NIEUW ARCHIEF VOOR WISKUNDE

Vierde serie Deel 17 No. 2 juli 1999, pp. 175 – 186

# On Integral Zeroes of Binary Krawtchouk Polynomials

Roelof J. Stroeker
*Econometric Institute, Erasmus University,*
*P.O.Box 1738, 3000 DR Rotterdam, The Netherlands,*
*e-mail:* stroeker@few.eur.nl

Benjamin M.M. de Weger*
*Sportsingel 30,*
*2924 XN Krimpen aan den IJssel,*
*The Netherlands,*
*e-mail:* deweger@xs4all.nl

**In this paper we provide complete sets of integral zeroes of the binary Krawtchouk polynomials of degree 6 and 7. The zeroes of these polynomials correspond to points on certain rational elliptic curves. Our results are obtained by applying estimates of associated linear forms in elliptic logarithms.**

## 1. Introduction

Krawtchouk polynomials obtain their importance from discrete mathematics, especially coding theory. Their combinatorial significance is almost evident from the following standard definition:

$$P_k^n(x) := \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j} (q-1)^{k-j}.$$

Alternatively, the sequence of Krawtchouk polynomials $(P_k^n(x))_{k\geq 0}$ is defined by its generating function

$$\sum_{k=0}^{\infty} P_k^n(x) z^k = (1-z)^x \, (1+(q-1)z)^{n-x}.$$

*This author's research was supported by the Netherlands Mathematical Research Foundation SWON with financial aid from the Netherlands Organization for Scientific Research NWO.

The Krawtchouk polynomials are an example of a class of orthogonal polynomials, and therefore share many properties with other such polynomials. Orthogonality is expressed by the following relation:

$$\sum_{j=0}^{n} \binom{n}{j} (q-1)^j P_k^n(j) P_l^n(j) = \delta_{kl} \binom{n}{k} (q-1)^k q^n.$$

The question of the existence of integral zeroes arises in many combinatorial settings and problems in coding theory. An overview is given in [7]. Very little seems to be known in a general way. See also [5]. In this paper we shall only be concerned with zeroes of binary Krawtchouk polynomials ($q = 2$).

The first interesting polynomial in this respect is $P_4^n$. In [4] DIACONIS and GRAHAM expressed the wish to determine the integral roots of $P_4^n(x) = 0$ for all $n$. STROEKER and DE WEGER [13], and independently MIGNOTTE and PETHŐ [8], constructed complete sets of these roots. In his thesis [6] HANROT did the same for $P_5^n(x) = 0$. The present paper is devoted to the construction of complete sets of integral zeroes for $P_6^n(x)$ and $P_7^n(x)$. These are special instances of the general case we completely work out in our paper [14]. For $k = 4, 5, 6, 7$, equation $P_k^n(x) = 0$ can be associated with an elliptic curve; our method is firmly based on this relationship. For $k = 8$, this equation corresponds to a curve of genus 3, which renders generalization of our approach unlikely.

For the moment it is convenient to adopt the following notation:

$$Q_k(y, n) := k! P^n(\tfrac{1}{2}(n - y)). \tag{1}$$

Table 1 below lists the first few ($k = 0, 1, \ldots, 8$) Krawtchouk polynomials in their modified form.

TABLE 1. Modified Krawtchouk polynomials (1)

| Modified Krawtchouk polynomials $Q_k(y,n)$, $k = 0, \ldots, 8$ | |
|---|---|
| $k$ | $Q_k(y,n)$ |
| 0 | $1$ |
| 1 | $y$ |
| 2 | $y^2 - n$ |
| 3 | $y(y^2 - 3n + 2)$ |
| 4 | $y^4 - 6y^2n + 8y^2 + 3n^2 - 6n$ |
| 5 | $y(y^4 - 10y^2n + 20y^2 + 15n^2 - 50n + 24)$ |
| 6 | $y^6 - 15y^4n + 40y^4 + 45y^2n^2 - 210y^2n - 15n^3 + 184y^2 + 90n^2 - 120n$ |
| 7 | $y(y^6 - 21y^4n + 70y^4 + 105y^2n^2 - 630y^2n - 105n^3 + 784y^2 + 840n^2 - 1764n + 720)$ |
| 8 | $y^8 - 28y^6n + 112y^6 + 210y^4n^2 - 1540y^4n - 420y^2n^3 + 2464y^4 + 4200y^2n^2 + 105n^4 - 11872y^2n - 1260n^3 + 8448y^2 + 4620n^2 - 5040n$ |

We shall now formulate the results we obtained.

On putting $U = n$ and $V = y^2$ in $Q_6(y, n) = 0$, and $U = n - 1$ and $V = y^2 - 1$ in $Q_7(y, n) = 0$ the following binary cubic diophantine equations emerge:

$$-15U^3+45U^2V-15UV^2+V^3+90U^2-210UV+40V^2-120U+184V = 0 \quad (2)$$

$$-105U^3+105U^2V-21UV^2+V^3+630U^2-462UV+52V^2-840U+360V = 0 \quad (3)$$

THEOREM 1 *The diophantine equation* (2) *has integral solutions* $(U, V)$ *as given in Table* 2 *below, and no others. In addition to the solutions, the table also gives the corresponding values of* $x, n, y$. *Symmetry about* $x = n/2$ *permits the restriction to* $x$*-values* $\leq n/2$.

TABLE 2. Solutions of (2)

| Solutions $(U,V)$ of (2), $U = n$, $V = y^2 = (n-2x)^2$, $x \leq n/2$ | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $(U,V)$ | $x$ | $n$ | $y$ | $(U,V)$ | $x$ | $n$ | $y$ | $(U,V)$ | $x$ | $n$ | $y$ |
| $(-14,-56)$ | | | | $(3,1)$ | 1 | 3 | 1 | $(9,25)$ | 2 | 9 | 5 |
| $(-4,-20)$ | | | | $(3,9)$ | 0 | 3 | 3 | $(12,4)$ | 5 | 12 | 2 |
| $(-1,-9)$ | | | | $(4,0)$ | 2 | 4 | 0 | $(12,36)$ | 3 | 12 | 6 |
| $(0,0)$ | 0 | 0 | 0 | $(4,4)$ | 1 | 4 | 2 | $(12,100)$ | 1 | 12 | 10 |
| $(1,1)$ | 0 | 1 | 1 | $(4,16)$ | 0 | 4 | 4 | $(16,144)$ | 2 | 16 | 12 |
| $(2,-14)$ | | | | $(5,1)$ | 2 | 5 | 1 | $(25,9)$ | 11 | 25 | 3 |
| $(2,0)$ | 1 | 2 | 1 | $(5,9)$ | 1 | 5 | 3 | $(67,25)$ | 31 | 67 | 5 |
| $(2,4)$ | 0 | 2 | 2 | $(5,25)$ | 0 | 5 | 5 | $(345,1225)$ | 155 | 345 | 35 |
| $(3,-5)$ | | | | | | | | | | | |

THEOREM 2 *The diophantine equation* (3) *has integral solutions* $(U, V)$ *as given in Table* 3 *below, and no others. In addition to the solutions, the table also gives the corresponding values of* $x, n, y$. *Symmetry about* $x = n/2$ *permits the restriction to* $x$*-values* $\leq n/2$.

TABLE 3. Solutions of (3)

| Solutions $(U,V)$ of (3), $U=n-1$, $V=y^2-1=(n-2x)^2-1$, $x \leq n/2$ | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $(U,V)$ | $x$ | $n$ | $y$ | $(U,V)$ | $x$ | $n$ | $y$ | $(U,V)$ | $x$ | $n$ | $y$ |
| $(-22,-132)$ | | | | $(3,-7)$ | | | | $(5,35)$ | 0 | 6 | 6 |
| $(-6,-42)$ | | | | $(3,3)$ | 1 | 4 | 2 | $(8,8)$ | 3 | 9 | 3 |
| $(-3,-25)$ | | | | $(3,15)$ | 0 | 4 | 4 | $(13,15)$ | 5 | 14 | 4 |
| $(0,0)$ | 0 | 1 | 1 | $(4,0)$ | 2 | 5 | 1 | $(13,63)$ | 3 | 14 | 8 |
| $(1,3)$ | 0 | 2 | 2 | $(4,8)$ | 1 | 5 | 3 | $(13,143)$ | 1 | 14 | 12 |
| $(2,-18)$ | | | | $(4,24)$ | 0 | 5 | 5 | $(16,80)$ | 4 | 17 | 9 |
| $(2,0)$ | 1 | 3 | 1 | $(5,3)$ | 2 | 6 | 2 | $(21,255)$ | 4 | 22 | 16 |
| $(2,8)$ | 0 | 3 | 3 | $(5,15)$ | 1 | 6 | 4 | $(1028,1368)$ | 496 | 1029 | 37 |

The solution process employs recent developments in the estimation of linear forms in elliptic logarithms. Extensive coverage of this method is given in [11, 14, 15]. We intend to give a detailed proof of Theorem 1 in the next section. The proof of Theorem 2 has an entirely similar structure; the main ingredients of the latter are presented in [14].

## 2. THE SOLUTION PROCESS

Instead of first giving a general overview of the elliptic logarithm method, we intend to guide the reader through the successive steps of the solution process of equation (2) and explain the different aspects of the method as we proceed. We shall closely follow [14] where a thorough treatment is given of the elliptic logarithm method as applied to the most general cubic diophantine equation in two unknowns that represents an elliptic curve over $\mathbb{Q}$.

We turn to equation (2). The graph of this equation in the $(U,V)$-plane shows three distinct asymptotes, in other words, there are three distinct points at infinity. So, in order to locate the finitely many integral points, we have to investigate what happens to a rational point on the curve when it moves towards one of these three infinite points.

The birational transformations

$$\begin{aligned}(U,V) &= \left(\frac{-4036X-276Y+623404}{3X^2-1982X-76Y+222415}, \frac{1500X-180Y+72780}{3X^2-1982X-76Y+222415}\right),\\ (X,Y) &= \left(\frac{11865U-4817V-31680}{15U-23V}, \frac{1574100U^2+2469720UV-425260V^2-3960000U-10655040V}{(15U-23V)^2}\right)\end{aligned} \tag{4}$$

relate equation (2) to the global minimal Weierstraß model

$$Y^2+XY+Y=X^3-X^2-62705X+5793697. \tag{5}$$

Let us denote the elliptic curve by $E$, and the group of real points $(X,Y)$ by $E(\mathbb{R})$, including the point at infinity $\mathcal{O}$, which is the group identity. Moreover,

we shall denote the compact component of $E(\mathbb{R})$ by $E_C(\mathbb{R})$ and the infinite component by $E_0(\mathbb{R})$.
A further transformation

$$(X, Y) = (\tfrac{1}{4}x + \tfrac{1}{4}, \tfrac{1}{8}y - \tfrac{1}{8}x - \tfrac{5}{8}), \quad (x, y) = (4X - 1, 8Y + 4X + 4)$$

maps (5) to the short Weierstraß model

$$y^2 = x^3 - 1003275x + 369793350. \tag{6}$$

Applying Connell's program Apecs (see [1]) to this curve we quickly compute its particulars, for instance we learn that its torsion subgroup is trivial. By Cremona's program mrank (see [2]) we find out that its rank is 4, and four independent rational points are $P_1 = (439, 7700)$, $P_2 = (109, 440)$, $P_3 = (199, -1180)$, $P_4 = (43, -1804)$, with regulator $R = 0.898422\ldots$. Computing canonical heights we find that $\hat{h}(P_1) = 0.358638\ldots$, and we intend to show that there are no points with canonical height below this value.

Silverman's and Siksek's bounds for the difference of canonical and naive heights, as computed by Apecs, read

$$-3.95986 < \hat{h}(P) - \tfrac{1}{2}h(X(P)) < 5.14593 \tag{7}$$

for any $P$ (see also [9, 10]). So, if there were a point $P$ with $\hat{h}(P) < \hat{h}(P_1)$, then $h(X(P)) < 8.63700$ for such a point. With Cremona's findinf we searched for all such points, showing that if $h(X(P)) < 8.63700$ then $P = \mathcal{O}$ or $\hat{h}(P) \geq \hat{h}(P_1)$. Thus we can take $\lambda = 0.358638$ in Siksek's upper bound (see [10, Theorem 3.1]) for the index of the group generated by $P_1, P_2, P_3, P_4$ in the full Mordell-Weil group, which yields

$$\text{index} \leq \sqrt{R}\frac{2}{(2\lambda)^2} = 3.68\ldots.$$

In order to show that $P_1, P_2, P_3, P_4$ form a basis for the full group of rational points, it remains to prove that the index cannot be equal to 3, because information from mrank tells us that the index must be odd. Siksek sieving with $p = 3$ and $v = 13, 23, 37, 53$ gives the relation matrix

$$\begin{pmatrix} 1 & 1 & -1 & -1 \\ 0 & 1 & -1 & 1 \\ 1 & 0 & 1 & -1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \pmod 3,$$

in which each column represents a prime $v$. Clearly its rank is 4, which means the index is 1.

It is quite easy to show that our choice of basis is optimal in the sense that the least eigenvalue of the Néron-Tate height pairing matrix is as large as possible (see [12]). This least eigenvalue is $c_1 = 0.259202\ldots$.

By means of the birational transformations (4), it not difficult to establish the following relations between the differential forms associated with the different models for our curve.

$$\frac{\mathrm{d}V}{-45U^2+90UV-15V^2+180U-210V-120} = -\tfrac{1}{2}\frac{\mathrm{d}X}{2Y+X+1} = -\tfrac{1}{2}\frac{\mathrm{d}x}{y}. \tag{8}$$

Let us now give a description of the asymptotes, so that we can trace rational points on (2) when $(U,V) \to \infty$. Let $\alpha_i$ $(i=1,2,3)$ be a root of

$$\alpha^3 - 15\alpha^2 + 45\alpha - 15 = 0,$$

and put $\beta_i = -\frac{1}{6}(7\alpha_i + \alpha_i^2)$. The three asymptotes are then given by $V = \alpha_i U + \beta_i$ for $i = 1,2,3$. The corresponding points at infinity, given in $(X,Y)$-coordinates, are

$$Q_0 = (X_0, Y_0) = \left(\frac{11865 - 4817\alpha}{15-23\alpha}, \frac{1574100 + 2469720\alpha - 425260\alpha^2}{(15-23\alpha)^2}\right).$$

| $i$ | $\alpha_i$ | $\beta_i$ | $Q_{0,i}$ |
|---|---|---|---|
| 1 | 0.380327... | −0.467822... | (1604.63..., 62718.5...) |
| 2 | 3.56898... | −6.28675... | (79.4018..., 1104.66...) |
| 3 | 11.0506... | −33.2454... | (172.960..., −403.242...) |

Note that $Q_0 \in E(\mathbb{K})$, where $\mathbb{K} = \mathbb{Q}(\alpha)$ is a cubic number field. The numerical values of the $\alpha_i$, $\beta_i$ and $Q_{0,i}$ are gathered in the table above.

We now distinguish six $(U,V)$-ranges on (2), one for each half-asymptote. They are:

$1_1$ : The range between $(4,0)$ and $Q_{0,1}$,
$1_2$ : The range between $(0,0)$ and $Q_{0,1}$,
$2_1$ : The range between $(2,0)$ and $Q_{0,2}$, with $U \geq 2$ and $V \geq 0$,
$2_2$ : The range between $(2,0)$ and $Q_{0,2}$, with $U \leq 2$ and $V \leq 0$,
$3_1$ : The range between $(0,0)$ and $Q_{0,3}$,
$3_2$ : The range between $(4,0)$ and $Q_{0,3}$.

On each of the three separate branches of (2) $U$ can be viewed as a strictly increasing function of $V$. On each branch let $F : \mathbb{R} \to \mathbb{R}$ be given by

$$F(v) = \frac{11865u(v) - 4817v - 31680}{15u(v) - 23v},$$

where $u(v)$ is the unique solution on that branch implicitly given by equation (2). Then $X = F(V)$. For each of the six $(U,V)$-ranges, the unique $V$-interval

and its $X$-image under $F$ are as follows:

$$\begin{array}{lllll}
1_1: & I=[V,\infty) & \longrightarrow & J=[X,X_{0,1}) & \\
1_2: & I=(-\infty,V] & \longrightarrow & J=(X_{0,1},X] & \\
2_1: & I=[V,\infty) & \longrightarrow & J=[X,X_{0,2}) & \text{if } V\geq 8 \\
2_2: & I=(-\infty,V] & \longrightarrow & J=(X_{0,2},X] & \text{if } V\leq -1 \\
3_1: & I=[V,\infty) & \longrightarrow & J=[X,X_{0,3}) & \\
3_2: & I=(-\infty,V] & \longrightarrow & J=(X_{0,3},X] & \text{if } V\leq -17
\end{array}$$

The conditions imposed in some cases are necessary to make sure that the correspondence of intervals is a bijective one. Note that in the cases $1_1$, $1_2$, $3_1$ and $3_2$ the points corresponding to the $J$-interval are located on $E_0(\mathbb{R})$, while in the remaining cases $2_1$ and $2_2$ they are on $E_C(\mathbb{R})$.
In all cases we have by (8)

$$\int_I \frac{\mathrm{d}V}{-45U^2+90UV-15V^2+180U-210V-120} = \tag{9}$$

$$\pm\tfrac{1}{2}\int_J \frac{\mathrm{d}X}{2Y+X+1} = \pm\tfrac{1}{2}\int_{J'}\frac{\mathrm{d}x}{y}, \tag{10}$$

where $J'$ is an obvious linear adjustment of the interval $J$. If $V\leq -17$ or $V\geq 8$ then, by explicitly solving equation (2) for $U=U(V)$, it can be seen that

$$-45U^2+90UV-15V^2+180U-210V-120\geq 5.54428V^2.$$

Hence

$$\int_I \frac{\mathrm{d}V}{-45U^2+90UV-15V^2+180U-210V-120} < \tag{11}$$

$$0.180366\int_I \frac{\mathrm{d}V}{V^2} = 0.180366\,\frac{1}{|V|}. \tag{12}$$

Now the time has come to consider an arbitrary point $P$ on (2) with integral coordinates $U$, $V$. Then $P=m_1P_1+m_2P_2+m_3P_3+m_4P_4$ for certain integers $m_i$ $(i=1,\ldots,4)$. Let $M=\max_{1\leq i\leq 4}|m_i|$. Our final goal is to compute an absolute upper bound for $M$. Therefore we need to establish a relationship between $(U,V)$ (for large $|V|$) and these coefficients $m_i$ $(i=1,\ldots,4)$. The way to do this is via elliptic integrals, or rather by means of elliptic logarithms, which essentially are values of the inverse function of the Weierstraß $\wp$-function. The $\phi$-function, which was used in [11] for this purpose, cannot be employed without some adjustment, because in [11] it is defined only on the infinite branch $E_0(\mathbb{R})$. Here we shall use the trick introduced by Tzanakis [15], but we prefer to describe it as follows.

Let $\omega = 0.237702\ldots$ and $\eta = 0.151315\ldots i$ be the fundamental real and imaginary periods of the Weierstraß $\wp$-function for the model (6). Then the elliptic logarithm can be seen as a function

$$u : E(\mathbb{C}) \to \omega[0,1) \times \eta[0,1),$$

the inverse of which is given by the Weierstraß parametrization

$$u^{\text{inv}} : z \to (\wp(z), \wp'(z)).$$

Let $\gamma_1 < \gamma_2 < \gamma_3$ be the roots of $\gamma^3 - 1003275\gamma + 369793350 = 0$, and let $T_i = (\gamma_i, 0)$ $(i = 1,2,3)$ be the 2-torsion points (which incidently are not rational). Then $T_1, T_2 \in E_{\mathrm{C}}(\mathbb{R})$ and $T_3 \in E_0(\mathbb{R})$. Note that

$$\begin{aligned} &u : E_0(\mathbb{R}) \to [0,\omega), && u(\mathcal{O}) = 0, && u(T_3) = \tfrac{1}{2}\omega, \\ &u : E_{\mathrm{C}}(\mathbb{R}) \to [0,\omega) + \tfrac{1}{2}\eta, && u(T_1) = \tfrac{1}{2}\eta, && u(T_2) = \tfrac{1}{2}\omega + \tfrac{1}{2}\eta. \end{aligned}$$

We now define $\phi : E(\mathbb{R}) \to [0,1)$—for points on $E_0(\mathbb{R})$ as well as $E_{\mathrm{C}}(\mathbb{R})$—as the result of applying Zagier's algorithm (see [17]), i.e. $\phi(\mathcal{O}) = \phi(T_2) = 0$, $\phi(T_1) = \phi(T_3) = \frac{1}{2}$, and otherwise

$$\phi(P) = \sum_{i=0}^{\infty} a_i 2^{-(i+1)},$$

where

$$a_i = \begin{cases} 0 & \text{if } y(2^i P) \geq 0 \text{ or } 2^i P = \mathcal{O} \\ 1 & \text{if } y(2^i P) < 0 \end{cases} \quad (i = 0, 1, \ldots).$$

As a matter of fact, $u(P) = \omega\phi(P)$ for $P \in E_0(\mathbb{R})$. And it is an easy exercise to show that for $P \in E_{\mathrm{C}}(\mathbb{R})$ we have

$$u(P) = \omega\phi(P) + \tfrac{1}{2}\eta + \operatorname{sign}(y(P))\tfrac{1}{2}\omega.$$

It follows that

$$\phi(P) = \phi(P + T_2),$$

which is exactly what Tzanakis does in [15]. Observe that our $\phi$-function is linear (mod 1). Further we can express $\phi(P)$ in terms of an elliptic integral as follows.

$$\phi(P) = \operatorname{sign}(y(P)) \frac{1}{\omega} \int_{x(P)}^{D} \frac{\mathrm{d}t}{\sqrt{t^3 - 1003275t + 369793350}} \pmod 1,$$

where

$$D = \begin{cases} \infty & \text{if } P \in E_0(\mathbb{R}), \\ \gamma_2 & \text{if } P \in E_{\mathrm{C}}(\mathbb{R}). \end{cases}$$

We leave the proof of this formula to the reader.
It is clear that we always need to work with a difference of elliptic logarithms $u(P)-u(Q_0)$, where $P$ and $Q_0$ lie close together on the same component. Hence $P-Q_0$ is always on the infinite component, and $u(P)-u(Q_0) = \omega\phi(P)-\omega\phi(Q_0)$ is real.
As a consequence of all this, we see that

$$\int_{J'} \frac{\mathrm{d}x}{y} = \pm\omega(\phi(Q_{0,i}) - \phi(P)). \tag{13}$$

Further,

$$\phi(P) = m_1\phi(P_1) + m_2\phi(P_2) + m_3\phi(P_3) + m_4\phi(P_4) + m_0,$$

with $m_0 \in \mathbb{Z}$ and such that all $\phi$-values are in $[0,1)$. Note that then $|m_0| \leq 4M$. Put $u_1 = \omega\phi(P_1) = 0.0492342\ldots$, $u_2 = \omega\phi(P_2) = 0.0219847\ldots$, $u_3 = \omega\phi(P_3) = 0.152036\ldots$, $u_4 = \omega\phi(P_4) = 0.184517\ldots$, $u_{0,1} = \omega\phi(Q_{0,1}) = 0.0250246\ldots$, $u_{0,2} = \omega\phi(Q_{0,2}) = 0.0406268\ldots$, and $u_{0,3} = \omega\phi(Q_{0,3}) = 0.132031\ldots$. Observe that it is of no importance on which component each of the points $P_i$ and $Q_{0,i}$ is situated—as a matter of fact the points $P_2, P_4$ and $Q_{0,2}$ are on the compact component, while $P_1, P_3, Q_{0,1}, Q_{0,3}$ are on the infinite component. Further, for the relevant $i$, let

$$L(P) = \omega(\phi(Q_{0,i}) - \phi(P)) = u_{0,i} - m_0\omega - m_1u_1 - m_2u_2 - m_3u_3 - m_4u_4.$$

Then (9), (11) and (13) imply

$$|L(P)| < 0.360732\,\frac{1}{|V|}. \tag{14}$$

Now if $V \leq -9$ or $V \geq 3$, then $|X| > 1$, and hence, using $U = U(V)$, implicitly given by (2), it follows that

$$h(X(P)) \leq \log|11865U - 4817V - 31680| < 10.2544 + \log|V|. \tag{15}$$

It is important to realize that at this point we need the fact that $U$ and $V$ are integers.

Finally we have

$$\hat{h}(P) \geq c_1M^2. \tag{16}$$

Recall that $c_1 = 0.259202$.

Putting it all together, by (14), (15), (7) and (16), provided $V \leq -17$ or $V \geq 8$, we deduce

$$|L(P)| < \exp(19.5267 - 0.518404M^2). \tag{17}$$

At this point we apply DAVID'S result [3] to the linear form in elliptic logarithms $L(P)$. Observe that $\omega\phi(P_i)$ and $\omega\phi(Q_{0,i})$ are indeed elliptic logarithms, though the $(X,Y)$-coordinates of these points are in a field of degree 9. We thus obtain

$$|L(P)| > \exp\left(-c_4(\log(4M)+c_5)(\log\log(4M)+c_6)^7\right).$$

The computed values of the constants are: $c_4 = 1.13604\cdots\times 10^{225}$, $c_5 = 1+\log 9$, $c_6 = c_5 + 31.7227\ldots$. Combined with (17) David's inequality yields an absolute upper bound $M_0 = 3.32250\times 10^{119}$ for $M$.

In order to complete the solution process we have to determine the solutions below this very large bound. To achieve this, we use several rounds of the reduction procedure based on the LLL-algorithm (see [16]). Let $C$ be a large number, to be chosen later. Consider the lattice spanned by the columns of

$$\mathcal{A} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ [Cu_1] & [Cu_2] & [Cu_3] & [Cu_4] & [C\omega] \end{pmatrix}.$$

The point $\boldsymbol{y} = (0,0,0,0,[Cu_0])^\top$ is not a lattice point, because $Q_0$ is not a rational point. Using the LLL-algorithm we compute $d = \min_{\boldsymbol{x}} |\mathcal{A}\boldsymbol{x} - \boldsymbol{y}|$. Now let $m_0, m_1, m_2, m_3, m_4$ be a solution of (17) with $M \le M_0$, and consider the lattice point

$$\mathcal{A}(m_1, m_2, m_3, m_4, m_0)^\top = (m_1, m_2, m_3, m_4, \lambda)^\top.$$

On the one hand, by the very definition of $d$, this point satisfies

$$d^2 \le m_1^2 + m_2^2 + m_3^2 + m_4^2 + \lambda^2 \le 4M_0^2 + \lambda^2, \tag{18}$$

and on the other hand, by the definition of $\lambda$ as an approximation to $CL(P)$, we also have

$$|\lambda - CL(P)| \le \tfrac{1}{2}(|m_1|+|m_2|+|m_3|+|m_4|+|m_0|+1) \le 4M_0 + \tfrac{1}{2}. \tag{19}$$

Thus, combining the inequalities (17), (18) and (19), we arrive at a reduced upper bound $M_1$ for $M$ of the following shape.

$$M_1 = \left\lfloor \sqrt{\frac{1}{2c_1}\left(\log C + 19.5267 - \log\left(\sqrt{d^2 - 4M_0^2} - (4M_0 + \tfrac{1}{2})\right)\right)} \right\rfloor.$$

Clearly, $M_1$ only makes sense if $d > \sqrt{20M_0^2 + 4M_0 + \frac{1}{4}}$. By heuristic argument, we expect a lattice of dimension dim and determinant det to have $d \approx \det^{1/\dim}$. Therefore, in the present case $d \approx C^{1/5}$. This means we should take $C \approx M_0^5$, and large enough. The reduced bound can then be expected to be $M_1 \approx \sqrt{\log C} \approx \sqrt{\log M_0}$.

Starting up with $C = 10^{608}$, the reduction process gives $d = 1.34075 \cdots \times 10^{121}$, which leads to $M_1 = 46$. We can now replace $M_0$ by $M_1$, i.e. we take $M_0 = 46$, and repeat the procedure. With $C = 10^{14}$ we obtain $d = 301.925\ldots$ and $M_1 = 9$. Yet another reduction round, with $C = 10^{10}$, yields $d = 49.3862\ldots$ and $M_1 = 8$. It is quite straightforward to retrieve all solutions that satisfy this final reduced bound of 8 for $M$. It is worth noting that the $m_i$-values never exceed 2.

It may be of interest to give an impression of the computation times. We must emphasize however that we never tried to optimize these by cleverly choosing our software code; we took the available programs and only adapted them where necessary to fit our purpose. With mrank it took approximately 26 minutes and 7 seconds on a Sun Sparcstation 4 to compute the rank, findinf used about 16 seconds on the same machine to find the points of small height, the Siksek sieving used about 0.9 seconds on a Pentium 75 PC. This Pentium needed 2.3 seconds to find an optimal $c_1$-basis, and Pari 1.39.03 used about 11 minutes and 24 seconds for the reduction procedure. Finally Apecs 4.2 under Maple V.4 used about 50 minutes and 38 seconds on our Pentium 75 to find the small solutions. We have no doubt that as a result of continuous software improvements, these computation times may be considerably reduced by the time you read this.

## References


1. I. Connell, *Elliptic Curve Handbook*, available from the ftp site of McGill University in the directory math.mcgill.ca/pub/ECH1. From the same site the Apecs package can be downloaded.
2. J.E. Cremona, 1992, *Algorithms for modular elliptic curves*, Cambridge Un. Press. The programs mrank, mwrank, findinf may be downloaded from John Cremona's ftp site euclid.ex.ac.uk/pub/cremona.
3. S. David, 1995, Minorations de formes linéaires de logarithmes elliptiques. *Mémoires Soc. Math. France (N.S)*, **62**, iv + 143 pp.
4. Persi Diaconis and R.L. Graham, 1985, The Radon transform on $\mathbb{Z}_2^k$. *Pacific J. Math.* **118**(2), 323–345.
5. Laurent Habsieger and Dennis Stanton, 1993, More zeros of Krawtchouk polynomials. *Graphs and Combinatorics* **9**, 163–172.
6. G. Hanrot, 1997, *Résolution effective d'équations diophantiennes: algorithmes et applications*, Thèse, Université Bordeaux 1.
7. Ilia Krasikov and Simon Litsyn, 1996, On integral zeros of Krawtchouk polynomials. *J. Comb. Theory* Ser. A **74**, 71–99.
8. M. Mignotte and A. Pethő, 1995, On the system of diophantine equations $x^2 - 6y^2 = -5$ and $x = 2z^2 - 1$. *Math. Scand.* **76**, 50–60.
9. J.H. Silverman, 1990, The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.* **55**, 723–743.
10. Samir Siksek, 1995, Infinite descent on elliptic curves. *Rocky Mountain J. Math.* **25**, 1501–1538.
11. R.J. Stroeker and N. Tzanakis, 1994, Solving elliptic diophantine equa-

tions by estimating linear forms in elliptic logarithms. *Acta Arith.* **67**, 177–196.
12. R.J. STROEKER and N. TZANAKIS, On the elliptic logarithm method for elliptic diophantine equations: Reflections and an improvement, to appear in *Experimental Math.*
13. R.J. STROEKER and B.M.M. DE WEGER, 1996, On a quartic diophantine equation. *Proc. Edinburgh Math. Soc* **39** (1996), 97–114.
14. R.J. STROEKER and B.M.M. DE WEGER, Solving elliptic diophantine equations: the general cubic case, Forthcoming.
15. N. TZANAKIS, 1996, Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations. *Acta Arith.* **75**, 165–190.
16. B.M.M. DE WEGER, 1989, Algorithms for Diophantine equations, CWI Tract 65, Stichting Mathematisch Centrum, Amsterdam.
17. D. ZAGIER, 1987, Large integral points on elliptic curves. *Math. Comp.* **48**, 425–436.