Simultaneous Pellian equations

R G E Pinch
Department of Pure Mathematics and Mathematical Statistics
University of Cambridge

31 May 1989

0. Introduction

In this paper we describe a method for finding integer solutions of simultaneous Pellian equations, that is, integer triples (x, y, z) satisfying equations of the form

$$(x+f)^2 - ay^2 = b \qquad (0.1$$

$$(x-f)^2 - cz^2 = d$$

where the coefficients a, b, c, d, f are integers and we assume that a, c and ac are not square.

The pair of solutions represents an intersection of two quadric surfaces in three-dimensional affine space, which is in general a curve of genus one. The number of integral points on such a curve is finite by results of Thue [20] and Siegel [18], and an effective bound for the solutions was obtained by Baker [1] (see also [2]) by the method of estimating linear forms in logarithms. The bounds obtained by Baker are very large (typically $10^{10^{100}}$), and have often been said to be beyond the range of practical computation. But in fact, Baker and Davenport [4] used such a bound to obtain the complete set of solutions to the pair of equations $3x^2 - 2 = y^2$, $8x^2 - 7 = z^2$ using techniques of Diophantine approximation. Their method required calculations of logarithms of certain algebraic numbers to some 600 decimal places. The number of decimal places required increases linearly with the logarithmic height h of the units in the quadratic fields involved, so that the running time would be at least quadratic in h and hence can be expected to increase significantly with the magnitude of the coefficients involved. Further, multi-length computation to many hundreds of decimal places involves special programming and is not generally available on most computers.

In this paper we describe a method for dealing with the computational aspect of solving these equations which avoids calculation to high accuracy, and which has a running time expected to be approximately linear in h; it is well adapted to practical computation. It is derived from a technique of Grinstead [8] who applied it to the problem of finding numbers which are simultaneously square, triangular and centred hexagonal; Brown [7] applied it to the problem of finding sets of integers all of whose products in pairs differ by a prescribed amount from a square; and Petho [15] applied a similar technique to the problem of finding Fibonnaci numbers which are perfect powers. The first two applications lead directly to simultaneous Pellian equations. Some related problems are considered in the survey of Zagier [22].

It should be noted that the method is used to verify that a set of previously obtained solutions is indeed complete. If there is a further solution, the method will usually give enough information to find it. By contrast, the Baker/ Davenport method almost certainly produces the complete list of solutions.

In Section 4 we apply the method to the solution of equations which arise in the tabulation of elliptic curves of 2-power conductor over $\mathrm{Q}(\sqrt{5})$ [16].

1 Recurrent sequences

The sets of solutions (x, y), (x, z) to each equation individually are well known from the theory of quadratic fields: see, for example, Nagell [14] Chapter 6. The solutions in general form either a finite set, or a finite union of binary recurrent sequences, according as the quadratic field in question is imaginary or real. If either a or c is negative, the corresponding equation has only finitely many solutions and these can be obtained by standard techniques. We suppose, therefore, that a, c are both positive, and that ϵ, η are the fundamental totally positive units of the fields $Q(\sqrt{a})$, $Q(\sqrt{c})$ respectively (normalised to be greater than 1). Let α' denote the conjugate of α in a quadratic field. The solutions to the equations (0.1) fall into a finite set of families

$$x + f + y\sqrt{a} = \beta\epsilon^m, \tag{1.1}$$

$$x - f + z\sqrt{c} = \delta\eta^n, \tag{1.2}$$

according to the solutions of the equations $\beta\beta' = b$ and $\delta\delta' = d$ up to units. We may suppose that β, δ are normalised so that $\beta \geq |\beta'|$, $\delta \geq |\delta'|$, $\beta\epsilon^{-1} \leq |\beta'|\epsilon$, $\delta\eta^{-1} \leq |\delta'|\eta$: that is, the solutions of (1.1) with $x + f$, y positive are just those with $m \geq 0$, and those of (1.2) with $x - f$, z positive are just those with $n \geq 0$.

In (1.1) the values $(x + f)_m$, y_m satisfy a binary recurrence relation

$$X_{m+1} = sX_m - X_{m-1}$$

whose auxiliary polynomial $X^2 - sX + 1$ is just the minimal polynomial for ϵ, and a similar relation holds for $(x - f)_n$, z_n. The problem can thus be rephrased as finding those values of two recurrent sequences (X_m), (X'_n) which differ by $2f$. We first find bounds for the magnitude of such values.

2. Bounds for the magnitude of the solutions

We observe that from (1.1) we have

$$2(x + f) = \beta\epsilon^n + \beta'\epsilon^{-n}.$$

so that if m, n are both large then the ratio of $\beta\epsilon^n$ to $\delta\eta^m$ is close to 1. Taking logarithms, the linear form

$$\Lambda = n \log \epsilon - m \log \eta + \log \frac{\beta}{\delta}$$

is close to, but not equal to, zero. We can therefore employ a lower bound for such a linear form to derive upper bounds for m, n. The bound used by Baker and Davenport in [4] is given by Theorem 2.1.

Let α be an algebraic number of degree d with conjugates $\alpha_(1) = \alpha, \alpha_(2), ..., \alpha_(d)$ and minimal equation $a_d X^d + ... + a_0$ over Z: that is, the a_i are coprime integers. The "usual" *height* of α is

$$H(\alpha) = \max\{|a_i|\}$$

and the *measure* of α is

$$M(\alpha) = a_d \prod_1^d \max\{1, \left|\alpha_(i)\right|\}.$$

Let K be a number field of degree n over Q with α in K; let ν run over the set V_K of valuations of K, normalised to satisfy the product formula, and let n_ν denote the local degree of ν. The *absolute logarithmic height* of α is

$$h(\alpha) = \frac{1}{n} \sum_{V_K} \log \max\{1, |\alpha|_\nu^{n_\nu}\}$$

$$= \frac{1}{d} \log M(\alpha).$$

The following result is due to Baker [3] .

Theorem 1 *Suppose $k \geq 2$ and that $\alpha_1, ..., \alpha_k$ are non-zero algebraic numbers of degree at most d, and height $H(\alpha_i)$ at most A, where $d \geq 4$, $A \geq 4$. If there are rational integers $b_1, ..., b_n$ such that*

$$0 < b_1 \log \alpha_1 + ... + b_k \log \alpha_k < \exp(-\lambda H)$$

where $0 < \lambda \leq 1$ and $\max\{|b_1|, ..., |b_k|\} \leq H$, then

$$H < (4^{k^2} \lambda^{-1} d^{2k} \log A)^{(2k+1)^2}.$$

This Theorem was used by Baker/ Davenport [4] and Grinstead [8] . We shall use a somewhat stronger result of Waldschmidt [21].

Theorem 2 *Let K be a number field of degree D, $\beta_0, ..., \beta_n$ and $\alpha_1, ..., \alpha_n$ in K. Put*

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + ... + \beta_n \log \alpha_n.$$

Let $V_1, ..., V_n, W, E$ be positive real numbers satisfying

$$\frac{1}{D} \leq V_1 \leq ... \leq V_n,$$

$$V_j \geq \max\left\{h(\alpha_j), \frac{|\log \alpha_j|}{D}\right\},$$

$$W \geq \max\{h(\beta_j)\}$$

and

$$1 < E < \min\left\{e^{DV_1}, \frac{4DV_j}{|\log \alpha_j|}\right\}.$$

Define $V_j^+ = \max\{1, V_j\}$.

If $\Lambda \neq 0$ then

$$|\Lambda| > \exp\left(-C(n) D^{n+2} V_1 ... V_n (W + \log(EDV_n^+))(\log(EDV_{n-1}^+))(\log E)^{-n-1}\right),$$

where $C(1) = 2^3 5$, $C(2) = 2^5 3$, $C(3) = 2^7 1$ and $C(n) \leq 2^{8n+51} n^{2n}$.

Lemma 3 *Suppose that p, q, r are positive with $r > q > p$. If*

$$pX < q \log X + r$$

then

$$X < \frac{r}{p}\left(1 + \frac{q \log(r/p)}{r - q}\right).$$

Let $f(X) = pX - q \log X - r$. Then $f'(X) = p - qX^{-1}$ and $f''(X) = qX^{-2}$. We have $f(X) -> \infty$ as $X -> 0$ and as $X -> \infty$; since $f'' > 0$, the graph of f is concave upwards. At $X = \frac{q}{p}$, $f(X) = q - r - q\frac{\log q}{p} < 0$ and $f'(X) = 0$, so there are two zeroes, between which f is negative. The point $X = \frac{r}{p}$, $Y = -q\frac{\log r}{p}$ is to the right of this minimum, since $r > q$, and the graph of f to the right of $\frac{r}{p}$ lies above the tangent, which has slope

$f'\left(\frac{r}{p}\right) = \frac{p}{r}(r-q)$. So the greater zero lies to the left of the intersection of this tangent with the X-axis, at the point

$$X = \frac{r}{p} + \left(\frac{q\log r}{p}\right)\frac{r}{p(r-q)}$$

$$= \frac{r}{p}\left(1 + \frac{q\log(r/p)}{r-q}\right).$$

Theorem 4 *Suppose $k \geq 2$ and that $\alpha_1, \ldots, \alpha_n$ are non-zero elements of a number field K of degree $D \geq 3$. Let $V_1, \ldots, V_n$, V_{n-1}^+, V_n^+, E, $C(n)$ be defined as in Theorem 2.2. Further define*

$$F = -C(n)D^{n+2}V_1 \ldots V_n(\log EDV_{n-1}^+)(\log E)^{-n-1},$$

$$G = \log EDV_n^+.$$

If there are rational integers $b_1, \ldots, b_n$ such that

$$0 < |b_1\alpha_1 + \ldots + b_n\alpha_n| < \exp(-\lambda H)$$

where $0 < \lambda < F$ and $H = \max\{|b_1|, \ldots, |b_n|\}$, then

$$H < \frac{FG}{\lambda}\left(1 + \frac{\log(FG/\lambda)}{G-1}\right).$$

Apply Theorem 2.2 with

$$W = \max\{h(b_i)\} = \max\log|b_i| = \log H.$$

Then we have

$$\exp(-F(G + \log H)) < |\Lambda| < \exp(-\lambda H).$$

Put $p = \lambda$, $q = F$ and $r = FG$. We have $p < q$ by assumption; since E, ${V_n}^+ \geq 1$ and $D \geq 3$, we have $G \geq \log(3) > 1$ and so $r > q$. We can now apply Lemma 2.3 and the Theorem follows immediately.

The bound in the Theorem increases with increasing F or G, and hence with increasing V_j.

We omit the simple proof of the next result.

Lemma 5 *Let $0 < |\alpha| < \frac{1}{2}$. Then*

$$|\log(1-\alpha)| < |\alpha| + \alpha^2.$$

We can now prove an estimate for the magnitude of the solutions to (0.1).

Theorem 6 *Suppose m, n furnish a solution to*

$$x + f + y\sqrt{a} = \beta\epsilon^m$$

$$x - f + z\sqrt{c} = \delta\eta^n$$

with β, δ normalised as in Section 1, and $x \pm f$, y, z positive. Assume $\epsilon < \eta$. Let μ be a real number with $0 < \mu < 1$ and put $\lambda = 2(1-\mu)\log\epsilon$ if $f = 0$ and $\lambda = (1-\mu)\log\epsilon$ if $f \neq 0$.

Then $max\{m,n\} \leq \max\{B,C,D\}$, where

$$B = \frac{FG}{\lambda}\left(1 + \frac{\log(FG/\lambda)}{G-1}\right),$$

$$C = \frac{\log 10(5|f| + 2|b| + \frac{19}{9}|d| + 1)}{\mu \log \epsilon},$$

$$D = \frac{4A + (4|f| + |\beta'| + |\delta'|)/\delta}{\log \eta/\epsilon}$$

$$F = 2^7 7A^3 \log 16A(\log 2)^{-4},$$

$$G = \log 16A$$

and

$$A = \max\{h(\epsilon), h(\eta), h(\beta/\delta)\}.$$

The condition on $x \pm f$, y, z implies that $m, n \geq 0$. Assume, that one of m, n exceeds both C and D. We shall show that this implies $B > m > n$.

Let $P = \beta\epsilon^m$, $Q = \delta\eta^n$, so that

$$2(x+f) = P + b/P,$$

$$2(x-f) = Q + d/Q.$$

Define auxiliary quantities

$$L = |b| + \frac{10}{9}|d|,$$

$$M = 4|f| + |\beta'| + |\delta'|,$$

$$N = |\beta'| + |\delta'| + L + 1,$$

$$E = \frac{\log(10M/\beta)}{\log \epsilon}.$$

We have $|\beta'| \leq \sqrt{|b|} \leq |b|$, $|\delta'| \leq \sqrt{|d|} \leq |d|$ and $\beta \geq \sqrt{|b|} \geq 1$, so that $E < C$.

We shall estimate the linear form

$$\Lambda = \left|\log \frac{P}{Q}\right| = \left|m \log \epsilon - n \log \eta + \log \frac{\beta}{\delta}\right|.$$

We proceed by showing that $\max\{m,n\} > D$ implies that $m > n$; that $m > E$ implies $|P - Q| < 4|f| + L/P$; that $m > C$ implies $\Lambda < \exp(-\lambda m)$; and finally we apply Theorem 2.4 to show that $B > m$.

Now

$$|b/P| = |\beta' \epsilon^{-m}| \leq |\beta'|,$$

$$|d/Q| = |\delta' \eta^{-n}| \leq |\delta'|,$$

since $m, n \geq 0$. Hence

$$P - Q = 4f - b/P + d/Q$$

$$|P - Q| \leq 4|f| + |\beta'| + |\delta'| = M.$$

We claim that $m > n$. Suppose not: then $m \leq n$ and so $n > D$. Now $A \geq h(\beta/\delta) \geq \frac{1}{4}\log(\beta/\delta)$, so

$$n > D \geq \frac{M/\delta + \log \beta/\delta}{\log \eta/\epsilon}.$$

Now

$$n \log \eta/\epsilon - \log \beta/\delta > M/\delta \geq M/(\delta\eta^n) = M/Q,$$

so

$$\log \frac{P}{Q} \geq \frac{\log \delta\eta^n}{\beta\epsilon^n} > \frac{M}{Q},$$

since $m \leq n$. Hence

$$\frac{P}{Q} > \exp \frac{M}{Q} > 1 + \frac{M}{Q}$$

and so $P > Q + M$. But $|P - Q| \leq M$, a contradiction. Hence $m > n$.

We now have $max\{m, n\} = m$, so that $m > E$. So

$$P = \beta\epsilon^m > \beta \exp(E \log \epsilon) = 10M.$$

Since $P \neq Q$, $0 < |P - Q| < M$ and $Q > \frac{9}{10}P$. Now

$$|P - Q| = \left|4f - \frac{b}{P} + \frac{d}{Q}\right| < 4|f| + \frac{|b|}{P} + \frac{10|d|}{9P}$$

$$< 4|f| + \frac{L}{P}.$$

We defined

$$\Lambda = \left|\log \frac{P}{Q}\right| = \left|m \log \epsilon - n \log \eta + \log\left(\frac{\beta}{\delta}\right)\right|;$$

we shall show that $\Lambda < \exp(-\lambda m)$. We have

$$0 < \Lambda = \left|\log\left(1 - \frac{P - Q}{P}\right)\right| < \left|\frac{P - Q}{P}\right| + \left(\frac{P - Q}{P}\right)^2$$

by Lemma 2.5. There are two cases, depending on whether $f = 0$.

Suppose first that $f = 0$, so that $\lambda = 2(1 - \mu)\log \epsilon$, and put

$$C_1 = \frac{\log((L + 1)/\beta^2)}{2\mu \log \epsilon}.$$

Since $(L + 1) \leq (L + 1)^2$, we have $C_1 \leq C$ and so $m > C_1$. Now $|P - Q| < L/P$ so

$$\Lambda < LP^{-2} + L^2P^{-4}$$

$$< P^{-2}(L + (L/P)^2)$$

$$< P^{-2}(L + 1)$$

since $P > 10L > L$. Now

$$\Lambda < \frac{L + 1}{\beta^2}\epsilon^{-2m}$$

and, since $C_1 < m$,

$$\log \frac{L + 1}{\beta^2} < \mu m \log \epsilon^2$$

so

$$\log \Lambda < (\mu - 1) m \log \epsilon^2 = -\lambda m,$$

as required.

Now suppose that $f \neq 0$, so that $\lambda = (1-\mu)\log \epsilon$, and put

$$C_2 = \frac{\log 6|f|/\beta}{\mu \log \epsilon}.$$

Clearly $C_2 \leq C$, and so $C_2 < m$. Now $|P - Q| < 4|f| + L/P$ and $P > 10L$; so that $L/P < \frac{1}{10} < |f|$, and hence $|P - Q| < 5|f|$. Now

$$\Lambda < \frac{5|f|}{P} + \left(\frac{5|f|}{P}\right)^2$$

$$< \frac{6|f|}{P},$$

since $P > 10M > 5|f|$. But $C_2 < m$, so

$$\log \frac{6|f|}{\beta} < \mu m \log \epsilon$$

and

$$\log \Lambda < (\mu - 1) m \log \epsilon = -\lambda m,$$

as required.

So in each case $\Lambda < e^{-\lambda m}$. We may now apply Theorem 2.4. Put $\alpha_1 = \epsilon$, $\alpha_2 = \eta$, $\alpha_3 = \frac{\beta}{\delta}$; $b_0 = 0$, $b_1 = m$, $b_2 = -n$, $b_3 = 1$.

Since ϵ is a unit with $\epsilon > 1 > \epsilon' > 0$, we have $M(\epsilon) = \log \epsilon$ and $h(\epsilon) = \frac{1}{2}\log\epsilon$; similarly $h(\eta) = \frac{1}{2}\log \eta$. The field $\mathbb{Q}(\sqrt{a}, \sqrt{c})$ contains ϵ, η, and $\frac{\beta}{\delta}$ and has degree $D = 4$. Put

$$V_1 = \frac{1}{2}\log \epsilon,$$

$$V_2 = \frac{1}{2}\log \eta,$$

$$V_3 = \max\left\{V_2, \frac{1}{4}|\log \beta/\delta|\right\}.$$

Since $\frac{3+\sqrt{5}}{2} \leq \epsilon < \eta$ and $\frac{1}{4} < \frac{1}{2}\log\left(\frac{3+\sqrt{5}}{2}\right)$, we have $\frac{1}{D} < V_1 < V_2 \leq V_3 \leq A$. We claim that putting $E = 4$ satisfies the conditions of Theorem 2.4. We have

$$\exp(DV_1) = \epsilon^2 \geq \left(\frac{3+\sqrt{5}}{2}\right)^2 > 4.$$

For $j = 1$ or 2,

$$\frac{4DV_j}{|\log \alpha_j|} = 8,$$

and for $j = 3$,

$$V_3 \geq \frac{|\log \beta/\delta|}{4},$$

so

$$\frac{4DV_3}{|\log \alpha_3|} \geq 4.$$

The constants of Theorem 2.4 are now

$$F_0 = C(3)4^5 V_1 V_2 V_3 (\log 16V_2)(\log 4)^{-4},$$

$$G_0 = \log 16V_3$$

and since $F_0 \leq F$, $G_0 \leq G$, the Theorem follows.

The parameter μ is at our disposal in applying the Theorem. Clearly taking μ small increases λ and hence will improve the bound B at the expense of C.

The terms C and D cannot both be eliminated from the Theorem, since B is independent of f. However, in the applications below, we find that the dominant contribution to the bound is the term B. If we used Theorem 2.1, then we could take instead

$$\tilde{B} = 2^1 470 \tilde{\lambda}^- 49 (\log \tilde{A})^4 9,$$

where $\tilde{A}$ is the maximum of the "usual" heights of ϵ, η, $\frac{\beta}{\delta}$ and $\tilde{\lambda} = \min\{\lambda, 1\}$.

3. Common values of recurrent sequences

The discussion of the previous section shows that we may solve a pair of simultaneous Pellian equations by solving equations of the form $X_n - Y_m = g$, where g is a constant and (X_n), (Y_m) are recurrent sequences satisfying *unital* binary recurrence relations, that is, of the form

$$X_{n+1} = sX_n - X_{n-1}$$

so that the roots of the auxiliary equation are quadratic units of norm 1. In general, the common values of two such sequences form a finite set together with a finite union of arithmetic progressions (with respect to the indexing variables m, n), and will form a finite set if the roots of the two auxiliary equations lie in distinct quadratic fields. It is the latter case that we are interested in.

The set of values taken by a recurrent sequence is discussed by Kiss [9] and Mignotte [11], [12] and [13]; the multiplicities of such values are discussed by Beukers [5] and Loxton/van der Poorten [10] There is a survey in the recent tract of Shorey and Tijdeman [17]

Suppose then that we wish to solve the equation

$$X_n = Y_m + g \tag{3.1}$$

where (X_n), (Y_m) are given by

$$X_{n+1} = sX_n - X_{n-1},$$

$$Y_{m+1} = tY_m - Y_{m-1},$$

together with prescribed initial values X_0, X_1, Y_0, Y_1, and that neither of the discriminants $s^2 - 4$, $t^2 - 4$ nor their ratio is a square. Suppose further that we already have a list of solutions which we wish to prove complete.

By replacing the sequences (X), (Y) by subsequences, and translating the starting point of m or n, we may replace (3.1) by a finite list of similar equations for each of which we wish to prove that the only solution is $X_0 = Y_0 + g$, and we assume that the problem is in this form.

From Section 2, we have a bound B such that any solution to (3.1) must satisfy $|m|, |n| < B$. We can deduce that $m = n = 0$ is the only solution if we can find integer moduli M, N, with $M, N > B$, such that $X_n = Y_m + g$ implies $M|m, N|n$. We describe a method for finding such M, N. We need to find a set of primes p with associated exponents e such that (3.1) implies $p^e|m$, and a similar set for n. To obtain M we perform step P for a suitable set of primes p.

Step P

Input

Moduli M, N for which (3.1) implies $M|m, N|n$; a prime p.

Output

Moduli M, Np, or M, N for which (3.1) implies $M|m, N|n$.

Procedure

Suppose that p^{e-1} already divides N. Form a set S of possible values for $m \bmod p^e$: initially S will consist of the p multiples of p^{e-1}. Form a set Q of primes q such that the sequence $(X_n) \bmod q$ has a cycle length exactly divisible by p^e. Perform Step Q for each q in Q until S is reduced to the single element 0, in which case return moduli Mp, N, or else fail, in which case return M,N.

Step Q

Input

A prime q such that $(X_n) \bmod q$ has cycle length exactly divisible by p^e; a set S of values modp^e such that (3.1) implies that $n \bmod p^e$ is in S.

Output

A modified set $S' \subset S$ such that (3.1) implies that $n \bmod p^e$ is in S'.

Procedure

Let the cycle lengths of $(X), (Y) \bmod q$ be ell_X, ell_Y respectively, and let h_X be $\gcd(N, ell_X)$, h_Y be $\gcd(M, ell_Y)$. Let V be the set of values $Y_m + g \bmod q$ for m between 1 and ell_Y with m divisible by h_Y. Let S' initially be the set $\{0\}$. For n from 1 to ell_X with n divisible by h_X and $n \bmod p^e$ in S, add $n \bmod p^e$ to S' if $X_n \bmod q$ is in V. Return S'.

Algorithm 7 *Input*

Two unital recurrent sequences (X_n), (Y_m), an integer g such that $X_0 = Y_0 + g$.

Output

Integers M, N such that $X_n = Y_m + g$ implies M divides m, N divides n.

Procedure:

Let P$'$, Q$'$ denote steps P and Q with the roles of X, Y interchanged. Take a list L of primes to use as candidates for the modulus q of step Q and compute the cycle lengths ell_X , ell_Y of X, Y modulo (q) for every prime in L. Take a list K of primes to use as the possible factors p of M and N. Set M and N initally to 1. Repeat the following steps R and R$'$ until no more primes can be added to M and N.
R) For each prime p in K, and for each power e of p, perform step P for p^e using the primes of L to form the set Q, taking the next prime from K when step P fails.
R') Proceed as step R with X, Y interchanged.
Output M, N.

It may happen that there is more than one solution to the equation (3.1). In this case, step Q will never reduce the set S of possible values to $\{0\}$, and step P will always fail. However, examination of the possible values in S will give information about the congruence classes of the further solutions (m, n) modulo p for the p in K and it should then be possible to use the Chinese Remainder Theorem and the bound of Theorem 2.6 to find the further solutions exactly. These can then be added to the known list and the process repeated with appropriate subsequences of the X and Y.

It will not be possible to carry out Step Q in order to add a prime p from K to the modulus N unless there is a prime q in L with the corresponding cycle length ell_X divisible by p. For given p, it is not clear that there exists any such q. The existence of such q for sufficiently large p is guaranteed by Theorem 1 of Stewart [19], although it should be noted that the lower bound for p in our applications would be of the order 10^266. However Theorem 2 (ibid.) shows that there are only finitely many sequences for which this lower bound cannot be taken to be 13. In this context it would be interesting to know how many p will not divide the cycle lengths of a recurrent sequence. Some related results are referred to in chapter 3 of Shorey and Tijdeman [17].

The Algorithm was implemented on an IBM 3081 computer at the Cambridge University Computer Laboratory, programmed in Algol-68C (see Bourne, Birrell and Walker [6]). For the applications of Section 4, where in each case the bound B satisfies $\log B < 63$, we found it sufficient to let the list K be the first 100 primes (to 541) and the list L be the primes to 153. At least one fifth of the applications of Step P were successful in increasing the modulus and the average number of applications of Step Q in each such successful application of Step P was less than 2. Each of the four runs took less than 17 seconds of CPU time, a total of less than one minute.

We also applied the Algorithm in one case to obtain a modulus greater than the bound $\tilde{B}$ which would be given by Theorem 2.1 rather than Theorem 2.2. In this case $\log \tilde{B} < 1083$ and we found it sufficient to let the list K be the first 1700 primes (to 14519) and the list L be the primes to 2135. The run took less than 35 minutes of CPU time.

4. Applications

In this section we apply the method described in Section 3 to the solution of simlultaneous Pellian equations which arise in finding the elliptic curves over $Q(\sqrt{5})$ with good reduction away from 2 [16].

Proposition 8 *The simultaneous Pellian equations*

$$(X + 2)^2 - 2Y^2 = -1$$

$$(X - 2)^2 - 10Z^2 = -1$$

have only the solutions $X = -1, Y = \pm 1, Z = \pm 1$ *and* $X = -5, Y = \pm 2, Z = \pm 5$.

Proof:

The field $Q(\sqrt{2})$ has class-number 1, fundamental unit $1 + \sqrt{2}$, so put $\epsilon = 3 + 2\sqrt{2}$: $Q(\sqrt{10})$ has class-number 2, fundamental unit $3 + \sqrt{10}$, so put $\eta = 19 + 6\sqrt{10}$. We have

$$X + 2 + Y\sqrt{2} = \pm(1 + \sqrt{2})\epsilon^m,$$

$$X - 2 + Z\sqrt{10} = \pm(3 + \sqrt{10})\eta^n.$$

Applying Theorem 2.6 with $\mu = 10^{-6}$, we have (correct to the figures given) $A = 1.818$, $\log B = 62.060$, $C = 909678$, $D = 0.243$, $\log F = 58.161$ and $G = 3.371$. Hence $|m|, |n| < B$ where $\log B < 62.07$.

If we put

$$A_{m+1} = 6A_m - A_{m-1}, A_0 = 1, A_1 = 7,$$

$$B_{n+1} = 38B_n - B_{n-1}, B_0 = 3, B_1 = 117,$$

then $X + 2 = \pm A_m$, $X - 2 = \pm B_n$, and so we need to solve the equations $A_m = B_n \pm 4$. Since $A_{-m} = -A_m$, and $B_{-n} = -B_n$, it suffices to solve $A_m = B_n + 4$. Inspection reveals the solutions $A_0 = 1$, $B_{-1} = -3$ and $A_1 = 7$, $B_0 = 3$: we claim that these are the only solutions.

We replace (B_n) by the two subsequences given by

$$B_{n+1} = 1442B_n - B_{n-1}$$

with initial values $B_0 = -3$, $B_1 = 117$ and $B_0 = 3$, $B_1 = 4443$ respectively.

For the subsequence with $B_0 = -3$, we claim that $A_0 = B_0 + 4$ is the only solution. Applying Algorithm 3.1 to a list of 100 primes, we obtain moduli M, N with $\log M > 70.69$ and $\log N > 69.58$, both of which are greater than $\log B$, so that there are no further solutions by Theorem 2.6.

For the subsequence with $B_0 = 3$, we change m so that $A_0 = 7$, $A_1 = 41$ and claim that $A_0 = B_0 + 4$ is the only solution. We similarly obtain M, N with $\log M > 67.65$, $\log N > 69.58$ and again there are no further solutions by Theorem 2.6.

Proposition 9 *The simultaneous Pellian equations*

$$X^2 - 2Y^2 = -1$$

$$X^2 - 10Z^2 = -9$$

have only the solutions $X = \pm 1$, $Y = \pm 1$, $Z = \pm 1$; $X = \pm 41$, $Y = \pm 29$, $Z = \pm 13$.

Proof:

As before, we take $\epsilon = 3 + 2\sqrt{2}$, $\eta = 19 + 6\sqrt{10}$. We have

$$X + Y\sqrt{2} = \pm(1 + \sqrt{2})\epsilon^m,$$

$$X + Z\sqrt{10} = \pm\delta\eta^n,$$

where δ runs over a set of non-associate and non-conjugate integers of norm -9. The prime 3 splits in $Q(\sqrt{10})$, since 10 is a residue $\bmod (3)$, and $(3) = (3, 1 + \sqrt{10})(3, 1 - \sqrt{10})$.

The prime ideal factors are not principal, since ± 3 are not residues mod(5), but their squares are principal on $1 \pm \sqrt{10}$ respectively. So we may take δ to be either $3(3+\sqrt{10})$ or $1+\sqrt{10}$. But taking $\delta = 9 + 3\sqrt{10}$ does not lead to a solution of our equations, for in this case 3 would divide X, and the first equation would give 2 as a quadratic residue of 3. So we have $\beta = 1 + \sqrt{2}$ and $\delta = 1 + \sqrt{10}$.

Applying Theorem 2.6 with $\mu = 10^{-6}$ we have $|m|, |n| < B$ where $\log B < 61.36$. The other bounds of the Theorem are $C < 204900$ and $D < 0.041$. If we put

$$A_{m+1} = 6A_m - A_{m-1}, A_0 = 1, A_1 = 7,$$

$$B_{n+1} = 38B_n - B_{n-1}, B_0 = 1, B_1 = 79,$$

then $X = \pm A_m = \pm B_n$, and so we need to solve the equations $A_m = \pm B_n$. Since $A_{-m} = -A_{m-1}$, it suffices to solve $A_m = B_n$. Inspection reveals the solutions $A_0 = B_0 = 1$ and $A_{-2} = B_{-1} = -41$: we claim that these are the only solutions.

We replace (B_n) by the two subsequences given by

$$B_{n+1} = 1442B_n - B_{n-1}$$

with initial values $B_0 = 1$, $B_1 = 3003$ and $B_0 = -41$, $B_1 = 79$ respectively.

For the subsequence with $B_0 = 1$, we claim that $A_0 = B_0$ is the only solution. Applying Algorithm 3.1 to a list of 100 primes, we obtain moduli M, N with $\log M > 70.69$ and $\log N > 68.88$, both of which are greater than $\log B$, so that there are no further solutions by Theorem 2.6.

For the subsequence with $B_0 = -41$, we change m so that $A_0 = -41$, $A_1 = -7$ and claim that $A_0 = B_0$ is the only solution. We similarly obtain M, N with $\log M > 67.00$, $\log N > 65.50$ and again there are no further solutions by Theorem 2.6.

Acknowledgements

I am grateful to Professor A. Baker for helpful discussions on the subject of this paper, to the referee for his comments on a previous version and to the Cambridge University Computing Service for the provision of computer facilities.

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika **15** (1968), 204–216.

[2] ______, *Transcendental number theory*, Cambridge University Press, 1975.

[3] ______, *The theory of linear forms in logarithms*, Transcendence theory: Advances and applications (London) (A. Baker and D.W. Masser, eds.), Academic Press, 1977.

[4] A. Baker and H. Davenport, *On the equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford (2) **20** (1969), 129–137.

[5] F. Beukers, *The multiplicity of binary sequences*, Compositio Math. **40** (1980), 251–267.

[6] S.R Bourne, A.D. Birrell, and I. Walker, *Algol68c reference manual*, Cambridge University Computer Laboratory, 1975.

[7] E. Brown, *Sets in which $xy + k$ is always a square*, Math. Comp. **45** (1985), 613–620.

[8] C.M. Grinstead, *On a method of solving a class of Diophantine equations*, Math. Comp. **32** (1978), 936–940.

[9] P. Kiss, *On common terms of linear recurrences*, Acta Math. Acad. Sci. Hungaricae **40** (1982), 119–123.

[10] J.H. Loxton and A.J. van der Poorten, *On the growth of recurrence sequences*, Math. Proc. Cambridge Philos. Soc. **81** (1977), 369–376.

[11] M. Mignotte, *A note on linear recursive sequences*, J. Austral. Math. Soc. **20** (1975), 242–244.

[12] ______, *Intersection des images de certaines suites récurrentes linéaires*, Theoretical Computer Science **7** (1978), 117–122.

[13] ______, *Une extension du théorème de Skolem–Mahler*, C. R. Acad. Sci. Paris (A) **288** (1979), 233–235.

[14] T. Nagell, *Introduction to number theory*, Almqvist & Wiksell, Stockholm, 1951.

[15] A. Pethö, *Full cubes in the Fibonacci sequence*, Publ. Math. Debrecen **30** (1983), 117–127.

[16] R.G.E. Pinch, *Elliptic curves with good reduction away from 2: III*, Submitted.

[17] T.N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge tracts in mathematics, vol. 87, Cambridge University Press, 1986.

[18] C.L. Siegel, *Über einige anwendungen diophantischer approximationen*, Abh. Preuss. Akad. Wiss. (1929), no. 1.

[19] C.L. Stewart, *Primitive divisors of Lucas and Lehmer numbers*, Transcendence theory: Advances and applications (London) (A. Baker and D.W. Masser, eds.), Academic Press, 1977, pp. 79–92.

[20] A. Thue, *Über annäherungenswerte algebraischen zahlen*, J. reine angew. Math. **135** (1909), 284–305, = [14] no. 12, pp. 232–254.

[21] M. Waldschmidt, *A lower bound for linear forms in logarithms*, Acta Arithmetica **37** (1980), 257–283.

[22] D. Zagier, *Large integral points on elliptic curves*, Math. Comp. **48** (1987), no. 177, 425–436.