $r$ by Hensel's Lemma. In 1921 Nagell [54] and Ore [55] independently proved that

$$N \leq rp^{2l}.$$

[1]Research supported in part by Grant A3528 from the National Sciences and Engineering Research Council of Canada.

This was improved by Sándor [60], in a paper which appeared in 1952, to

$$N \leq rp^{l/2} \quad \text{for } k > l \ .$$

In fact Sándor was killed in 1944 in the Second World War. He had communicated his result to Rédei who arranged for its publication. In 1981, Huxley [38], unaware of the work of Sándor, proved

$$N \leq rp^{l/2} \quad \text{for } k > 0 \ .$$

For any real number $\theta$ let $[\theta]$ denote the largest integer less than or equal to $\theta$. In 1991 we proved [80] that

$$N \leq 2p^{[l/2]} + r - 2 \ . \tag{1}$$

Let us see that this result is, in general, best possible. Let $r$ and $j$ be positive integers with $r \geq 2$ and let $p$ be a prime with $p > r$. Put

$$f(x) = x(x + p^j)(x + 1) \cdots (x + r - 2) \ .$$

Then $l = \mathrm{ord}_p D = 2j$ and the solutions of $f(x) \equiv 0 (\mathrm{mod} p^{2j+1})$ are given by $x \equiv 0 (\mathrm{mod} p^{j+1}), x \equiv -p^j (\mathrm{mod} p^{j+1})$ and $x \equiv -i (\mathrm{mod} p^{2j+1})$ for $i = 1, \ldots, r-2$. In this case the number of solutions modulo $p^{2j+1}$ is

$$p^j + p^j + r - 2 = 2p^{l/2} + r - 2 \ .$$

While our upper bound (1) is, in general, precise, if $k$ is small compared to $l$ then we can improve on (1). For any prime $p$ and integers $r, k$ and $D$ with $r \geq 2$ and $D \neq 0$ we define $T = T(r, k, p, D)$ by

$$T = \min_{j=0,\ldots,r-2} \left\{ \left[ \frac{l}{(j+1)(j+2)} + \frac{jk}{(j+2)} \right] \ , \ \left[ \left( \frac{r-1}{r} \right) k \right] \right\} \ . \tag{2}$$

Thus

$$T = \begin{cases} \left[ \dfrac{l}{2} \right] & \text{if } k \geq l \ , \\ \left[ \dfrac{l}{(j+1)(j+2)} + \left( \dfrac{j}{j+2} \right) k \right] & \text{if } \dfrac{l}{j} \geq k \geq \dfrac{l}{j+1} \text{ for } j = 1, \ldots, r-2 \ , \\ \left[ \left( \dfrac{r-1}{r} \right) k \right] & \text{if } \dfrac{l}{r-1} \geq k \geq 1 \ . \end{cases}$$

**Theorem 1** *Let $p$ be a prime and let $f$ be a polynomial with integer coefficients, degree $r(\geq 2)$, non-zero discriminant $D$ and content coprime with $p$. For each positive integer $k$ there is an integer $t$ with $0 \leq t \leq r$ and there are non-negative integers $b_1, \ldots, b_t$ and $u_1, \ldots u_t$ such that the complete solution of the congruence*

$$f(x) \equiv 0 (\mathrm{mod} p^k)$$

*is given by the t congruences* $x \equiv b_i (\mathrm{mod} p^{k-u_i})$, *for* $i = 1, \ldots, t$. *Further*

$$u_1 + \cdots + u_t \leq 2 \left[ \frac{l}{2} \right] \tag{3}$$

*and*

$$0 \leq u_i \leq T \ , \tag{4}$$

*for* $i = 1, \ldots, t$.

Estimates (3) and (4) are both sharp. Observe that the single congruence $x \equiv b_i (\mathrm{mod} p^{k-u_i})$ is equivalent to the $p^{u_i}$ congruence $x \equiv a_j (\mathrm{mod} p^k)$ where $a_j = b_i + j p^{k-u_i}$ for $j = 1, \ldots, p^{u_i}$. Thus the number of solutions modulo $p^k$ of $f(x) \equiv 0 (\mathrm{mod} p^k)$ is $p^{u_1} + \cdots + p^{u_t}$. Since for any positive integers $u, v$ with $u \geq v$ we have

$$p^{u+1} + p^{v-1} > p^u + p^v \ ,$$

and since $t \leq r, u_1 + \cdots + u_t \leq 2 \left[ \frac{l}{2} \right]$ and $T \leq \left[ \frac{l}{2} \right]$, we see that

$$p^{u_1} + \cdots + p^{u_t} \leq 2 p^{[\frac{l}{2}]} + r - 2 \ .$$

The proof of Theorem 1 depends on a careful $p$-adic analysis in $\Omega_p$, the completion of an algebraic closure of $\mathbb{Q}_p$. In the fall term of 1992 I visited Wolfgang Schmidt at the University of Colorado in Boulder. We studied the related problem of determining the possible solution trees of polynomial congruences modulo powers of a prime $p$, [68].

# 3 Lucas and Lehmer numbers

For any integer $n$, let $P(n)$ denote the greatest prime factor of $n$ with the convention that $P(0) = P(1) = P(-1) = 1$. In 1965 Erdös conjectured that

$$\frac{P(2^n - 1)}{n} \to \infty$$

as $n$ tends to infinity. The elementary result that $P(a^n - b^n) \geq n + 1$ when $n > 2$ and $a > b > 0$, was first proved by Zsigmondy [89] in 1892 and was rediscovered by Birkhoff and Vandiver [11] in 1904. Bang [9] had obtained such a result when $b = 1$ in 1886. In 1962 Schinzel [63] showed that $P(a^n - b^n) \geq 2n + 1$ if $ab$ is a square or twice a square. Let $\kappa$ be a real number with $0 < \kappa < 1/\log 2$. In my first paper [73] I made some progress towards Erdös' conjecture. We proved that

$$\frac{P(a^n - b^n)}{n} \to \infty$$

as $n$ runs through the sequence of primes and more generally as $n$ runs through those integers with at most $\kappa \log\log n$ distinct prime factors. Andrzej Schinzel was a visitor to Cambridge

when I obtained this result and his interest in my work was enormously encouraging for me since at the time I was a beginning graduate student.

In 1878 Lucas, [47], in an article in the first volume of the American Journal of Mathematics, investigated the integer sequences $(u_n)_{n=0}^{\infty}$ where

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{for } n = 0, 1, 2, \dots \ ,$$

and where $\alpha$ and $\beta$ are distinct roots of a quadratic equation $x^2 - Px - Q = 0$ with relatively prime non-zero integer coefficients $P$ and $Q$. Lucas was not the first to study such sequences, Euler, Lagrange, Gauss, Dirichlet and others did so also , but his treatment was the most comprehensive. Such sequences are the natural generalization of the sequences $(a^n - b^n)_{n=0}^{\infty}$ with $a$ and $b$ coprime integers and are known as Lucas sequences. Lucas sequences are divisibility sequences. In other words if $m|n$ then $u_m|u_n$. In fact, more generally, we have

$$(u_m, u_n) = u_{(m,n)} \ ,$$

for all positive integers $m$ and $n$. Matijasevic exploited this property of Lucas sequences in order to resolve Hilbert's $10^{th}$ problem. Lucas numbers arise in many other settings, for example in the solutions of Pell's equation $x^2 - dy^2 = 1$, where $d$ is a positive integer which is not a perfect square, and in primality testing.

In 1930 Lehmer [43] introduced the sequences $(u_n)_{n=0}^{\infty}$ where

$$u_n = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & \text{for } n \text{ odd} \ , \\ \\ \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{for } n \text{ even} \ , \end{cases}$$

and where $\alpha\beta$ and $(\alpha + \beta)^2$ are coprime integers. The sequences are known as Lehmer sequences. Lehmer showed that his sequences had similar divisibility properties to those of Lucas sequences and he used them to extend the Lucas test for primality.

In [69], with T. N. Shorey, and in [74] and [79] we generalized our results on $P(a^n - b^n)$ to give lower bounds for the greatest prime factor and the greatest square-free factor of the $n$-th term of a Lucas or Lehmer sequence $(u_n)_{n=0}^{\infty}$. For example, we proved that there is a positive number $c$, which is effectively computable in terms of $\alpha$ and $\beta$, such that if $p$ is a prime number then

$$P(u_p) > cp \log p \ .$$

A primitive divisor of a Lucas number $u_n$ is a prime which divides $u_n$ but does not divide $(\alpha - \beta)^2 u_2 \cdots u_{n-1}$. Similarly a primitive divisor of a Lehmer number $u_n$ is a prime which divides $u_n$ but does not divide $(\alpha - \beta)^2(\alpha + \beta)^2 u_3 \cdots u_{n-1}$. Suppose now that $(\alpha + \beta)^2$ and $\alpha\beta$ are coprime integers. We may write

$$\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha, \beta) \ , \tag{5}$$

where

$$\Phi_d(\alpha,\beta) = \prod_{\substack{j=1\\(j,d)=1}}^{d} (\alpha - \zeta^j\beta)$$

and where $\zeta$ is a primitive $d$-th root of unity. $\Phi_d(\alpha,\beta)$ is an integer for $d$ larger than 2 and so, by (5), primitive divisors of a Lucas or Lehmer number $u_n$ must divide $\Phi_n(\alpha,\beta)$.

In 1913 Carmichael [18] showed that if $u_n$ is a Lucas number with $\alpha,\beta$ real and $n$ larger than 12 then $u_n$ possesses a primitive divisor. In 1955 Ward [87] proved the analogous result for Lehmer numbers, see also [21]. This dealt only with the case when $\alpha$ and $\beta$ are real numbers. Schinzel, in [64], [67], overcame this hurdle. He proved that there is an effectively computable positive number $c_0$ such that if $n$ exceeds $c_0$ then the $n$-th term of a Lucas or Lehmer sequence possesses a primitive divisor. In [75] we modified an argument of Baker [5] to give an, at the time, sharp estimate from below for a linear in two logarithms of the form

$$b_1 \log(-1) + b_2 \log \alpha \ ,$$

where $\alpha$ is an algebraic number and $b_1$ and $b_2$ are rational integers. We used this estimate to show that one could take $c_0 = e^{452}4^{67}$. More significantly however, we were able to prove that there are only finitely many Lehmer sequences whose $n$-th term, $n > 6, n \neq 8, 10$ or 12, does not possess a primitive divisor and that these sequences may be explicitly determined. For Lucas sequences the restriction $n > 6, n \neq 8, 10$ or 12 may be replaced by $n > 4, n \neq 6$. The restrictions on $n$ cannot be weakened and so the problem of determining all exceptional Lucas and Lehmer numbers, (those without a primitive divisor and $n$ outside of the forbidden ranges), is solved in principle. However in practice much work needs to be done still since we reduced the problem to one of solving a finite, but large, number of Thue equations. Paul Voutier, a former Master's student of mine at the University of Waterloo, determined in his thesis all exceptional numbers $u_n$ with $n$ at most 30 and he conjectured that there are no exceptional numbers $u_n$ with $n$ larger than 30, [85]. Furthermore by making use of recent work of Laurent, Mignotte and Nesterenko [42] on estimates for linear forms in two logarithms he has shown [86] that one can take $c_0 = 30,030$.

# 4 Recurrence sequences

Let $r$ and $s$ be integers with $r^2 + 4s$ non-zero. Let $u_0$ and $u_1$ be integers and put

$$u_n = ru_{n-1} + su_{n-2} \ , \tag{6}$$

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

$$u_n = a\alpha^n + b\beta^n \ , \tag{7}$$

where $\alpha$ and $\beta$ are the roots of $x^2 - rx - s$ and

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

whenever $\alpha \neq \beta$. The sequence of integers $(u_n)_{n=0}^{\infty}$ is a binary recurrence sequence and it is said to be non-degenerate if $ab\alpha\beta \neq 0$ and $\alpha/\beta$ is not a root of unity. Observe that if $u_0 = 0$ and $u_1 = 1$ and $r$ and $s$ are coprime we have a Lucas sequence.

In 1934, Mahler [49] used a $p$-adic version of the Thue-Siegel theorem to prove that if $(u_n)_{n=1}^{\infty}$ is a non-degenerate binary recurrence sequence then

$$P(u_n) \to \infty \quad \text{as } n \to \infty \ .$$

In 1967, Schinzel was able to give an effective version of Mahler's result by means of Gelfond's estimates for linear forms in two logarithms of algebraic numbers. Let $d$ be the degree of $\alpha$ over the rationals. He proved [66] that

$$P(u_n) > c_1 n^{\theta_1} (\log n)^{\theta_2} \ ,$$

where $c_1$ is a positive number which is effectively computable in terms of $a, b, \alpha$ and $\beta$ and where $\theta_1 = 1/84$ and $\theta_2 = 7/12$ if $d$ is 1 and $\theta_1 = 1/133$ and $\theta_2 = 7/19$ if $d$ is 2. In 1982 we proved [78], using estimates for linear forms in logarithms due in the complex case to Baker [4] and in the $p$-adic case to van der Poorten [58], that

$$P(u_n) > c_2 (n/\log n)^{1/(d+1)} \ , \tag{8}$$

where $c_2$ is a positive number which is effectively computable in terms of $a$ and $b$ only. In [78] we were also able to give non-trivial effective lower bounds for the greatest prime factor of the $n$-th term of a general linear recurrence provided that one of the roots of the characteristic polynomial of the recurrence was larger in absolute value than the rest.

With Tarlok Shorey [69] we studied occurrences of squares, cubes and higher powers in binary recurrence sequences. We proved the following result.

**Theorem 2.** *Let $h$ be a non-zero integer and let $u_n$, as in (7), be the $n$-th term of a non-degenerate binary recurrence sequence. If*

$$hx^q = u_n \ ,$$

*for integers $x$ and $q$ larger than one, then the maximum of $x, q$ and $n$ is less than $c_3$, a number which is effectively computable in terms of $a, \alpha, b, \beta$ and $h$.*

Since $|u_n| \to \infty$ as $n \to \infty$ whenever $(u_n)_{n=0}^{\infty}$ is a non-degenerate binary recurrence sequence, we see that $u_n$ is a pure power for only finitely many integers $n$. Independently Petho [56] proved a similar result to Theorem 2. He assumed, in addition to the hypotheses of Theorem 2, that $r$ and $s$ in (6) are coprime and then showed that the maximum of $x, q$ and $n$ is less than a number which is effectively computable in terms of $a, \alpha, b, \beta$ and the greatest prime factor of $h$.

# 5 Lehmer's question

Let $f(x) = a_r x^r + a_{r-1}x^{r-1} + \cdots + a_0$ be a polynomial with integer coefficients of degree $r(\geq 1)$. We define $M(f)$, the Mahler measure of the polynomial $f$, to be

$$M(f) = |a_r| \prod_{i=1}^{r} \max(1, |\alpha_i|) \ ,$$

where $\alpha_1, \ldots, \alpha_r$ are the roots of $f$. Equivalently, we have, by Jensen's theorem,

$$M(f) = \exp \int_0^1 \log |f(e^{2\pi i t})| \ dt \ .$$

For any algebraic number $\alpha$ we define $M(\alpha)$ to be equal to $M(f)$ where $f$ is the minimal polynomial of $\alpha$. Observe that $M(f_1 f_2) = M(f_1)M(f_2)$ and that $M(\alpha\beta) \leq M(\alpha)M(\beta)$ for any algebraic numbers $\alpha$ and $\beta$. .

It is easy to see that if $\alpha$ is a non-zero algebraic number which is not a unit then $M(\alpha) \geq 2$ and that if $\alpha$ is a root of unity then $M(\alpha) = 1$. In 1857, Kronecker [39] proved that if $\alpha$ is a non-zero algebraic number with $M(\alpha) = 1$ then $\alpha$ is a root of unity. In 1933 D.H. Lehmer [44] asked whether for each positive number $\epsilon$ there exists a polynomial $f$ with integer coefficients for which $1 < M(f) < 1 + \epsilon$. A negative answer to Lehmer's question would give a substantial improvement on Kronecker's theorem and Lehmer did some searching to find polynomials with small measure larger than one. The smallest example he found was $M(f_0) = 1.17628081...$ where

$$f_0(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1 \ ,$$

and more extensive searches by Boyd [16] and others have failed to turn up any smaller examples.

Lehmer's question has turned up in a variety of settings, [17], [76]. For instance a negative answer would resolve the question of whether the Salem numbers are dense in $[1, \infty)$. Recall that a Salem number is a real algebraic integer larger than 1 having one conjugate on the unit circle and all other conjugates, apart from itself, on or inside the unit circle. Further, Lind [45] has shown that the set of possible values for the entropy of a continuous algebraic automorphism of a separable compact group can be described subject to the answer to Lehmer's question.

In 1971 Blanksby and Montgomery [12] took a big step towards resolving Lehmer's question. They proved, by means of Fourier analysis, that if $f$ is a polynomial with integer coefficients and degree $r$ and

$$M(f) < 1 + (52r \log 6r)^{-1} \tag{9}$$

then $M(f) = 1$. I spent the academic year 1976-77 at the Mathematisch Centrum in Amsterdam after completing my Ph.D. and during that time I found a new method of approaching Lehmer's question based on an idea from transcendental number theory; although I didn't write up my result [77] until the following academic year which I spent at I.H.E.S. . The idea was to construct an exponential polynomial related to $f$ with many zeros and small integer

coefficients by means of Siegel's lemma and then to extrapolate to produce more zeros and, ultimately, a contradiction. This led to a result of comparable strength to that of Blanksby and Montgomery but with a smaller constant; in (9) 52 was replaced by $10^4$. Dobrowolski [20] took up this approach and introduced a lovely idea which allowed him to prove that there exists a positive number $c_4$ such that if $\alpha$ is a non-zero algebraic number of degree $r(> 2)$, and

$$M(\alpha) < 1 + c_4 \left( \frac{\log\log r}{\log r} \right)^3 ,$$

then $\alpha$ is a root of unity and this is the most precise result known.

The transcendence theory approach has proved to be useful in related settings. For instance, Anderson, Masser and others have used it to investigate the elliptic and abelian analogues of Lehmer's question [1], [52].

# 6 The *abc* conjecture

For any positive integers $x, y$ and $z$ define $G = G(x, y, z)$ by

$$G = \prod_{\substack{p \mid xyx \\ p \text{ a prime}}} p .$$

Suppose now that $(x, y, z) = 1$ and $x + y = z$. Oesterlé, motivated by the theory of elliptic curves, conjectured that there exists a positive constant $c_5$ such that

$$z < G^{c_5} .$$

Masser, in 1985, refined this conjecture by analogy with a result of Mason [51] in the function field case. He conjectured that for any positive real number $\epsilon$ there exists a positive number $c_6(\epsilon)$, depending on $\epsilon$, such that

$$z < c_6(\epsilon) G^{1+\epsilon} . \tag{10}$$

This last conjecture is known as the *abc* conjecture. The conjecture is significant because it links the additive and multiplicative properties of the integers and it has a multitude of important consequences. It is perhaps surprising that such a simple and beautiful conjecture was not made years earlier.

It is not obvious, a priori, that any bound for $z$ in terms of $G$ should exist. With Tijdeman [81] we proved that such a bound does exist, indeed that there exists an effectively computable positive number $c_7$ such that

$$z < \exp(c_7 G^{15}) .$$

In 1991 we refined this result with Yu [83] by proving that for each positive number $\epsilon$ there is a positive number $c_8(\epsilon)$ which is effectively computable in terms of $\epsilon$, for which

$$z < c_8(\epsilon) \exp(G^{2/3+\epsilon}) .$$

On taking $x = 1$ , $y = 2^n$ and $z = 1 + 2^n$ for $n = 1, 2, \ldots$ we see that $z \geq G/2$ for infinitely may triples $(x, y, z)$ of coprime positive integers. Thus the exponent of $G$ on the right hand side of inequality (10) must be at least 1. Could we replace the term $G^\epsilon$ by a power of $\log G$? The answer is no and this is a consequence of the next result which we obtained with Tijdeman [81].

**Theorem 3.** *Let $\delta > 0$. There exist infinitely many triples $(x, y, z)$ of coprime positive integers with $x + y = z$ for which*

$$z > G \exp\left((4 - \delta)\frac{\sqrt{\log G}}{\log\log G}\right) .$$

# 7 The arithmetical character of sumsets

For any set $X$ let $|X|$ denote its cardinality. Let $N$ be a positive integer and let $A$ and $B$ be subsets of $\{1, \ldots, N\}$. What can one say about the arithmetical character of sums $a+b$ with $a$ in $A$ and $b$ in $B$? It turns out that if $A$ and $B$ are sufficiently dense subsets of $\{1, \ldots, N\}$ then many of the arithmetical properties of the sumset $A + B$ are similar to those of the set of consecutive integers $\{1, \ldots, 2N\}$. When $A$ and $B$ are less dense this analogy breaks down but some structure is still present.

For any positive integer $n$ let $\omega(n)$ denote the number of distinct prime factors of $n$. In 1934 Erdös and Turán [27] proved that if $|A| = k$ then, for $k \geq 2$,

$$\omega\left(\prod_{a,a' \epsilon A} (a + a')\right) > c_9 \log k ,$$

where $c_9$ is an effectively computable positive number. They conjectured that a similar result should hold when we replace sums $a + a'$ by sums $a + b$ from sets $A$ and $B$ respectively. We resolved this with György and Tijdeman [36] in 1986 when we used a result of Evertse [28] on $S$-unit equations to prove that if $|A| = k$ and $|B| = l$ with $k \geq l \geq 2$ then

$$\omega\left(\prod_{a \epsilon A, b \epsilon B} (a + b)\right) > c_{10} \log k . \tag{11}$$

Thus, by the prime number theorem, there exists an $a$ in $A$ and a $b$ in $B$ for which

$$P(a + b) > c_{11} \log k \log\log k ; \tag{12}$$

here $c_{10}$ and $c_{11}$ are effectively computable positive numbers. With Erdös and Tijdeman [26] we showed that, when $l = 2$, (11) and (12) are not far from best possible. In particular the right hand sides of the inequalities cannot be replaced by $(\frac{1}{8} + \epsilon)(\log k)^2 \log\log k$ and $(\frac{1}{4} + \epsilon)(\log k \log\log k)^2$ respectively for any positive real number $\epsilon$.

For the above results we have not required the sets $A$ and $B$ to be dense subsets of $\{1, \ldots, N\}$. For thin sets the techniques applied to extract information come from combinatorial number theory and Diophantine approximation. For dense sets different methods

are called for and they usually come from the province of analytic number theory. András Sárközy visited me at the University of Waterloo in 1983. Since then we have kept up an active collaboration studying problems of the latter type, sometimes together with Paul Erdös and Carl Pomerance [24], [57]. Let me mention a few such results. We shall adapt Vinogradov's notation $>>$ for brevity. Thus $|A| >> N$ means there is a positive constant $c$, which is independent of $N$, such that $|A| > cN$. If $c$ depends on a parameter $k$ we write $|A| >>_k N$. The first problem we consider is the following. If $A$ and $B$ are dense subsets of $\{1, \dots, N\}$ can we find a sum $a + b$ which is divisible by a large prime or by a power of a large prime? In 1984 Balog and Sárközy [8] used the large sieve inequality to prove that if $|A| >> N$ and $|B| >> N$ then there exist an $a$ in $A$ and a $b$ in $B$ such that

$$P(a + b) >> N/\log N \ .$$

In 1986, Sárközy and I used the Hardy-Littlewood circle method to sharpen the above conclusion [61]. We proved that

$$P(a + b) >> N \ ,$$

for $>> N^2/\log N$ pairs $(a, b)$ with $a$ in $A$ and $b$ in $B$. In 1988 we extended this method to treat the case of large prime powers [62]. Let $k$ be a positive integer. If $|A| >> N$ and $|B| >> N$ then there exist $>>_k N^{1+1/k}/\log N$ pairs $(a, b)$ for which $a + b$ is divisible by $p^k$ where $p$ is a prime and $p^k >>_k N$. The result is sharp, up to determination of constants, with respect to the lower bounds for $p^k$ and the number of pairs $(a, b)$. It is worth noting that, unlike the case $k = 1$ where we have (12), if $k \geq 2$ then there is no analogue of this result for thin sets.

The second problem I wish to discuss in this context is that of finding sums $a+b$ for which $\omega(a+b)$ is large. By means of an argument of a combinatorial nature involving the repeated application of the large sieve inequality, Sárközy and I were able to prove the following result [63].

**Theorem 4.** *Let $\theta$ be a real number with $\frac{1}{2} < \theta \leq 1$ and let $N$ be a positive integer. There exists a positive number $c_{12}$, which is effectively computable in terms of $\theta$, such that if $A$ and $B$ are subsets of $\{1, \dots, N\}$ with $N$ greater than $c_{12}$ and*

$$(|A||B|)^{1/2} \geq N^{\theta} \ ,$$

*then there exists an integer $a$ from $A$ and an integer $b$ from $B$ for which*

$$\omega(a + b) > \frac{1}{6}\left(\theta - \frac{1}{2}\right)^2 (\log N)/\log\log N \ . \tag{13}$$

By the prime number theorem the maximum of $\omega(n)$ in $\{1, \dots, 2N\}$ is $(1+o(1))\log N/\log\log N$ and so, up to the dependence on $\theta$, estimate (13) is optimal.

# 8 $S$-unit equations

Let $K$ be an algebraic number field of degree $d$ over $\mathbb{Q}$. Let $M_K$ be the set of places (equivalence classes of multiplicative valuations) on $K$. Let $S$ be a finite set of places of $K$ containing

all infinite places. An algebraic number $\alpha$ from $K$ is said to be an $S$-unit if $|\alpha|_v = 1$ for every valuation $|\ |_v$ from a place $v \epsilon M_K \backslash S$. The $S$-units form a group. Let $\alpha_1, \alpha_2$ and $\alpha_3$ be non-zero elements of $K$ and consider the $S$-unit equation

$$\alpha_1 x + \alpha_2 y = \alpha_3 \ , \tag{14}$$

in $S$-units $x$ and $y$. The study of many Diophantine equations can be reduced to the study of $S$-unit equations, see [6], [41] and [71] and see [30] for other applications. Lang [40] proved that (14) has only finitely many solutions. Denote this number by $\nu_S(\alpha_1, \alpha_2, \alpha_3)$ and let $s$ denote the cardinality of $S$. In 1984, Evertse [28] proved that

$$\nu_S(\alpha_1, \alpha_2, \alpha_3) \leq 3 \cdot 7^{d+2s} \tag{15}$$

for every $(\alpha_1, \alpha_2, \alpha_3) \epsilon (K^*)^3$. With Erdös and Tijdeman [26] we showed that estimate (15) cannot be improved much in general. On the other hand, with Evertse, György and Tijdeman [29] we showed that most $S$-unit equations have few solutions.

Let us first discuss the latter result. We call two triples $(\alpha_1, \alpha_2, \alpha_3)$ and $(\beta_1, \beta_2, \beta_3)$ in $(K^*)^3$ $S$-equivalent if there exists a permutation $\sigma$ of $(1, 2, 3)$, a $\lambda$ in $K^*$ and $S$-units $\epsilon_1, \epsilon_2$ and $\epsilon_3$ such that

$$\beta_i = \lambda \epsilon_i \alpha_{\sigma(i)} \quad \text{for } i = 1, 2, 3 \ .$$

Plainly if $(\alpha_1, \alpha_2, \alpha_3)$ and $(\beta_1, \beta_2, \beta_3)$ are $S$-equivalent then $\nu_S(\alpha_1, \alpha_2, \alpha_3) = \nu_S(\beta_1, \beta_2, \beta_3)$. In 1988 we proved with Evertse, György and Tijdeman [29] the following result.

**Theorem 5.** *Let $S$ be a finite subset of $M_K$ containing all infinite places. Then there exists a finite set $A$ of triples in $(K^*)^3$ such that for each triple $(\alpha_1, \alpha_2, \alpha_3) \epsilon (K^*)^3$ which is not $S$-equivalent to a triple from $A$,*

$$\nu_S(\alpha_1, \alpha_2, \alpha_3) \leq 2 \ . \tag{16}$$

The quantity 2 on the right hand side of inequality (16) cannot be replaced by 1. The proof of Theorem 5 depends, ultimately, on a $p$-adic version of Schmidt's Subspace Theorem.

While Theorem 5 shows that most $S$-unit equations have few solutions the next result, which we obtained with Erdös and Tijdeman [26], shows that even when $K = \mathbb{Q}$ there are $S$-unit equations with many solutions.

**Theorem 6.** *Let $\epsilon$ be a positive real number. There exists a number $c_{13}$, which is effectively computable in terms of $\epsilon$, such that if $s$ exceeds $c_{13}$ then there exists a set $S$ of prime numbers with $|S| = s$ for which the equation*

$$x + y = z \ ,$$

*has at least $\exp((4-\epsilon)(s/\log s)^{1/2})$ solutions in coprime positive integers composed of primes from $S$.*

For the proof we use a combinatorial argument in conjunction with estimates for $\psi(x, y)$, the function which counts the number of positive integers up to $x$ all of whose prime factors are at most $y$. My two coauthors on this paper were a big help to me when I was starting my career. The second paper I wrote was a joint one with Paul Erdös [25] and he kept in touch

afterwards with a steady stream of letters. Further, Robert Tijdeman arranged to bring me to the Mathematisch Centrum in Amsterdam for my first job in the year after I obtained my Ph.D. .

Theorem 6 and the techniques used to prove it allowed us to show the existence of Thue-Mahler equations and Ramanujan-Nagell equations with very many solutions [26], [53]. In addition it has been used by Zagier [88] in his study of linear relations between values of polylogarithms.

# 9 Thue equations

In 1844, Liouville [46] proved that if $\alpha$ is an algebraic number of degree $r > 1$, then there exists a positive real number $c_{14}(\alpha)$ which is effectively computable in terms of $\alpha$, such that for all rational numbers $p/q$ with $q > 0$,

$$\left|\alpha - \frac{p}{q}\right| > \frac{c_{14}(\alpha)}{q^r} \ . \tag{17}$$

In 1955 Roth [59], building on earlier work of Thue [84] and Siegel [72], was able to show that, for each positive number $\epsilon$, estimate (17) holds with $r$ replaced by $2 + \epsilon$ and $c_{14}(\alpha)$ replaced by $c_{15}(\alpha, \epsilon)$. The work of Thue, Siegel and Roth was ineffective, however, since given $\alpha$ and $\epsilon$ their proofs did not give a method for determining $c_{15}(\alpha, \epsilon)$. The first explicit improvement on the Liouville exponent of $r$ for an algebraic number of degree $r > 2$ was obtained by Baker [2] in 1964 by means of the hypergeometric method. For instance, he proved that for all rationals $p/q$ with $q > 0$ we have

$$\left|\alpha - \frac{p}{q}\right| > \frac{c_{16}}{q^\kappa} \ , \tag{18}$$

with $\alpha = \sqrt[3]{2}$ , $c_{16} = 10^{-6}$ and $\kappa = 2.955$. This was refined by Chudnovsky [19] in 1983. David Easton, my first Ph.D. student, made some of the work of Chudnovsky explicit [22] in 1986 and in 1994 Michael Bennett [10], as a postdoctoral fellow at Waterloo, showed that one could take $\alpha = \sqrt[3]{2}$ , $c_{16} = 1/4$ and $\kappa = 2.5$ in (18).

The hypergeometric method gives many striking improvements on Liouville's theorem but it does not apply to all algebraic numbers $\alpha$. The first general effective improvement is due to Baker [3] and it follows from his estimates for linear forms in the logarithms of algebraic numbers. This was subsequently refined by Feldman [31] and made explicit by Györy and Papp [35]. Bombieri [13], [14] has recently found an effective approach based on the Thue-Siegel method.

I spend the first half of 1985 on sabbatical at Institut des Hautes Études Scientifique and during this period Alan Baker, my Ph.D. supervisor, was also a visitor. We decided to tailor the linear forms in logarithms arguments in order to yield improvements to Liouville's result. We chose to focus on the case when $\alpha$ is the cube root of an integer and we completed our work [7] during a visit by Baker to Waterloo later that year.

**Theorem 7.** *Let $\alpha$ be a positive integer which is not a perfect cube and let $\alpha = \sqrt[3]{a}$. Further let $\epsilon(> 1)$ be the fundamental unit in the field $\mathbb{Q}(\sqrt[3]{a})$. Then (18) holds for all rational numbers $p/q$ , $q > 0$ with $c_{16} = 1/(3ac_{17})$ and $\kappa = 3 - 1/c_{18}$, where*

$$c_{17} = \epsilon^{(50 \log\log \epsilon)^2} \ , \ c_{18} = 10^{12} \log \epsilon \ . \tag{19}$$

An immediate consequence of Theorem 7 is that if $a$ and $h$ are positive integers with $a$ not a perfect cube then all solutions in integers $x$ and $y$ of the Diophantine equation

$$x^3 - ay^3 = h \ , \tag{20}$$

satisfy

$$\max(|x|, |y|) < (c_{17}h)^{c_{18}} \ .$$

Equation (20) is an example of a Thue equation. Let $F(x, y) = a_r x^r + a_{r-1}x^{r-1}y + \cdots + a_0 y^r$ be a binary form with integer coefficients, content 1, discriminant $D$ and with $r \geq 3$. Let $h$ be a non-zero integer. The equation

$$F(x, y) = h \ , \tag{21}$$

is known as the Thue equation; in 1909 Thue proved that if $F$ is irreducible over $\mathbb{Q}$ then (21) has only finitely many solutions. A solution of (21) with $x$ and $y$ coprime is said to be a primitive solution. In 1933, Mahler [48] proved that if $F$ is irreducible then (21) has at most $c_{19}^{1+\omega(h)}$ primitive solutions, where $c_{19}$ is effectively computable in terms of $F$. In 1984, Evertse [28] solved a conjecture of Siegel by proving that if $D \neq 0$ then (21) has at most

$$2 \cdot 7^{r^3(2\omega(h)+3)}$$

primitive solutions. In 1987, Bombieri and Schmidt [15] refined this result by showing that if $F$ is irreducible then (21) has at most $c_{20}r^{1+\omega(h)}$ primitive solutions where $c_{20}$ is a positive number which can be taken to be 430 for $r$ sufficiently large. Four years later [80] we showed, by appealing to Theorem 5, that if $D \neq 0$ then (21) has at most $4r^{\omega(h)}$ primitive solutions for $h$ sufficiently large. Also, following an approach initiated by Erdös and Mahler [23] in 1938, we showed that if the discriminant of $F$ is non-zero and $h$ is divisible by a large integer composed of few prime factors then we could improve the above estimates.

**Theorem 8.** *Let $F$ be a binary form with integer coefficients of degree $r(\geq 3)$, content 1 and non-zero discriminant $D$. Let $h$ be a non-zero integer and let $\epsilon$ be a positive real number. Let $g$ be any divisor of $h$ with $g \geq |h|^{2/r+\epsilon}$. If $|h| \geq (D, g^2)^{1/\epsilon}$ then the number of primitive solutions of (21) is at most*

$$2800\left(1 + \frac{1}{4\epsilon r}\right) r^{1+\omega(g)} \ .$$

# 10 Elliptic curves

Let $E$ be an elliptic curve over $\mathbb{Q}$. It has a Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b$ in $\mathbb{Q}$ and $4a^3 + 27b^2 \neq 0$. The set of rational points on $E$ together with the point at $\infty$ can be

endowed with a group structure in a natural way by means of the chord and tangent process. The group is abelian and it consists of a finite torsion subgroup and a subgroup isomorphic to the direct product of $r$ copies of $\mathbb{Z}$; $r$ is known as the rank of $E$. How does the rank vary as we run over twists of a given elliptic curve $E$? That is, we restrict our attention to families of elliptic curves defined over $\mathbb{Q}$ which are isomorphic over $\mathbb{C}$. There are families of quadratic, cubic, quartic and sextic twists.

Let $d$ be a non-zero integer and let $E_d$ denote the quadratic twist of $E$ given by the equation $dy^2 = x^3 + ax + b$. Let $r(d)$ denote the rank of $E_d$. Note that if $d_1$ and $d_2$ are non-zero integers then $E_{d_1}$ is isomorphic to $E_{d_2}$ over $\mathbb{Q}$ if and only if $d_1/d_2$ is the square of a rational number. Goldfeld [32] conjectured that the average value for $r(d)$ is $1/2$ and this corresponds to computational evidence. Can we show that there are in fact quite a few curves of rank at least 2? The first theoretical results in this context were obtained by Gouvêa and Mazur [33] in 1991. Let $\epsilon > 0$. Under the assumption of the Parity Conjecture, they proved that there are positive numbers $c_{21}$ and $c_{22}$, which depend on $\epsilon$ and $E$, such that for any positive integer $T$ larger that $c_{21}$ the number of square-free integers $d$ with $|d| \leq T$ for which the rank of $E_d$ is at least 2 is at least $c_{22}T^{1/2-\epsilon}$. Mai [50] extended this work to cubic twists of $x^3 + y^3 = 1$.

Jaap Top and I started to work together in this area while Jaap held a postdoctoral position in Queen's University in 1990. I was fortunate to have a Killam Research Fellowship during this period. We managed to avoid the use of the Parity Conjecture and give unconditional analogues of the above results. For instance we proved [82] that there is a positive number $c_{23}$ such that if $T$ exceeds 657 then the number of cube-free integers $d$ with $|d| \leq T$ for which the curve given by $x^3 + y^3 = d$ has rank at least 3 is at least $c_{23}T^{1/6}$. Further let $E$ be the elliptic curve with equation $y^3 = x^3 + ax + b$ with $ab \neq 0$. There are positive numbers $c_{24}$ and $c_{25}$, which depend on $E$, such that if $T$ exceeds $c_{24}$ then the number of square-free integers $d$ with $|d| \leq T$ for which the rank of $dy^2 = x^3 + ax + b$ is at least 2 is at least $c_{25}T^{1/7}/(\log T)^2$.

Let $k$ be an integer with $k \geq 2$. An integer is said to be $k$-free if it is not divisible by the $k$-th power of a prime. Let $F$ be a binary form with integer coefficients, non-zero discriminant and degree $r$ with $r \geq 3$. Let $R_k(x)$ denote the number of $k$-free integers $t$ with $|t| \leq x$ for which there exist integers $a$ and $b$ with $F(a, b) = t$. For our estimates on the ranks of twists of elliptic curves we required information on the function $R_k(x)$. Suppose that there is no fixed $k$-th power larger than 1 which divides $F(a, b)$ for all $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Let $m$ be the largest degree of an irreducible factor of $F$ over $\mathbb{Q}$ and suppose that $m \leq 2k+1$ or that $k = 2$ and $m = 6$. With Top [82], we proved that there are positive numbers $c_{26}$ and $c_{27}$, which depend on $k$ and $F$, such that if $x$ is a real number larger than $c_{26}$ then

$$R_k(x) > c_{27}x^{2/r}.$$

This estimate is best possible up to the determination of $c_{27}$. For the proof we appealed to a sieve theoretical result of Greaves [34], which built on work of Gouvêa and Mazur [33] and also Hooley [37], and to Theorem 8.

# References


[1] M. Anderson and D. W. Masser, *Lower bounds for heights on elliptic curves*, Math. Z. **174** (1980), 23–34.

[2] A. Baker, *Rational approximations to* $\sqrt[3]{2}$ *and other algebraic numbers*, Quart. J. Math. Oxford, **15** (1964), 375–383.

[3] _____, *Contributions to the theory of Diophantine equations I: On the representation of integers by binary forms*, Phil. Trans. Royal Soc. **A 263** (1968), 173–191.

[4] _____, *A sharpening of the bounds for linear forms in logarithms II*, Acta Arith. **24** (1973), 33–36.

[5] _____, The theory of linear forms in logarithms. Transcendence Theory: Advances and Applications, edited by A. Baker and D.W. Masser, Academic Press, 1977, 1–27.

[6] _____, Transcendental Number Theory (2nd edition), Cambridge University Press, 1979.

[7] A. Baker and C.L. Stewart, On effective approximations to cubic irrationals, New Advances in Transcendence Theory, (A. Baker ed.), Cambridge University Press, 1988, 1–24.

[8] A. Balog and A. Sárközy , *On sums of sequences of integers, II*, Acta Math. Hung. **44** (1984), 169–179.

[9] A.S. Bang, *Taltheoretiske undersogelser*, Tidsskrift for Mat. (5) **4** (1886), 70–80. 130–137.

[10] M.A. Bennett, *Effective measures of irrationality for certain algebraic numbers*, to appear.

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

[12] P.E. Blanksby and H.L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith. **28** (1971), 355–369.

[13] E. Bombieri, *On the Thue-Siegel-Dyson theorem*, Acta Math. **148** (1982), 255–296.

[14] _____, *Effective Diophantine approximation on* $G_m$, Ann. Scuola Norm. Sup. Pisa. Cl. Sci., **20** (1993), 61–89.

[15] E. Bombieri and W.M. Schmidt, *On Thue's equation*, Invent. Math **88** (1987), 69–81.

[16] D.W. Boyd, *Reciprocal polynomials having small measure*, Math. Comp., **35** (1980), 1361–1377.

[17] _____, *Speculations concerning the range of Mahler's measure*, Canad. Math. Bull. **24** (1981), 453–469.

[18] R.D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. (2) **5** (1913), 30–70.

[19] G.V. Chudnovsky, *On the method of Thue-Siegel*, Ann. of Math. **117** (1983), 325–382.

[20] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta. Arith. **34** (1979), 391–401.

[21] L.K. Durst, *Exceptional real Lehmer sequences*, Pacific J. Math. **9** (1959), 437–441.

[22] D. Easton, *Effective irrationality measures for certain algebraic numbers*, Math. Comp. **46** (1986), 613–622.

[23] P. Erdös and K. Mahler, *On the number of integers which can be represented by a binary form*, J. London Math. Soc. **13** (1938), 134–139.

[24] P. Erdös, C. Pomerance, A. Sárközy and C.L. Stewart, *On elements of sumsets with many prime factors*, J. Number Theory, **44** (1993), 93–104.

[25] P. Erdös and C.L. Stewart, *On the greatest and least prime factors of* $n! + 1$, J. London Math. Soc., (2) **13** (1976), 513–519.

[26] P. Erdös, C.L. Stewart, and R. Tijdeman, *Some diophantine equations with many solutions*, Compositio Math. **66** (1988), 37–56.

[27] P. Erdös and P. Turán, *On a problem in the elementary theory of numbers*, Amer. Math. Monthly **41** (1934), 608–611.

[28] J.H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75** (1984), 561–584.

[29] J.H. Evertse, K. Győry, C.L. Stewart, and R.Tijdeman, *On S-unit equations in two unknowns*, Invent. Math. **92** (1988), 461-477.

[30] _____, *S-unit equations and their applications*, New Advances in Transcendence Theory, (A. Baker ed.), Cambridge University Press, 1988, 110-174.

[31] N.I. Feldman, *An effective refinement of the exponent in Liouville's theorem* (in Russian), Izv. Akad. Nauk. SSSR, **35** (1971), 973–990.

[32] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory (Proc. Conf. in Carbondale, 1979) (M. B. Nathanson, ed.), Lecture Notes in Math., vol. 751 Springer-Verlag, Berlin, New York and Heidelberg, 1979, pp. 108-118.

[33] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc., **4** (1991), 1-23.

[34] G. Greaves, *Power-free values of binary forms*, Quart. J. Math. Oxford Ser (2), **43** (1992), 45-65.

[35] K. Győry and Z.Z. Papp, *Norm form equations and explicit lower bounds for linear forms with algebraic coefficients*, Studies in Pure Mathematics (to the memory of P. Turán) (Budapest, 1983), 245–257.

[36] K. Győry, C.L. Stewart and R. Tijdeman, *On prime factors of sums of integers I*, Compositio Math. **59** (1986), 81–88.

[37] C. Hooley, *On power-free values of polynomials*, Mathematika, **14** (1967), 21-26.

[38] M.N. Huxley, *A note on polynomial congruences*, Recent Progress in Analytic Number Theory, Vol. 1 (H. Halberstam and C. Hooley, eds.), Academic Press, London, 1981, pp. 193–196.

[39] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. reine angew. Math. **53** (1857), 173–175.

[40] S. Lang *Integral points on curves*, Inst. Hautes Études Sci. Publ. Math. **6** (1960), 27–43.

[41] _____, *Eliptic Curves Diophantine Analysis*, Grund. math. Wiss. **231**, Springer-Verlag, Berlin, 1978.

[42] M. Laurent, M. Mignotte et Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory **55** (1995), 285–321.

[43] D.H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2) **31** (1930), 419–448.

[44] _____, *Factorization of certain cyclotomic functions*, Ann. of Math. **(2) 34** (1933), 461–479.

[45] D.A. Lind, *Skew products with group automorphisms*, Israel J. Math. **28** (1977), 205–248.

[46] J. Liouville, *Sur des classes très–étendues de quantités dont la valeur n'est ni algébrique, ni même reductible à des irrationelles algébrique*, Comptes rendus de l'Acad. Sci. (Paris) **18** (1844), 883–885.

[47] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.

[48] K. Mahler, *Zur Approximation algebraischer Zahlen. II. Uber die Anzahl der Darstellungen ganzer Zahlen durch Binärformen*, Math. Ann. **108** (1933), 37–55.

[49] _____, *Eine arithmetische Eigenschaft der rekurrierenden Reihen*, Mathematica (Leiden) **3** (1934-35), 153–156.

[50] L. Mai, *The analytic rank of a family of elliptic curves*, Can. J. Math. **45** (1993), 847-862.

[51] R.C. Mason, *Diophantine equations over function fields*, London Math. Soc. Lecture Notes 96, Cambridge University Press, (1984).

[52] D.W. Masser, *Small values of the quadratic part of the Néron-Tate height on an abelian variety*, Compositio Math. **53** (1984), 153–170.

[53] P. Moree and C.L. Stewart, *Some Ramanujan-Nagell equations with many solutions*, Nederl. Akad. Wetensch. Proc. Ser. A. (N.S.) **1** (1990), 465–472.

[54] T. Nagell, *Généralisation d'un théorème de Tchebicheff*, J. Math. **8** (1921), 343–356.

[55] Ö. Ore, *Anzahl der Wurzeln höherer Kongruenzen*, Norsk Matematisk Tidsskrift, 3 Aagang, Kristiana (1921), 343–356.

[56] A. Petho, *Perfect powers in second order linear recurrences*, J. Number Theory **15** (1982), 5–13.

[57] C. Pomerance, A. Sárközy and C.L. Stewart, *On divisors of sums of integers, III*, Pacific J. Math. **133** (1988), 363–379.

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

[59] K.F. Roth, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 1–20.

[60] G. Sándor, *Uber die Anzahl der Lösungen einer Kongruenz*, Acta. Math. **87** (1952), 13–17.

[61] A. Sárközy and C.L. Stewart, *On divisors of sums of integers, II*, J. reine angew Math. **365** (1986), 171–191.

[62] _____, *On divisors of sums of integers, IV*, Can. J. Math. **50** (1988), 788–816.

[63] _____, *On divisors of sums of integers, V*, Pacific J. Math. **166** (1994), 373–384.

[64] A.Schinzel, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ark. Mat. **4** (1962), 413–416.

[65] _____, *On primitive prime factors of $a^n - b^n$*, Proc. Camb. Phil. Soc. **58** (1962), 555–562.

[66] _____, *On two theorems of Gelfond and some of their applications*, Acta Arith. **13** (1967), 177–236.

[67] _____, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. reine angew. Math. **268/269** (1974), 27–33.

[68] W.M. Schmidt and C.L. Stewart, *Congruences, trees and p-adic integers*, Transactions of the A.M.S., to appear.

[69] T.N. Shorey and C.L. Stewart, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers II*, J. London Math. Soc. (2) **23** (1981), 17–23.

[70] ———, *On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences*, Math. Scand. **52** (1983), 24–36.

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

[72] C.L. Siegel, *Approximation algebraischer Zahlen*, Math. Z. **10** (1921), 173–213.

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

[74] ———, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers*, Proc. London Math. Soc. (3) **35** (1977), 425–447.

[75] ———, *Primitive divisors of Lucas and Lehmer numbers*, Transcendence theory: advances and applications, A. Baker and D.W. Masser ed., London and New York 1977.

[76] ———, *On a theorem of Kronecker and a related question of Lehmer*, Sém. Théorie des Nombres (Bordeaux) (1978), 7:01–7:11.

[77] ———, *Algebraic integers whose conjugates lie near the unit circle*, Bull. Soc. Math. France **106** (1978), 169–176.

[78] ———, *On divisors of terms of linear recurrence sequences*, J. reine angew. Math. **333** (1982), 12–31.

[79] ———, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers III*, J. London Math. Soc. (2) **28** (1983), 211–217.

[80] ———, *On the number of solutions of polynomial congruences and Thue equations*, J. Amer. Math. Soc., **4** (1991), 793-835.

[81] C.L. Stewart and R. Tijdeman, *On the Oesterlé-Masser conjecture*, Monastshefte Math. **102** (1986), 251–257.

[82] C.L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms,* J. Amer. Math. Soc., **8** (1995), 943-973.

[83] C.L. Stewart and Kunrui Yu, *On the abc conjecture*, Math. Annalen, **29** (1991), 225–230.

[84] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. reine angew. Math. **35** (1909), 284–305.

[85] P.M. Voutier, *Primitive divisors of Lucas and Lehmer sequences*, Math. Comp. **64** (1995), 869–888.

[86] ———, *Primitive divisors of Lucas and Lehmer sequences III*, to appear.

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

[88] D. Zagier, *Polylogarithms, Dedekind zeta functions and the algebraic K-theory of fields, Arithmetic algebraic geometry* (Texel, 1989), 391–430, Progress in Math. 89, Birkhauser Boston 1991.

[89] K. Zsigmondy, *Zur Theorie der Potenzreste*, Montash. Math. **3** (1892), 265–284.

Department of Pure Mathematics
The University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
email: cstewart@watserv1.uwaterloo.ca