ACTA ARITHMETICA
151.3 (2012)

Diophantine equations of matching games II

by

Wai Yan Pong (Carson, CA)
and Roelof J. Stroeker (Krimpen aan den IJssel)

1. Introduction. Consider a game in which the player draws d balls from a bag of balls with n different colors. The player wins if the balls drawn are of the same color, otherwise he loses. We call this an (n,d)-*matching game* or briefly an (n,d)-*game*. A game is *fair* if the winning and losing chances for the player are equal. Let a_i be the number of ith color balls in the bag. It is easy to see that $(a_1,\dots,a_n)$ represents a fair (n,d)-game if it satisfies the following equation:

$$\binom{\sum_{i=1}^n x_i}{d} = 2\sum_{i=1}^n \binom{x_i}{d}. \tag{1.1}$$

Conversely, a solution $(a_1,\dots,a_n)$ of the equation above is a fair game if the a_i's are non-negative and their sum is at least d.

The quadratic case, i.e. $d=2$, of equation (1.1) has been solved in [HP11]. We believe that equation (1.1) is hard to solve in full generality. In this paper we will only deal with the "curve" case, i.e. $n=2$. But even with this restriction, we can only handle cases of degree at most 5. We use x,y instead of x_1,x_2 for the two variables and equation (1.1) becomes

$$\binom{x+y}{d} = 2\binom{x}{d} + 2\binom{y}{d}. \tag{1.2}$$

We shall completely solve the three cases $d \in \{3,4,5\}$, and although for a solution (x,y) of (1.2) to represent a fair $(2,d)$-game we require both x and y to be non-negative and $x+y \geq d$, it takes little extra effort to consider all integral values of x and y satisfying the diophantine equation (1.2). Therefore we need the binomial coefficient to be defined by

2010 *Mathematics Subject Classification*: Primary 11D09, 11D25; Secondary 11G05, 11Y50.
Key words and phrases: game of chance, diophantine equation, elliptic curve, elliptic logarithm.

DOI: 10.4064/aa151-3-6

$$\binom{x}{d} = \frac{x(x-1)\dots(x-d+1)}{d!}$$

for any rational integers x, y, and $d \geq 2$. As

$$\binom{2d}{d} = 2\binom{1}{d} + 2\binom{2d-1}{d}$$

for every $d \geq 2$, there is always a fair $(2,d)$-game; it is represented by the solution $(1, 2d-1)$ of equation (1.2). It turns out that there are infinitely many fair $(2,3)$-games; we give a full description in the next section. On the other hand, for $d = 4$ and $d = 5$, there are no other fair $(2,d)$-games than the one mentioned. A little search reveals that for $d = 6$ the number of fair $(2,d)$-games is at least two: $(1, 11)$ and $(2, 19)$ are the representatives. We suspect that there are no others, but we are unable to prove this. Our methods do not work for the cases $d \geq 6$.

2. The degree 3 case. In this section we completely solve equation (1.2) for $d = 3$; in particular, we will find all fair $(2,3)$-games.

Clearing denominators in (1.2) yields

$$s(s-1)(s-2) = 2x(x-1)(x-2) + 2y(y-1)(y-2), \tag{2.1}$$

where $s = x+y$. Observe that $x(x-1)(x-2) \equiv -y(y-1)(y-2)$ modulo $s-2$. In other words, $x + y - 2$ is a factor of both sides of equation (2.1). Note here that this is not only true in this special case, but something similar happens for all odd values of d. In fact, for d odd, the line $x + y = d - 1$ is a component of the variety defined by equation (1.2). Canceling $x + y - 2$ on both sides of (2.1) and rearranging terms yields

$$x^2 + y^2 - 4xy - x - y = 0. \tag{2.2}$$

First note that $xy \geq 0$ for all solutions $(x, y) \in \mathbb{Z}^2$ of equation (2.2). To be more precise, either $x \geq 0$ and $y \geq 0$, or $x < 0$ and $y < 0$. First consider the non-negative case. Suppose $b \geq 0$ is a coordinate of a fair $(2,3)$-game. Substituting b for y in equation (2.2) yields

$$x^2 - (4b+1)x + (b^2 - b) = 0. \tag{2.3}$$

Since b is a coordinate of a fair game, equation (2.3) must have another integer solution. In fact, it has two distinct integer solutions since $4b + 1$ is an odd integer. Let us call the solutions a and c. Since $ac = b^2 - b \geq 0$, a and c have the same sign, and since $a+c = 4b+1 > 0$, they are non-negative and cannot both be zero. Now $ac = b^2 - b \leq b^2$, so either a or c is at most b. Without loss of generality, suppose $a \leq b$. Then $c = 4b + 1 - a > b$. So we have $0 \leq a \leq b < c$ and the equalities hold if and only if $b = 0$. If $b > 0$, repeat the argument with b replaced by a until we get 0 as the smaller root of equation (2.3). When $b = 0$, the two roots of equation (2.3) are 0 and 1. Thus, from $c = 4b + 1 - a$ and $0 \leq a < b < c$ we conclude that

THEOREM 1. *The non-negative solutions of equation* (2.2) *are pairs of consecutive terms of the solution of the second-order recurrence*

$$n_{k+1} = 4n_k + 1 - n_{k-1}, \tag{2.4}$$

with the initial conditions $n_0 = n_1 = 0$. *The negative solutions of* (2.2) *are pairs of consecutive terms of the solution of the same recurrence* (2.4) *with the initial conditions* $n_0 = n_1 = -1$.

The negative case can be proven by an argument quite similar to the descent argument used above.

The general solution of recurrence (2.4) is

$$n_k = c_1\lambda_1^k + c_2\lambda_2^k - \tfrac{1}{2},$$

where $\lambda_1 = 2 + \sqrt{3}$ and $\lambda_2 = 2 - \sqrt{3}$ are the eigenvalues of the matrix $\left(\begin{smallmatrix} 4 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ associated with the second order difference equation (2.4), and c_1 and c_2 are constants depending on the initial values. In the non-negative case the constants are $c_1 = \frac{1}{12}(3-\sqrt{3})$, $c_2 = \frac{1}{12}(3+\sqrt{3})$, and in the negative case we have $c_1 = \frac{1}{12}(-3+\sqrt{3})$, $c_2 = \frac{1}{12}(-3-\sqrt{3})$. All this leads to the following results: the fair $(2,3)$-games are represented by the pairs (n_k, n_{k+1}) for $k \geq 2$, where $(n_k)_{k\geq 0}$ is the sequence

$$0, 0, 1, 5, 20, 76, 285, 1065, 3976, 14840, 55385, \ldots,$$

and the solution set $\{(x,y) \in \mathbb{Z}^2 \mid (x,y) \text{ satisfies (2.2) and } x \leq y\}$ consists of the trivial pairs $(0,0), (0,1)$, the pairs $(-n_{k+1}-1, -n_k - 1)$ for $k \geq 0$, and the fair $(2,3)$-games.

3. The degree 4 case. In this section we intend to prove the following

THEOREM 2. *The diophantine equation* (1.2) *with* $d = 4$ *and* $(x,y) \in \mathbb{Z}^2$ *has the twelve solutions*

$$(x,y) = (0,0), (0,1), (0,2), (0,3), (1,0), (1,1),$$
$$(1,2), (1,7), (2,0), (2,1), (3,0), (7,1)$$

and no others.

As a consequence, there is only one fair $(2,4)$-game, namely the one represented by $(1,7)$.

A quick search with the computer algebra package Maple14 reveals no other solutions (x,y) with $-1000 \leq x, y \leq 1000$. Other software packages we shall repeatedly use are SAGE 4.5.3 and PARI/gp 2.3.5. With the help of the Maple package **algcurves** we find that equation (1.2) with $d = 4$ represents a non-singular rational curve of genus 3. Therefore, by Faltings' theorem (see [Fa83]), there can only be finitely many rational solutions and thus also at most finitely many integral ones. What we need to do is find an upper bound for the size of these solutions. Unfortunately, no general method is

known for computing such an upper bound. We can however associate a rational curve E of genus 1 with (1.2), and for such curves a method does exists that may succeed in computing all rational integer solutions, namely Ellog (see [ST94], [ST03]). For general information we also refer to [Sm98, Chapter XIII].

Every integral solution of (1.2) with $d = 4$ maps to an integral solution of the associated curve E of genus 1 by

$$(x, y) \mapsto (xy, x + y).$$

Clearly, this means that the rational integral solutions of (1.2) can be recovered from those of the elliptic equation. We shall closely follow [ST03] and [Tz96] in presenting and combining the necessary calculations.

Putting $s = x + y$ and $p = xy$ into (1.2) with $d = 4$ yields

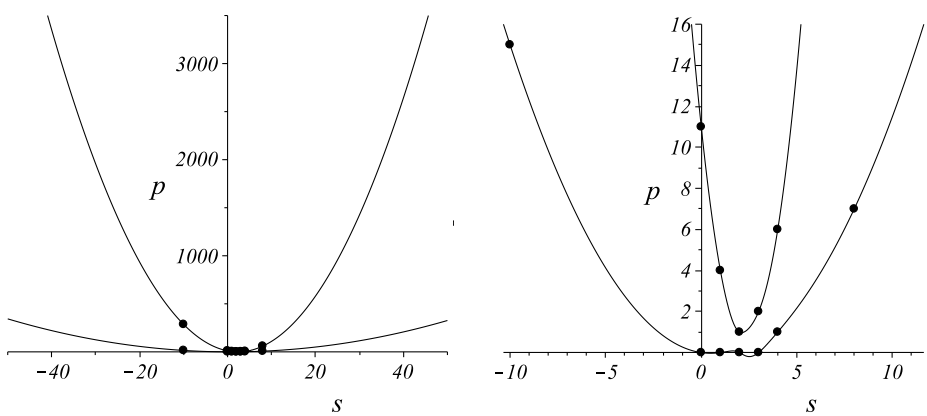
$$F = 0, \quad \text{with} \quad F = s(s-1)(s-2)(s-3) + 4p(-2s^2 + 9s + p - 11). \tag{3.1}$$

Another quick search shows that equation (3.1) has the 14 rational integral solutions

$$(s, p) = (-10, 15), (-10, 286), (0, 0), (0, 11), (1, 0), (1, 4), (2, 0), (2, 1), (3, 0), (3, 2), (4, 1), (4, 6), (8, 7), (8, 60)$$

and no others in the range $-1000 \le s, p \le 1000$. It is easily established that our work is done if it can be shown that (3.1) has no other rational integer solutions. Hence we may assume that $|s| > 1000$ for a solution $(s, p) \in \mathbb{Z}^2$ of (3.1). In order to get an idea in which parts of the (s, p)-plane large solutions of (3.1) may be expected, we look at the graph of the equation.

The visible integer solutions are shown in Figure 1. It appears that there are four infinite branches. We can check this by considering Puiseux series.



(a) Four infinite branches (b) Zoomed in near the origin

Fig. 1. Graphs of the non-singular curve (3.1) of genus 1

We find, again with the assistance of **algcurves**, that

$$p = \alpha s^2 + \left(\tfrac{1}{2} - 5\alpha\right)s - 1 + \tfrac{13}{2}\alpha + O(s^{-1}) \quad (s \to \pm\infty). \tag{3.2}$$

Here α is one of the roots of $4t^2 - 8t + 1 = 0$, that is, $\alpha = 1 \pm \frac{1}{2}\sqrt{3}$.

The curve represented by equation (3.1) is a non-singular curve E of genus 1 over $\mathbb{Q}$ with a distinguished point and hence an elliptic curve. Its short Weierstraß model is

$$v^2 = u^3 - 24u + 4, \tag{3.3}$$

and this also happens to be a minimal equation for E. This is a well known curve, it has Cremona label 4572b1. The birational transformation equations are

$$u = \frac{2(41s^2 - 195s - 22p + 242)}{s^2}, \tag{3.4}$$

$$v = \frac{2(357s^3 - 2602s^2 - 192sp + 6402s + 484p - 5324)}{s^3}, \tag{3.5}$$

and

$$s = \frac{192u + 22v - 36}{u^2 - 76u - 8},$$

$$p = \frac{94u^3 + 3u^2v + 2982u^2 + 960uv - 23472u - 4512v + 9280}{u^4 - 152u^3 + 5760u^2 + 1216u + 64}.$$

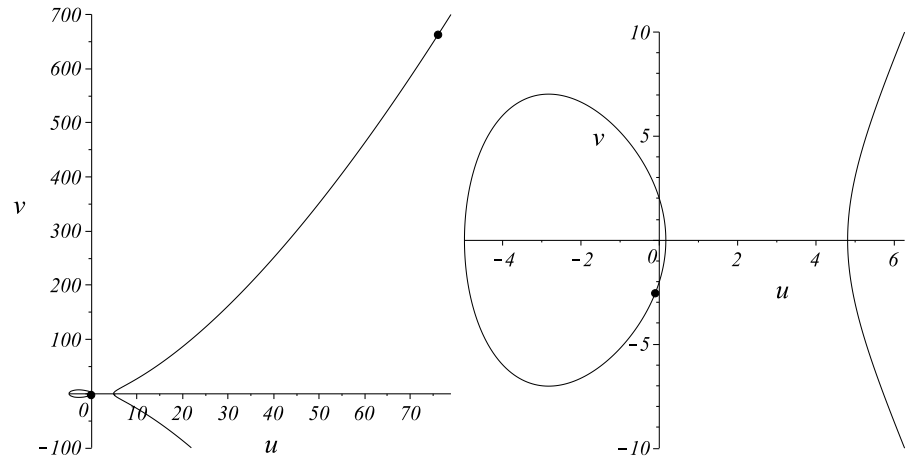
All this can be quickly computed with the Maple package **algcurves**. Now as s tends to $\pm\infty$, we know from (3.2) how any point (s, p) moves along its branch of the curve (3.1), and from (3.4) and (3.5) we have similar information about the point (u, v) on the Weierstraß model (3.3). Hence for each of the parameterizations given by the Puiseux series (3.2),

$$Q_0 = (u_0, v_0) := \lim_{s \to \pm\infty} (u(s), v(s)) = (82 - 44\alpha, 714 - 384\alpha) \tag{3.6}$$

is a point on (3.3). This gives two points, one on each of the two components of this curve (see Figure 2). Therefore we have to consider two separate cases.

We turn to SAGE to find information on the structure of the curve (3.3). It turns out that this is an elliptic curve E over $\mathbb{Q}$ with trivial torsion and of rank 2. A basis for the Mordell–Weil group is $\{(-4, 6), (-3, 7)\}$; this is a certified basis, computed by John Cremona's *mwrank* which is incorporated in SAGE. Also with SAGE we calculated several height values that we shall need shortly; they are given in Table 1 below.

Let us have a further look at equation (3.3). The cubic polynomial $q(u) := u^3 - 24u + 4$ has three distinct real roots, e_1, e_2, e_3, say with $e_1 > e_2 > e_3$. Let $Q_i = (e_i, 0)$ $(i = 1, 2, 3)$ be the corresponding points on the curve. These points are torsion points of order 2 of the curve E defined over a cubic number field generated by a zero of q. The group $E(\mathbb{R})$ has two components (see Figure 2(b)), $E_0(\mathbb{R})$ containing the identity element,



(a) One finite, one infinite branch (b) Zoomed in near the origin

Fig. 2. Graphs of the non-singular curve (3.3) of genus 1; the points Q_0 are drawn in.

Table 1. Important constants for E with equation (3.3)

The functions h and $\hat{h}$ are the naïve logarithmic height and the canonical height functions respectively	
$h_E = h(j_E)$, real height of E	12.3067502132836
upper bound height difference, $\hat{h}(Q) - \frac{1}{2}h(Q)$	1.4735023850806
least eigenvalue of height pairing matrix	0.1271279537058

and the bounded component $E_1(\mathbb{R})$. If $R \in E(\mathbb{R})$ does not belong to $E_0(\mathbb{R})$ then $R' := R + Q_2 \in E_0(\mathbb{R})$. The group isomorphism (see [ST94] and [Za87])

$$\phi : E_0(\mathbb{R}) \to [0,1) = \mathbb{R}/\mathbb{Z} \tag{3.7}$$

can be extended to a two-to-one epimorphism $\tilde{\phi}$ by

$$\tilde{\phi}(Q) = \phi(Q) \text{ or } \phi(Q')$$

for any point $Q \in E(\mathbb{R})$, depending on whether $Q \in E_0(\mathbb{R})$ or not. By the way, the basis elements of the Mordell–Weil group given above do not belong to $E_0(\mathbb{R})$. Now, if ω is the fundamental real period then $\omega\tilde{\phi}(Q)$ is the elliptic logarithm of Q or of Q', whichever makes sense.

Any point $Q \in E(\mathbb{Q})$ can be written as $Q = m_1P_1 + m_2P_2$ where $\{P_1, P_2\}$ is the Mordell–Weil basis given above. As $P_i \notin E_0(\mathbb{R})$, we add Q_2 to each of them, so that $Q = m_1P_1' + m_2P_2' + T$, where T is the identity or a torsion point of order 2. We do the same for Q_0 in case this point happens to lie on the compact component of E. As $2\phi(T) \equiv 0 \pmod 1$ we have

$$\tilde{\phi}(Q) = m_1\phi(P_1') + m_2\phi(P_2') + m_0 + \tfrac{1}{2}\varepsilon,$$

where m_0 is a rational integer with $|m_0| \le 2M + \frac{1}{2} < 2M + 1$ and $\varepsilon \in \{0, 1\}$; here $M := \max(|m_1|, |m_2|)$. In terms of elliptic logarithms we now have (see [ST03, Section 2.5])

$$\int_u^{u_0} \frac{du}{\sqrt{q(u)}} = -\omega\tilde{\phi}(Q_0) + \big(m_0 + \tfrac{1}{2}\varepsilon\big)\omega + m_1\omega\phi(P_1') + m_2\omega\phi(P_2'). \tag{3.8}$$

Now suppose $Q = (s, p)$ is an integral point of (3.1), $s > \mathrm{res}_p\big(F, \frac{\partial F}{\partial p}\big) = 3.2368$, and (u, v) is the birationally corresponding point on (3.3). Further, let us denote the right-hand side of (3.8) by $\mathcal{L}(Q)$. The elliptic integral of (3.8) is connected to one of the elliptic integrals corresponding with the model (3.1) by means of the birational transformations (3.4) and (3.5) in the obvious way, that is,

$$\int_s^{\infty} G\,ds = \pm\int_u^{u_0} \frac{du}{\sqrt{q(u)}} \quad \text{or} \quad \int_{-\infty}^{s} G\,ds = \pm\int_u^{u_0} \frac{du}{\sqrt{q(u)}} \tag{3.9}$$

depending on the point Q, where

$$G := \frac{2(v_s F_p - v_p F_s)}{(3u^2 - 24)F_p}.$$

Specializing p as a Puiseux series (see (3.2)) and hence u and v as well via (3.4) and (3.5), we find the following Puiseux expansion for G in terms of powers of s:

$$G = \big(\tfrac{2}{3} - \tfrac{2}{3}\alpha\big)s^{-2} + \big(\tfrac{10}{3} - \tfrac{10}{3}\alpha\big)s^{-3} + O(s^{-4}) \quad (s \to \pm\infty).$$

Combining this expression with (3.8) and (3.9) should give an upper bound for $|\mathcal{L}(Q)|$ in terms of the abscissa of the integral point Q, namely (see [ST03, Section 2.4])

$$|\mathcal{L}(Q)| \le c_1|s|^{-1}. \tag{3.10}$$

To find a suitable value for c_1, solve $F = 0$—which is quadratic in p (see (3.1))—explicitly for p and substitute the solutions $p = p(s)$ into G. This gives, for both values of α,

$$|G| = \frac{1}{\sqrt{3s^4 - 30s^3 + 114s^2 - 192s + 121}} \le 0.6s^{-2}$$

for $|s| > 1000$ and therefore we may take $c_1 = 0.6$.

We have now established an upper bound for $|\mathcal{L}(Q)|$ in terms of s, but we need an upper bound in terms of the maximum M of the absolute values of the coefficients m_1, m_2 of Q with respect to the given Mordell–Weil basis. Therefore we need the constants c_2, c_3 of [ST03, Lemma 2.5.1]. These can be found using (3.2) and (3.4). To be more precise, if (u, v) are the coordinates of Q on (3.3) then the naïve logarithmic height of Q is

$$h(u) = \log\max(|2(41s^2 - 195s - 22p + 242)|, s^2) \le \log 77 + \log s^2$$

for $|s| > 1000$. On the other hand (see Table 1)

$$h(u) \geq 2(\hat{h}(Q) - 1.48) \geq 2(0.127M^2 - 1.48),$$

and hence

$$\log|s| \geq -1.48 - \tfrac{1}{2}\log 77 + 0.127M^2. \tag{3.11}$$

Combining (3.10) with (3.11) leads to

$$|\mathcal{L}(Q)| \leq \exp(3.15 - 0.127M^2). \tag{3.12}$$

Finally, the lower bound for $\mathcal{L}(Q)$ is provided by S. David's theorem [Da95, Théorème 2.1]:

$$|\mathcal{L}(Q)| > \exp(-c_4(\log N + c_5)(\log\log N + c_6)^5). \tag{3.13}$$

Here N is an upper bound for all the coefficients in the linear form of elliptic logarithms $\mathcal{L}(Q)$, so that $N \leq 2M+1$. This lower bound is valid provided M is not less than a certain small positive constant. For a detailed discussion of the constants c_4, c_5 and c_6 the reader can consult [Tz96, Appendix]. We calculated $c_4 = 0.995 \cdot 10^{118}$, $c_5 = 2.8$, $c_6 = 15.1$. Observe that the points Q_0 and P_1', P_2' are defined over a number field of degree 6. As the right-hand side of (3.13) is larger than the right-hand side of (3.12) for large M, this gives an upper bound for M. Our calculations give the initial upper bound $0.622 \cdot 10^{64}$ for M.

Table 2. Integer points (s, p) on (3.1) and their corresponding points on (3.3)

Integer points on (3.1) with corresponding rational points $(u, v) = m_1(-4, 6) + m_2(-3, 7)$ on (3.3)					
s	p	m_1	m_2	u	v
8	60	−3	0	−7/16	−243/64
−10	286	−2	−1	0	−2
4	1	−2	0	12	38
3	2	−1	0	−4	−6
1	0	−1	1	176	−2334
2	1	0	1	−3	7
2	0	1	1	8	−18
0	11	1	2	20/121	258/1331
1	4	2	1	0	2
3	0	2	2	52/9	206/27
4	6	3	2	−7/4	−51/8
−10	15	3	3	2981/25	162621/125
8	7	4	2	36	214

The final step is to reduce this large upper bound to a manageable size. We use the LLL algorithm as implemented by de Weger; we closely follow the detailed description in [Tz96, Section 5]. General information on the LLL method can be found in [Sm98, Section V.4]. The calculations were done by PARI/gp. Observe that here we are in the inhomogeneous case because of the first term in $\mathcal{L}(Q)$ (see (3.8)). This makes the reduction process slightly more complicated. The first reduction gives an upper bound of 49, the second gives 14 and the third reduction gives an upper bound of 13 for M; no further reduction of the bound was obtained. Considering the range $[-13, 13]$ for m_1, m_2 with $Q = m_1P_1 + m_2P_2$ we get precisely the expected values. The results are contained in Table 2. Observe that $(s, p) = (0, 0)$ is missing from the table; this point comes from the group identity (the point at infinity) of the Weierstraß model (3.3).

4. The degree 5 case. This case is very similar to the degree 4 case. Also the shapes of the curves look very much the same. Therefore we can shorten this section considerably, and refer to the corresponding description in the previous section.

We shall prove the following

THEOREM 3. *The diophantine equation* (1.2) *with* $d = 5$ *and* $(x, y) \in \mathbb{Z}^2$ *has the twelve solutions*

$$(x, y) = (0, 0), (0, 1), (0, 2), (0, 3), (1, 0), (1, 1), \\ (1, 2), (1, 9), (2, 0), (2, 1), (3, 0), (9, 1)$$

together with all integer pairs on the line $x + y - 4 = 0$*, and no others.*

As a consequence, there is only one fair $(2, 5)$-game, namely the one represented by $(1, 9)$.

Now, equation (1.2) is reducible, and we first factor out the linear factor $x + y - 4$. The remaining irreducible factor again gives a curve of genus 3. Putting $s = x + y$ and $p = xy$ in the equation for this curve yields (compare with (3.1))

$$F = 0, \quad \text{with} \quad F = s(s-1)(s-2)(s-3) + 10p(-s^2 + 4s + p - 5). \tag{4.1}$$

This time we find the 12 integer solutions

$$(s, p) = (-10, 13), (-10, 132), (0, 0), (0, 5), (1, 0), (1, 2), \\ (2, 0), (2, 1), (3, 0), (3, 2), (10, 9), (10, 56)$$

in the range $-1000 \le s, p \le 1000$ and no others, and so we may assume $|s| > 1000$ for a solution $(s, p) \in \mathbb{Z}^2$ of (4.1). The curve $F = 0$ is of genus 1 so that we may apply the elliptic logarithm method Ellog in this case too. The real graph of $F = 0$ reveals four infinite branches and the corresponding

Puiseux series begin as follows:

$$p = \alpha s^2 + \left(\tfrac{1}{3} - \tfrac{14}{3}\alpha\right)s - \tfrac{19}{18} + \tfrac{64}{9}\alpha + O(s^{-1}) \quad (s \to \pm\infty), \tag{4.2}$$

where α is a root of $10t^2 - 10t + 1 = 0$, so that $\alpha = \frac{1}{2} \pm \frac{1}{10}\sqrt{15}$.

The curve represented by equation (4.1) is a non-singular curve E of genus 1 over $\mathbb{Q}$ with a distinguished point and hence an elliptic curve. Its short Weierstraß model

$$v^2 = u^3 - 3100u - 20000 \tag{4.3}$$

is also the minimal equation for E. The birational transformation equations are

$$u = \frac{10(43s^2 - 194s - 50p + 250)}{s^2}, \tag{4.4}$$

$$v = \frac{100(-82s^3 + 583s^2 + 94sp - 1440s - 250p + 1250)}{s^3}, \tag{4.5}$$

and

$$s = \frac{-940u + 50v - 5800}{u^2 - 360u - 5100},$$

$$p = \frac{430u^3 - 6u^2v + 60100u^2 - 9840uv - 5597000u + 490600v + 1210000}{u^4 - 720u^3 + 119400u^2 + 3672000u + 26010000}.$$

Now, as s tends to $\pm\infty$, we know from (4.2) how any point (s, p) moves along its branch of the curve (4.1), and from (4.4) and (4.5) we have similar information about the point (u, v) on the Weierstraß model (4.3). Hence for each of the four parameterizations given by the Puiseux series the point

$$Q_0 = (u_0, v_0) := \lim_{s \to \pm\infty} (u(s), v(s)) = (430 - 500\alpha, -8200 + 9400\alpha) \tag{4.6}$$

is a point on (4.3). This gives two distinct points, one on each of the two components of this curve. The graphs of (4.3) are quite similar to the ones in Figure 2 except for the precise positions of the Q_0.

The elliptic curve $E/\mathbb{Q}$ has trivial torsion and is of rank 3. A certified basis for the Mordell–Weil group is $\{(-50, 100), (-40, 200), (-36, 212)\}$. Important constants for E are given in Table 3. The cubic polynomial $q(u) := u^3 - 3100u - 20000$ (see the Weierstraß equation (4.3) for E) has

Table 3. Important constants for E with equation (4.3)

The functions h and $\hat{h}$ are the naïve logarithmic height and the canonical height functions respectively	
$h_E = h(j_E)$, real height of E	17.7566815628194
upper bound height difference, $\hat{h}(Q) - \frac{1}{2}h(Q)$	2.8224454784140
least eigenvalue of height pairing matrix	0.3081893302623

three distinct real roots, e_1, e_2, e_3, say with $e_1 > e_2 > e_3$. As before, the $Q_i = (e_i, 0)$, $i = 1, 2, 3$, are the corresponding points on the curve; Q_i is a torsion point of E of order 2 over the cubic number field $\mathbb{Q}(e_i)$. In order to work out the upper bound for the linear form in elliptic logarithms we follow exactly the same argument that was used in the previous section, starting with the definition of the group isomorphism (3.7). The only difference is the rank of E, which results in an extra term in this linear form. All three group generators correspond with points in the compact part $E_0(\mathbb{R})$.

We now find

$$\frac{2(v_s F_p - v_p F_s)}{(3u^2 - 3100)F_p} = \big(-\tfrac{1}{3} + \tfrac{2}{3}\alpha\big)s^{-2} + \big(-\tfrac{14}{9} + \tfrac{28}{9}\alpha\big)s^{-3} + O(s^{-4}) \quad (s \to \pm\infty),$$

so that

$$|\mathcal{L}(Q)| \le c_1 |s|^{-1}, \tag{4.7}$$

where $\mathcal{L}(Q) = -\omega\tilde{\phi}(Q_0) + \big(m_0 + \frac{1}{2}\varepsilon\big)\omega + m_1\omega\phi(P_1') + m_2\omega\phi(P_2') + m_3\omega\phi(P_2')$. Now

$$|G| = \frac{1}{\sqrt{15s^4 - 140s^3 + 540s^2 - 940s + 625}} \le 0.3s^{-2}$$

for $|s| > 1000$ and both values of α, and we can therefore take $c_1 = 0.3$. As we shall need to find an upper bound for $|\mathcal{L}(Q)|$ in terms of the maximum M of the absolute values of the coefficients m_1, m_2, m_3 of Q with respect to the given Mordell–Weil basis, we proceed as follows.

Let $(u, v) \in E(\mathbb{Q})$ be the coordinates of Q on (4.3). Then the naïve logarithmic height of Q is

$$h(u) = \log \max(|10(43s^2 - 194s - 50p + 250)|, s^2) \le \log 375 + \log s^2$$

for $|s| > 1000$. Combining this with the inequality (see Table 3)

$$h(u) \ge 2(\hat{h}(Q) - 2.83) \ge 2(0.308M^2 - 2.83),$$

ultimately leads to the upper bound

$$\begin{aligned} |\mathcal{L}(Q)| &\le \exp(\log 0.3 + 2.83 + \tfrac{1}{2}\log 375 - 0.308M^2) \\ &\le \exp(4.59 - 0.308M^2). \end{aligned} \tag{4.8}$$

The lower bound for $\mathcal{L}(Q)$ is provided by [Da95, Théorème 2.1]:

$$|\mathcal{L}(Q)| > \exp(-c_4(\log(3M+1) + c_5)(\log\log(3M+1) + c_6)^6). \tag{4.9}$$

We calculated $c_4 = 0.443 \cdot 10^{166}$, $c_5 = 2.8$, $c_6 = 20.6$. The points Q_0 and P_1', P_2', P_3' are defined over a number field of degree 6. As the right-hand side of (4.9) is larger than that of (4.8) for large M, this gives an upper bound for M. Our calculations give the initial upper bound $0.301 \cdot 10^{89}$ for M. The first LLL reduction step brings this large bound down to 37, the next one

gives 10 and finally the reduction stops at 9. Considering all rational points

$$(u, v) = m_1(-50, 100) + m_2(-40, 100) + m_3(-36, 212)$$

with $|m_i| \leq 9$ $(i = 1, 2, 3)$ on (4.3) coming from integral points (s, p) on (4.1), and checking which ones come from integral solutions of equation (1.2), brings no surprises. For details see Table 4.

Table 4. Integer points (s, p) on (4.1) and their corresponding points on (4.3)

Integer points on (4.1) with corresponding rational points $(u, v) = m_1(-50, 100) + m_2(-40, 200) + m_3(-36, 212)$ on (4.3)						
s	p	m_1	m_2	m_3	u	v
10	56	−2	0	−1	−19	−179
−10	13	−2	0	0	584	14048
−168	3213	−2	1	−1	169660/441	69134500/9261
3	2	−1	0	0	−50	−100
1	0	−1	1	0	990	−31100
2	1	0	1	0	−40	200
2	0	0	1	1	85	−575
0	5	0	2	1	−164/25	916/125
1	2	1	1	1	−10	100
3	0	1	2	1	550/9	3700/27
−168	25688	2	1	2	−215/16	−8875/64
−10	132	2	2	1	−11	−113
10	9	2	2	2	216	3064

Acknowledgements. We are grateful for a suggestion made by an anonymous referee that indirectly led to a reduction of the computational effort.

References

[Da95] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. France (N.S.) 62 (1995).

[Fa83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[HP11] C. Y. Hui and W. Y. Pong, *Diophantine equations of matching games I*, Integers 12 (2012), to appear.

[Sm98] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Math. Soc. Student Texts 41, Cambridge Univ. Press, 1998.

[ST94] R. J. Stroeker and N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. 67 (1994), 177–196.

[ST03] R. J. Stroeker and N. Tzanakis, *Computing all integer solutions of a genus* 1 *equation*, Math. Comp. 72 (2003), 1917–1933.

[Tz96] N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations*, Acta Arith. 75 (1996), 165–190.

[Za87] D. Zagier, *Large integral points on elliptic curves*, Math. Comp. 48 (1987), 425–436.

Wai Yan Pong
Department of Mathematics
California State University Dominguez Hills
1000 E. Victoria Street
Carson, CA 90747-0005, U.S.A.
E-mail: wpong@csudh.edu

Roelof J. Stroeker
Vlinderslag 17
2924 VK Krimpen aan den IJssel
Netherlands
E-mail: roel@stroeker.nl

Received on 8.2.2011
and in revised form on 19.5.2011 (6612)