Solving Elliptic Diophantine Equations: The General Cubic Case

Roelof J. Stroeker* Benjamin M.M. de Weger†

Abstract

In this paper we consider binary cubic diophantine equations of every form and shape, solely subjected to the requirement that they represent elliptic curves defined over $\mathbb{Q}$. How to deal with standard Weierstraß equations is well understood, but comparatively little is known about elliptic equations of different type. We give a detailed analysis of the general situation and subsequently apply the elliptic logarithm method to a variety of unusual elliptic equations, notably to some equations directly related to Krawtchouk polynomials.

1991 *Mathematics subject classification:* 11D25, 11G05, 11Y50, 12D10
Key words and phrases: cubic diophantine equation, elliptic curve, elliptic logarithm, LLL-reduction, binary Krawtchouk polynomial

---

*Econometric Institute, Erasmus University, P.O.Box 1738, 3000 DR Rotterdam, The Netherlands, e-mail: stroeker@few.eur.nl, internet URL of my homepage: http://www.few.eur.nl/few/people/stroeker/

†Sportsingel 30, 2924 XN Krimpen aan den IJssel, The Netherlands, e-mail: deweger@xs4all.nl; this author's research was supported by the Netherlands Mathematical Research Foundation SWON with financial aid from the Netherlands Organization for Scientific Research NWO.

Introduction

In recent years the explicit computation of integer points on special models of elliptic curves received quite a bit of attention, and many papers were published on the subject (see for instance [ST94], [GPZ94], [Sm94], [St95], [Tz96], [BST97], [SdW97], [ST97]).

The overall picture before 1994 was that of a field with many individual results but lacking a comprehensive approach to effectively settle the elliptic equation problem in some generality. But after S. David obtained an explicit lower bound for linear forms in elliptic logarithms (cf. [D95]), the elliptic logarithm method, independently developed in [ST94] and [GPZ94] and based upon David's result, provided a more generally applicable approach for solving elliptic equations. First Weierstraß equations were tackled (see [ST94], [Sm94], [St95], [BST97]), then in [Tz96] Tzanakis considered quartic models and in [SdW97] the authors gave an example of an unusual cubic non-Weierstraß model. In the present paper we shall treat the general case of a cubic diophantine equation in two variables, representing an elliptic curve over $\mathbb{Q}$. We are thus interested in the diophantine equation

$$f(u,v) = 0 \tag{1}$$

in rational integers u, v, where $f \in \mathbb{Q}[x, y]$ is of degree 3. Moreover, we require (1) to represent an elliptic curve E, that is a curve of genus 1 with at least one rational point (u_0, v_0).

C. Siegel showed in [Sie29] that equation (1) can have at most finitely many solutions, but his method of proof is ineffective. A. Baker and J. Coates offered an effective proof for Siegel's result in [BC70]. In fact they gave the following explicit upper bound for the solutions in terms of the height of the polynomial f:

$$\max\{|u|, |v|\} < \exp\exp\exp\left((2H)^{10^{3^{10}}}\right). \tag{2}$$

Here H is an upper bound for the height of f, or, in other words, for the absolute values of the numerators and denominators of f's coefficients. This bound (2) was improved by W.M. Schmidt in [Sch92] to

$$\max\{|u|, |v|\} < \exp\left(cH^{12^{13}}\right), \tag{3}$$

where c is an effective, but unspecified constant.

Although (2) and (3) are effective, they are obviously unattainable, even for small values of H. Without the use of an extremely powerful reduction process, it is clearly impossible to construct a practical algorithm on the basis of these astronomical upper bounds. Only in special cases efficient computational methods are known. For instance, for individual Thue equations

$$f(x, y) = m,$$

where $f \in \mathbb{Z}[x, y]$ is homogeneous of degree 3 and $m \in \mathbb{Z}$ ($m \neq 0$), and equations

$$y^k = F(x), \tag{4}$$

with $F \in \mathbb{Q}[x]$ of degree 3 and $k = 2$, there are the Thue method (see [TdW89]), the Bilu-Hanrot technique [BH96], and the elliptic logarithm approach which provide efficient tools for their solution. Also the superelliptic equations (4) with $k = 3$ have been succesfully tackled by the Thue method and by Bilu-Hanrot [BH98].

In this paper we shall adapt the elliptic logarithm method as described in [ST94] and [Tz96] to fit our purpose, that is to say, to conform to the general cubic diophantine equation (1). We claim that this approach provides a practical, often efficient tool for the solution of binary equations of the general cubic type.

Part I

The general cubic equation

1 Equations of shifted Weierstraß type

The elliptic logarithm method has been successfully applied to the general Weierstraß equation. For fear of repetition, we shall therefore pay little attention to those elliptic equations (1) that are in a sense close to the general Weierstraß form. By this we mean those equations for which the Weierstraß treatment (see [ST94]) or a slight adaptation thereof would furnish a complete solution. Below we shall give a characterization of those equations for which the standard procedure will suffice. We shall call these equations of shifted Weierstraß type.

On replacing u by $u + u_0$ and v by $v + v_0$ in (1), we may assume that the rational point is $P = (0, 0)$. Hence in (1) we may take

$$\begin{aligned} f(u, v) &= s_1 u^3 + s_2 u^2 v + s_3 u v^2 + s_4 v^3 + s_5 u^2 + s_6 uv + s_7 v^2 + s_8 u + s_9 v \\ &= f_3(u, v) + f_2(u, v) + f_1(u, v), \end{aligned} \tag{5}$$

with $s_i \in \mathbb{Z}$ for $i = 1, \ldots, 9$ and suitable binary forms f_j of degree j ($j = 1, 2, 3$). In case both s_8 and s_9 vanish, P is a singular point so that E is not elliptic. Therefore, at least one of s_8, s_9 is non-zero. Setting $u = U/W$, $v = V/W$ and multiplying through by W^3 transforms (1), subject to (5), into the homogeneous equation

$$f_3(U, V) + f_2(U, V)W + f_1(U, V)W^2 = 0. \tag{6}$$

We shall now show that for (6) to be of shifted Weierstraß type, we may assume that the infinite line $W = 0$ is not tangent to the curve in the projective plane. To prove this, suppose it is. The cubic form $f_3(U, V)$ will then have a double or threefold linear factor. This factor must necessarily be rational. Therefore, after a suitable rational linear substitution, we have $s_3 = s_4 = 0$ (or $s_1 = s_2 = 0$, which can be treated analogously). Then $s_7 \neq 0$, for otherwise our curve is rational, not elliptic. Further, if $s_2 = 0$, then (6) is a homogeneous Weierstraß model and we are done. On the other hand, if s_2 does not vanish, then $s_1 u^3$ may be absorbed into $s_2 u^2 v$ by a rational linear substitution, so that without loss of generality we may assume $s_1 = 0$. Equation (1) can now be transformed into the Weierstraß equation

$$Y^2 = X^3 + (s_6^2 - 4s_5 s_7 - 4s_2 s_9)X^2 + 8s_2 s_7(2s_5 s_9 - s_6 s_8)X + (4s_2 s_7 s_8)^2, \tag{7}$$

by the rational transformation

$$X = -4s_2 s_7 v, \quad Y = 4s_2 s_7(2s_2 uv + 2s_5 u + s_6 v + s_8),$$

as may be readily checked.

For an integral solution (u, v) of (1), the corresponding solution (X, Y) of (7) is integral and can therefore be recovered by the standard elliptic logarithm approach of [ST94]. As we have used only linear substitutions, all solutions (u, v) of (1), subject to (5) and also to the restrictions imposed by the choices of coefficients s_i, can be recovered from the integer solution (X, Y) of (7). This proves our point: those curves (6) to which the line $W = 0$ is tangent can be readily dismissed. From this point onwards, we shall therefore focus our attention on equations corresponding to curves that do not have this property.

2 Nagell's algorithm

We shall need to find birational transformations that link the general cubic equation (1) to a Weierstraß model, provided (1) represents an elliptic curve E over $\mathbb{Q}$ and a point $(u_0, v_0) \in \mathbb{Q}^2$ on (1) is known. In [N28] T. Nagell gives precisely such an algorithm. Here we shall follow Connell's description of Nagell's algorithm (see section 1.4 of [Co97]).

Consider (5) and the conditions imposed on the coefficients s_i, and further assume $s_9 \neq 0$. Next set $e_i = f_i(s_9, -s_8)$ for $i = 2, 3$. The tangent to the curve given by (6) at P is $f_1(U, V) = 0$ and this line meets the curve in a third point Q with projective coordinates $(-e_2 s_9, e_2 s_8, e_3)$. Naturally, e_2 and e_3 cannot both vanish, but if $e_2 = 0$ then $Q = P$ and if $e_3 = 0$ then Q is at infinity. The following changes of coordinates send Q to the origin $(0, 0, 1)$:

$$\begin{array}{llll} U = U' - s_9 \dfrac{e_2}{e_3} W', & V = V' + s_8 \dfrac{e_2}{e_3} W', & W = W', & \text{if } e_3 \neq 0 \text{ and} \\ U = U' - s_9 W', & V = V' + s_8 W', & W = U', & \text{if } e_3 = 0. \end{array}$$

Resetting $u' = U'/W'$, $v' = V'/W'$ returns the following equation in affine coordinates (u', v'):

$$f_3'(u', v') + f_2'(u', v') + f_1'(u', v') = 0, \tag{8}$$

where f'_i is a suitable binary form of degree i for $i = 1, 2, 3$. On writing

$$t = \frac{u'}{v'}, \quad \phi_i = f'_i(1, t) \quad (i = 1, 2, 3)$$

equation (8) takes the form

$$\phi_3 {u'}^2 + \phi_2 u' + \phi_1 = 0.$$

It is readily verified that $\delta = \phi_2^2 - 4\phi_1\phi_3$ is a polynomial of degree 4 in t with rational coefficients. By definition, the values of t are the slopes of the lines in the (u', v')-plane passing through the origin. Therefore, the t-values corresponding to the tangents to the curve which pass through the origin are precisely the zeroes of δ as a polynomial in t. Now $t_0 = -s_8/s_9$ is the slope of the tangent at P through the origin and hence $t - t_0$ is a rational factor of δ. Setting $\tau = (t - t_0)^{-1}$, it follows that $\tau^4\delta$ is a cubic polynomial in τ, say

$$\tau^4\delta = c\tau^3 + d\tau^2 + e\tau + k.$$

Then $c \neq 0$, for otherwise the original curve is not elliptic. Finally, put

$$x = c\tau \quad \text{and} \quad y = \pm c\tau^2\sqrt{\delta}.$$

Then for any rational point (u', v') on (8), the corresponding point (x, y) is a rational point on the Weierstraß model

$$y^2 = x^3 + dx^2 + cex + c^2k. \tag{9}$$

The birational equivalence between equation (1), subject to (5), and the Weierstraß equation (9) is given in the following lemma.

Lemma 1. *Let f be given by* (5) *with $s_9 \neq 0$, $e_i = f_i(s_9, -s_8)$ $(i = 2, 3)$, and such that $f(u, v) = 0$ represents an elliptic curve E over $\mathbb{Q}$. Then $E/\mathbb{Q}$ is also represented by the Weierstraß equation* (9)*, and birational transformations are given by*

$$x = cs_9 \frac{u + s_9\frac{e_2}{e_3}}{s_8u + s_9v}, \quad y = cs_9^2 \frac{(u + s_9\frac{e_2}{e_3})\frac{\partial f}{\partial u} + (v - s_8\frac{e_2}{e_3})\frac{\partial f}{\partial v}}{(s_8u + s_9v)^2}, \quad \textit{in case } e_3 \neq 0,$$

$$x = cs_9 \frac{1}{s_8u + s_9v}, \quad y = cs_9^2 \frac{s_9\frac{\partial f}{\partial u} - s_8\frac{\partial f}{\partial v}}{(s_8u + s_9v)^2}, \quad \textit{in case } e_3 = 0.$$

Note that the constant c is merely a scaling factor making both coefficients of x^3 and y^2 in (9) *match unity.*

Proof. The proof is straightforward and closely follows the steps in Nagell's algorithm. Because of Euler's theorem on homogeneous functions, we observe that

$$u'\frac{\partial f'}{\partial u'} + v'\frac{\partial f'}{\partial v'} = 3f'_3 + 2f'_2 + f'_1 = f'_2 + 2f'_3 = {u'}^2(\phi_2 + 2\phi_3 u') = \pm {u'}^2\sqrt{\delta}.$$

Further, $f(u,v) = f'(u',v')$ in case $e_3 \neq 0$, and $u'^3 f(u,v) = f'(u',v')$ when $e_3 = 0$, which implies that

$$\pm u'^2\sqrt{\delta} = \begin{cases} u'\dfrac{\partial f}{\partial u} + v'\dfrac{\partial f}{\partial v} & \text{when } e_3 \neq 0, \\ u'^2\left(s_9\dfrac{\partial f}{\partial u} - s_8\dfrac{\partial f}{\partial v}\right) & \text{when } e_3 = 0. \end{cases}$$

Now the transformation formulas immediately follow. □

If so required, the Weierstraß model (9) can be birationally transformed into a global minimal model

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{10}$$

with integral coefficients a_i by means of a transformation of the form

$$\begin{aligned} x &= \mathcal{U}^2X + \mathcal{V} \\ y &= \mathcal{U}^3Y + \mathcal{W}\mathcal{U}^2X + \mathcal{Z} \end{aligned}$$

for suitable integers $\mathcal{U}, \mathcal{V}, \mathcal{W}$ and $\mathcal{Z}$.

3 Elliptic logarithms

In order to bring our analysis of the general situation to a successful conclusion, we have to understand which elements of the standard elliptic logarithm method need adjusting to fit the general cubic equation (1), subject to (5). Now the general principle of this method and how it works in individual Weierstraß cases has been fully exposed in the literature. As there is no point repeating this, we shall merely focus on those aspects in which our treatment necessarily must diverge from the main course. Starting point is the exposition given in [ST94].

As the method is based on estimating elliptic logarithms, we shall briefly introduce them here.
Let the elliptic curve $E/\mathbb{Q}$ be given by the short Weierstraß model

$$y^2 = x^3 + Ax + B, \quad \text{with } A, B \in \mathbb{Z}. \tag{11}$$

The group $E(\mathbb{C})$ of points with coordinates in $\mathbb{C}$ is isomorphic to $\mathbb{C}/\Lambda$, where $\Lambda = \omega_1\mathbb{Z}+\omega_2\mathbb{Z}$ is a lattice with primitive periods ω_1 and ω_2, with $\mathrm{Im}(\omega_2/\omega_1) > 0$. We shall take $\omega = \omega_1$ to be real and ω_2 to be purely imaginary.
The isomorphism

$$\mathbb{C}/\Lambda \to E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$$

is given by the parameterization of E over $\mathbb{C}$ by the Weierstraß $\wp$-function relative to the lattice Λ and (11):

$$z \mapsto P = [\wp(z), \wp'(z), 1].$$

The inverse of this map is provided by the elliptic integral

$$u(P) = \int_{\mathcal{O}}^{P} \frac{\mathrm{d}z}{\sqrt{z^3 + Az + B}} \qquad (\mathrm{mod}\ \Lambda),$$

which is just the elliptic logarithm of the point P. Here $\mathcal{O}$ is the group identity.

As we are only interested in real points P, we are only concerned with $E(\mathbb{R})$. Now depending on the number of real zeroes of $x^3 + Ax + B$, the group $E(\mathbb{R})$ has either one or two components. In case $E(\mathbb{R})$ has a single component, we have $u(P) = \omega\phi(P)$ for $P \in E(\mathbb{R})$, where the function ϕ is as given in [ST94]. In order to calculate $u's$ values we use Zagier's algorithm, based on

$$\phi(P) = \sum_{i=0}^{\infty} c_i 2^{-i-1}, \quad \text{where} \quad c_i = \begin{cases} 0 & \text{if } y(2^i P) \geq 0 \text{ or } 2^i P = \mathcal{O} \\ 1 & \text{if } y(2^i P) < 0 \end{cases} \tag{12}$$

for $P = (x(P), y(P))$ on (11). On the other hand, if $x^3 + Ax + B = 0$ has three real roots $\gamma_1 < \gamma_2 < \gamma_3$, the group $E(\mathbb{R})$ has two components

$$\begin{aligned} E_0(\mathbb{R}) &= \{P \in E(\mathbb{R}) \mid x(P) \geq \gamma_3\}, \\ E_{\mathrm{C}}(\mathbb{R}) &= \{P \in E(\mathbb{R}) \mid \gamma_1 \leq x(P) \leq \gamma_2\}. \end{aligned}$$

Note that the 2-torsion points $T_i := (\gamma_i, 0)$ are not necessarily rational. Further

$$\begin{aligned} &u : E_0(\mathbb{R}) \to [0, \omega), & &u(\mathcal{O}) = 0, & &u(T_3) = \frac{1}{2}\omega, \\ &u : E_{\mathrm{C}}(\mathbb{R}) \to [0, \omega) + \frac{1}{2}\omega_2, & &u(T_1) = \frac{1}{2}\omega_2, & &u(T_2) = \frac{1}{2}\omega + \frac{1}{2}\omega_2. \end{aligned}$$

Now we define $\phi : E(\mathbb{R}) \to [0, 1)$, for points in $E_0(\mathbb{R})$ as well as in $E_{\mathrm{C}}(\mathbb{R})$, as $\phi(\mathcal{O}) = \phi(T_2) = 0$, $\phi(T_1) = \phi(T_3) = \frac{1}{2}$ and otherwise as in (12). Then for $P \in E_{\mathrm{C}}(\mathbb{R})$ we have

$$u(P) = \omega\phi(P) + \mathrm{sign}(y(P))\frac{1}{2}\omega + \frac{1}{2}\omega_2.$$

It follows that $\phi(P) = \phi(P + T_2)$, which incidently coincides with Tzanakis' approach in [Tz96]. Note that our ϕ-function is linear (modulo 1).
Summarizing, we can express the ϕ function in terms of an elliptic integral as follows:

$$\phi(P) = \mathrm{sign}(y(P))\frac{1}{\omega} \int_{x(P)}^{D} \frac{\mathrm{d}t}{\sqrt{t^3 + At + B}} \quad (\mathrm{mod}\ 1), \tag{13}$$

where

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

4 The asymptotes

We return to the affine curve (1), subject to (5), and we assume that the infinite line is not tangent to the curve. In other words, we only consider equations that are not of Weierstraß or shifted Weierstraß type. For any point $(u,v) \in \mathbb{Q}^2$ on this curve, Nagell's algorithm (see Lemma 1) tells us that the corresponding point (X,Y) on its global minimal Weierstraß model (10) satisfies

$$X = \frac{\sigma_1 u + \sigma_2 v + \sigma_3}{\rho_1 u + \rho_2 v} \tag{14}$$

for $\sigma_1, \sigma_2, \sigma_3, \rho_1, \rho_2 \in \mathbb{Z}$. Every reasonably sized bounded part of the (u,v)-plane, like a rectangle centered around the origin, can be directly screened for integral points without much effort. When traversing the curve moving outward, away from the origin, we must be able to identify the corresponding track in the (X,Y)-plane. In order to do so, we proceed in the following way.

Let $\alpha \in \mathbb{R}$ be a root of the equation

$$f_3(1,t) = s_1 + s_2 t + s_3 t^2 + s_4 t^3 = 0.$$

We include $\alpha = \infty$ in case $f_3(0,1) = 0$, that is when $s_4 = 0$. There is at least one such α and there are at most three. Obviously, these α's can be interpreted as the asymptotic directions of the curve in the (u,v)-plane. Because of our assumption excluding Weierstraß-type equations, it is easily seen that the expression $\frac{\partial f_3}{\partial v}(1,\alpha)$ does not vanish for $\alpha \in \mathbb{R}$, and neither does $\frac{\partial f_3}{\partial u}(0,1)$ in case $\alpha = \infty$. This means that the graph of (1) has as many asymptotes as there are α's, that is one or three; two cannot occur, because for $s_4 = 0$, $s_3 \neq 0$ which gives either none or two finite α's in addition to the infinite one. These asymptotes are

$$\begin{array}{lll} v = \alpha u + \beta, & \text{where } \beta = -\dfrac{f_2(1,\alpha)}{\frac{\partial f_3}{\partial v}(1,\alpha)} = -\dfrac{s_5 + s_6\alpha + s_7\alpha^2}{s_2 + 2s_3\alpha + 3s_4\alpha^2} & (\alpha \in \mathbb{R}), \\ u = \gamma, & \text{where } \gamma = -\dfrac{f_2(0,1)}{\frac{\partial f_3}{\partial u}(0,1)} = -\dfrac{s_7}{s_3} & (\alpha = \infty). \end{array}$$

Moving away from a suitably chosen rectangle, a point (u,v) travels along the graph close to one of the (two or six) half-asymptotes. We therefore need to inspect the half-asymptotes separately, unless symmetry considerations make a shortcut possible. Hence, positive lower bounds u_ℓ and v_ℓ exist such that in the vicinity of each half-asymptote, if $|u| > u_\ell$ and $|v| > v_\ell$, then equation $f(u,v) = 0$ implicitly gives u as a function of v. Obviously, constants δ_1, δ_2 can then be computed such that

$$\alpha u + \delta_1 < v < \alpha u + \delta_2,$$

if the said half-asymptote has direction α, and provided $|u| > u_\ell$ and $|v| > v_\ell$. In case $\alpha = \infty$, this has to be read as

$$\delta_1 < u < \delta_2.$$

All this enables us, in view of (14), to give an estimate for the naive height $h(X(P))$—which is the absolute logarithmic height of $X(P)$—of the point $P = (X(P), Y(P))$ satisfying (10), where the corresponding integral point $P = (u, v) \in \mathbb{Z}^2$ is close to one of the six half-asymptotes. The said estimate is of type

$$h(X(P)) \leq \text{constant} + \log |v|. \tag{15}$$

Here it is essential that (u, v) is an integral point.
Now if (u, v) tends to infinity along the graph close to a given half-asymptote of direction α, then the corresponding (X, Y) tends to $Q_0 = (X_0, Y_0)$, where

$$X_0 = X_0(\alpha) = \lim_{(u,v)\to\infty} \frac{\sigma_1 u + \sigma_2 v + \sigma_3}{\rho_1 u + \rho_2 v} = \begin{cases} \dfrac{\sigma_1 + \sigma_2\alpha}{\rho_1 + \rho_2\alpha}, & \text{if } \alpha \in \mathbb{R}, \\ \dfrac{\sigma_2}{\rho_2}, & \text{if } \alpha = \infty. \end{cases} \tag{16}$$

5 Putting it all together

We are now closing in on the required upper bound for the linear form in elliptic logarithms. But first we need to study the relation between the differential forms given by the different representations of E.

Lemma 2. *Considering the three representations of E given by* (1), (9), (10), *we have*

$$s\frac{\mathrm{d}v}{\frac{\partial f}{\partial u}} = -\frac{\mathrm{d}x}{y} = -\frac{2}{\mathfrak{U}}\frac{\mathrm{d}X}{2Y + a_1X + a_3},$$

where $s = 1$ if $e_3 \neq 0$ and $s = s_9^{-1}$ otherwise.

Proof. The latter relation is trivial. Consider the birational transformations given in Lemma 1. The first relation is an immediate consequence of the identities

$$\mathrm{d}x = \frac{\partial x}{\partial u}\mathrm{d}u + \frac{\partial x}{\partial v}\mathrm{d}v, \quad \text{and} \quad \mathrm{d}f = \frac{\partial f}{\partial u}\mathrm{d}u + \frac{\partial f}{\partial v}\mathrm{d}v = 0.$$

□

Now let $P = (u, v)$ be an integral point on (1) in the vicinity of one of the two half-asymptotes associated with the asymptotic direction α. There is no loss of generality assuming that $v \in [v_\ell, \infty)$—a restriction of type $v \geq v_\ell$ is necessary to ensure that the transformation $[v, \infty) \to [X(P), X_0]$ is bijective. Note that $X(P)$ and $Y(P)$ are the coordinates of P relative to (10).
From Lemma 2 and the discussion of the previous section, we deduce that

$$-s\int_v^\infty \frac{\mathrm{d}v}{\frac{\partial f}{\partial u}} = \frac{2}{\mathfrak{U}}\int_{X(P)}^{X_0} \frac{\mathrm{d}X}{2Y + a_1X + a_3}. \tag{17}$$

Observe that we always need to work with points P and Q_0 close together on the same component of $E(\mathbb{R})$. This means that their difference $P-Q_0$ is on the infinite component $E_0(\mathbb{R})$ and therefore $u(P)-u(Q_0)=\omega\phi(P)-\omega\phi(Q_0)$ is real. Working out the right-hand side of (17) yields (an obvious adjustment is needed in (13) to fit the minimal Weierstraß equation (10))

$$\frac{2}{|\mathfrak{U}|}\left|\int_{X(P)}^{X_0}\frac{\mathrm{d}X}{2Y+a_1X+a_3}\right|=|\omega\phi(P)-\omega\phi(Q_0)|=|u(P)-u(Q_0)|, \tag{18}$$

where the left-hand side of (17) gives

$$\left| s\int_v^{\infty}\frac{\mathrm{d}v}{\frac{\partial f}{\partial u}}\right| \leq \text{constant}\times|v|^{-1}, \tag{19}$$

because solving (1) explicitly for $u=u(v)$, while $v>v_\ell$ yields

$$\left|\frac{\partial f}{\partial u}(u(v),v)\right|\geq \text{constant}\times v^2.$$

Now let r be the rank of E, and let $\{P_1,\ldots,P_r\}$ be a Mordell-Weil basis, so that

$$E(\mathbb{Q})=\mathbb{Z}^r\times E_{\text{tors}}(\mathbb{Q}).$$

Then

$$P=\sum_{i=1}^r m_iP_i+T$$

for integers m_i $(i=1,\ldots,r)$ and general torsion point $T\in E_{\text{tors}}(\mathbb{Q})$. Hence

$$\phi(P)=\sum_{i=1}^r m_i\phi(P_i)+\phi(T)+m_0,$$

where $m_0\in\mathbb{Z}$ is chosen so that all ϕ-values belong to the interval $[0,1)$. By Mazur's theorem, $\phi(T)=r/s$ with $s,t\in\mathbb{Z}$, $0\leq s<t$ and $t\leq 12$. It then follows that $|m_0|\leq rM+1$ where $M:=\max_{1\leq i\leq r}|m_i|$. Setting $u_0:=\omega Q_0$, and $u_i:=\omega\phi(P_i)$ for $i=1,\ldots,r$, we have to estimate the following linear form in elliptic logarithms:

$$L(P):=\omega\phi(P)-\omega\phi(Q_0)=(m_0+\frac{r}{s})\omega+\sum_{i=1}^r m_iu_i-u_0. \tag{20}$$

By (17), (18) and (19) it follows that

$$|\ L(P)\ |<\text{constant}\times\frac{1}{|v|}, \tag{21}$$

which, together with (15), ultimately yields an upper bound

$$\mid L(P) \mid \leq \exp(c_2 - 2c_1 M^2) \tag{22}$$

for computable positive constants c_1 and c_2. Here we used Silverman's inequality [Sil90, Theorem 1.1]:

$$\hat{h}(P) - \tfrac{1}{2}h(X(P)) < \text{constant},$$

and

$$\hat{h}(P) \geq c_1 M^2,$$

where c_1 is the least eigenvalue of the Néron-Tate height pairing matrix. We refer to [ST94], and [Tz96] for the details.

In combination with David's lower bound for $|L(P)|$, an absolute upper bound for M is obtained, and after a few LLL-reduction rounds this very large upper bound is reduced to workable proportions. The resulting search region is usually small enough to make a brute force search for integral points feasible.

It should be noted that the main contribution of this paper is the demonstration that inequalities like (21) and (15) exist not only for equations of Weierstraß and shifted Weierstraß type but also for cubic equations of different shape. After these inequalities have been established, what remains to be done in order to complete the process of computing all integral points of individual cubic equations by means of the elliptic logarithm method, is not essentially different from the work needed for Weierstraß type equations.

Part II

Examples

In the previous sections we have distinguished between two different categories of cubic elliptic equations (1) by certain properties of their associated projective curve.

1. **Weierstraß or shifted Weierstraß type**. By definition, the infinite line $W = 0$ is tangent to the curve in the projective (U, V, W)-plane.
   This category can be subdivided into two subcategories:

   (a) True Weierstraß curves

   (b) Cubic curves with a single asymptote

2. **Non Weierstraß type**. The infinite line is not tangent to the projective curve.
   This category can also be subdivided into two parts:

   (a) Cubic curves with one asymptote

(b) Cubic curves with three asymptotes

The category of Weierstraß or shifted Weierstraß type equations is less interesting for our purpose because these equations can usually be solved in a variety of ways. We shall only give an example illustrating the second subcategory. The most interesting examples are those of cubic equations belonging to the second main category. The reason is that for these equations we not do see any other approach towards complete solution than by the elliptic logarithm method.

6 Equations of shifted Weierstraß type

The true Weierstraß equation can generally be solved by the elliptic logarithm method. There are very many examples available in the literature. See for instance [ST94], [GPZ94], [Sm94], [St95], [BST97], [SdW97], [ST97], and [HP98].
The following example only serves to illustrate the case of shifted Weierstraß equations, that are not of Weierstraß type.

6.1 Examples 1(b)

For non-zero $k \in \mathbb{Z}$ the equation

$$u^2 v = 2kv^2 + u$$

is a shifted Weierstraß equation. Indeed, the integral substitutions

$$X = 2kv, Y = k(2uv - 1)$$

(see (7)) give the well-known Mordell curve

$$Y^2 = X^3 + k^2.$$

The graph of (1) in the (u, v)-plane has a single asymptote, namely $v = 0$. All integral solutions can be immediately retrieved from those of the corresponding Mordell equation. For more information see [GPZ97].

7 Non Weierstraß type equations

In this main category we have chosen nine examples, of which seven result from a binomial equation and two come from Krawtchouk polynomials; all of these equations except one have not been solved before, at least not to our knowledge. The details are often quite tedious, but the solution processes are very similar, and therefore we have selected two equations most representative for the two subcategories, and of these equations full details are offered. The other seven equations are merely mentioned and their complete solution sets are presented; more detailed information is rarely given. Full details of all equations and their solution processes may be obtained from the authors.

7.1 Examples 2(a)

All curves associated with the equations of this section have a single asymptote.
The first example we wish to mention is the equation

$$15u^3 - 15u = v^3 - 4v^2 + 3v,$$

completely solved by us in [SdW97, Theorem B36] in the manner described. It comes from the binomial equation

$$\binom{n}{3} = \binom{m}{6}$$

in integers n and m. All integral solutions (u, v) of the cubic equation belong to either $\{-1, 0, 1\} \times \{0, 1, 3\}$ or $\{(2, 6), (8, 21)\}$.

Next consider the equation

$$u(u-1)(u+1) = \binom{m}{3}.$$

We claim that 120 is the only integer that can be expressed as the product of three consecutive integers and is at the same time of the form $\binom{m}{3}$ for an integer $m \geq 3$. In fact, the above equation has integral solutions $(u, m) \in \{-1, 0, 1\} \times \{0, 1, 2\}$ and $(u, m) = (-5, -8), (5, 10)$ and no others. On putting $v = m - 1$ it can be seen that this follows from the result below.

Theorem 1. *All integral solutions (u, v) of the diophantine equation*

$$6u^3 - 6u = v^3 - v \tag{23}$$

belong to the sets $\{-1, 0, 1\} \times \{-1, 0, 1\}$ or $\{(-5, -9), (5, 9)\}$.

We shall not give a proof of this result as the solution process does not really contain any surprising elements; by following the steps given in the previous sections the result follows more or less automatically. The rank of the associated elliptic curve is 2, and a Mordell-Weil basis is easily found. Moreover, the torsion subgroup of the Mordell-Weil group is trivial. A peculiarity of this example lies in the fact that Q_0 is a non-rational 2-torsion point. As a consequence, working with $2L(P)$ instead of $L(P)$ simplifies matters considerably, because doing so makes one term of the linear form disappear and this happens to be the only term that depends on a non-rational point. It also means that the linear form $2L(P)$ is homogeneous.

The next example is very similar but more involved. We shall give full details of the solution process.
We claim that 210 and 1716 are the only integers that can be expressed as a product of three consecutive integers and at the same time are of the form $\binom{m}{6}$ for a positive integer m. More precisely, if (u, m) is an integral solution of the diophantine equation

$$u(u-1)(u+1) = \binom{m}{6},$$

then $(u,m) \in \{-1,0,1\} \times \{0,1,2,3,4,5\}$ or $(u,m) \in \{(6,-5),(6,10),(12,-8),(12,13)\}$. On putting $v = \frac{1}{2}m^2 - \frac{5}{2}m + 3$, it can be seen that this is an immediate consequence of the following theorem.

Theorem 2. *If (u,v) is an integral solution of the diophantine equation*

$$90u^3 - 90u = v^3 - 4v^2 + 3v \tag{24}$$

then $(u,v) \in \{-1,0,1\} \times \{0,1,3\}$, or $(u,v) \in \{(6,28),(12,55)\}$.

Proof. The birational transformations

$$\begin{aligned} (u,v) &= \left(\frac{1299X + 40Y - 89500}{40X^2 + 40X - 301Y + 17980} \frac{9030X - 1200Y + 62970}{40X^2 + 40X - 301Y + 17980} \right), \\ (X,Y) &= \left(\frac{30u - 300v + 1200}{30u + v}, \frac{54000u^2 + 11980v^2 + 270900u - 38970v}{(30u+v)^2} \right) \end{aligned} \tag{25}$$

relate equation (24) to the minimal Weierstrass model

$$Y^2 = X^3 - 700X + 90100. \tag{26}$$

See Lemma 1 to verify these transformations. Connell's program Apecs ([Co97]) quickly gives the particulars of the curve represented by (26), in particular it shows that the torsion subgroup of its Mordell-Weil group is trivial. Cremona's program mrank ([Cr92]) tells us that the rank is 5, and it produces the five independent points $P_1 = (30, 310)$, $P_2 = (-20, 310)$, $P_3 = (-30, 290)$, $P_4 = (20, -290)$, and $P_5 = (46, -394)$—given here in (X,Y)-coordinates—with regulator $R = 31.0942\ldots$. Computing canonical heights we find $\hat{h}(P_3 - P_4) = 1.15985\ldots$, and we intend to show that there are no points P of canonical height below this value. This is achieved by assuming that such a point P does exist, which is subsequently proved contradictory. Silverman's and Siksek's bounds for the difference of heights on elliptic curves, as given by Apecs, are

$$-2.26871 < \hat{h}(P) - \tfrac{1}{2}h(X(P)) < 3.67558 \tag{27}$$

for any point P, so that $h(X(P)) < 6.91568$ for a point P with canonical height below 1.15985. With Cremona's findinf we searched for all such points, showing that if $h(X(P)) < 6.91568$ then either $P = \mathcal{O}$ or $\hat{h}(P) \geq \hat{h}(P_3 - P_4)$. Therefore we may take $\lambda = 1.26146$ in Siksek's upper bound for the index of the subgroup generated by $\{P_1, P_2, P_3, P_4, P_5\}$ of the Mordell-Weil group. This yields (see [Sik95, Theorem 3.1])

$$\text{index} \leq \sqrt{R}\, \frac{\sqrt{8}}{(2\lambda)^{5/2}} = 1.92\ldots.$$

Therefore the index must be 1, which proves that P_1, P_2, P_3, P_4, P_5 indeed form a basis for the Mordell-Weil group of $\mathbb{Q}$-rational points.

It is not difficult to show that this basis has an optimal value for the least eigenvalue of the

Néron-Tate height pairing matrix (see [ST97]), which equals $c_1 = 0.478212\ldots$. We shall need this number later.
From Lemma 2 (see also (25)) it follows that

$$\frac{\mathrm{d}v}{270u^2 - 90} = -\frac{1}{6}\frac{\mathrm{d}X}{Y}. \tag{28}$$

If $(u, v) \in \mathbb{R}^2$ on (24) is restricted by the inequalities $u \geq 1$ and $v \geq 3$ or $u \leq -1$ and $v \leq 0$, then u, implicitly given by (24), can be viewed as a strictly increasing function of v. For each such point (u, v) there is a unique point $(X, Y) \in \mathbb{R}^2$ on (26) with $Y \geq 0$, given by the transformation formula (25). Let $F : (-\infty, 0] \cup [3, \infty) \to \mathbb{R}$ be given by

$$F(v) = \frac{30u(v) - 300v + 1200}{30u(v) + v},$$

where $u(v) \in (-\infty, -1] \cup [1, \infty)$ is uniquely determined by (24) for the given v. Then $X = F(v)$. Let Q_0 be the image on (26) of the point at infinity on (24). Then by (25) $Q_0 = (X_0, Y_0)$, where

$$X_0 = \lim_{v\to\infty} F(v) = -10\alpha + \frac{1}{3}\alpha^2 = -38.1197\ldots \quad \text{and} \quad Y_0 = -20 + \frac{40}{3}\alpha^2 = 247.773\ldots,$$

with $\alpha = \sqrt[3]{90} = 4.48140\ldots$. Note that $Q_0 \in E(\mathbb{K})$, where $\mathbb{K} = \mathbb{Q}(\alpha)$ is a cubic field. Further, also note that $v = \alpha u + \frac{4}{3}$ is the asymptote of the curve.

For $v \geq 1$ we have by (28) that

$$\int_v^\infty \frac{\mathrm{d}v}{270u^2 - 90} = \frac{1}{6}\int_{X_0}^X \frac{\mathrm{d}X}{Y}, \tag{29}$$

and similarly for $v \leq 0$ we have

$$\int_{-\infty}^v \frac{\mathrm{d}v}{270u^2 - 90} = -\frac{1}{6}\int_{X_0}^X \frac{\mathrm{d}X}{Y}. \tag{30}$$

If $v \geq 1$, then $270u^2 - 90 > 10.5372v^2$, and $v \leq 0$ implies $270u^2 - 90 > 13.4442v^2$. These inequalities immediately follow from the explicit expression for $u(v)$. Hence

$$\int_I \frac{\mathrm{d}v}{270u^2 - 90} < 0.0949019 \int_I \frac{\mathrm{d}v}{v^2} = 0.0949019\frac{1}{|v|}, \tag{31}$$

where $I = [v, \infty)$ if $v \geq 3$, and $I = (-\infty, v]$ if $v \leq 0$.

We now take an arbitrary point $P = m_1P_1 + \ldots + m_5P_5$ on the curve with integral coordinates u, v on (24) and put $M = \max_{1\leq i\leq 5} |m_i|$. With the ϕ-function as described in section 3 and the fundamental real period $\omega = 1.30203\ldots$ we have

$$\int_{X_0}^X \frac{\mathrm{d}X}{Y} = \int_{X_0}^\infty \frac{\mathrm{d}X}{Y} - \int_X^\infty \frac{\mathrm{d}X}{Y} = \omega(\phi(Q_0) - \phi(P)), \tag{32}$$

where

$$\phi(P) = \phi(m_1P_1 + \ldots + m_5P_5) = m_1\phi(P_1) + \cdots + m_5\phi(P_5) + m_0$$

with $m_0 \in \mathbb{Z}$ and such that all ϕ-values are in $[0, 1)$. Note that this implies that $|m_0| \leq 5M$. Put $u_1 = \omega\phi(P_1) = 0.333381\ldots$, $u_2 = \omega\phi(P_2) = 0.801640\ldots$, $u_3 = \omega\phi(P_3) = 0.533496\ldots$, $u_4 = \omega\phi(P_4) = 0.935083\ldots$, $u_5 = \omega\phi(P_5) = 1.01502\ldots$, and $u_0 = \omega\phi(Q_0) = 0.563462\ldots$. Then by (29) or (30), (31) and (32), the usual linear form

$$L(P) = \omega(\phi(Q_0) - \phi(P)) = u_0 - m_0\omega - m_1u_1 - \ldots - m_5u_5$$

is estimated by

$$|L(P)| = 6\int_I \frac{\mathrm{d}v}{270u^2 - 90} \leq 0.569412\,\frac{1}{|v|}. \tag{33}$$

If $v \leq -2$ or $v \geq 5$ then $X < -1$, and hence

$$h(X(P)) \leq \log|30u - 300v + 1200| < 6.78327 + \log|v|. \tag{34}$$

Observe that the above inequality requires u and v to be integral.
Moreover we have

$$\hat{h}(P) \geq c_1M^2. \tag{35}$$

Recall that $c_1 = 0.478212$.

Putting it all together we obtain by (33), (34), (27) and (35), subject to $v \geq 5$ or $v \leq -2$, that

$$|L(P)| < \exp(13.5713 - 0.956424M^2). \tag{36}$$

Next we apply David's result [D95] to the linear form in elliptic logarithms $L(P)$. As $\max_{0\leq i\leq 5}|m_i| \leq 5M$, we obtain the lower bound

$$|L(P)| > \exp\left(-c_4(\log(5M) + c_5)(\log\log(5M) + c_6\right)^8.$$

Here we use Tzanakis' notation of [Tz96]). We computed $c_4 = 3.98179\cdots \times 10^{280}$, $c_5 = 2.09861\ldots$, and $c_6 = 20.3825\ldots$. Together with the upper bound (36) this lower bound yields an absolute upper bound $M_0 = 2.07239 \times 10^{147}$ for M.

In order to find all solutions below this large bound we use the reduction procedure based on the LLL-algorithm. Consider the lattice spanned by the columns of the matrix

$$\mathcal{A} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ [Cu_1] & [Cu_2] & [Cu_3] & [Cu_4] & [Cu_5] & [C\omega] \end{pmatrix},$$

and let $\boldsymbol{y}$ be the point $\boldsymbol{y} = (0,0,0,0,0,[Cu_0])^\top$. Observe that $\boldsymbol{y}$ is not a lattice point, because Q_0 is not defined over $\mathbb{Q}$. Using the LLL-algorithm we compute the minimum d of $\|\mathcal{A}\boldsymbol{x} - \boldsymbol{y}\|$, where $\boldsymbol{x}$ runs through $\mathbb{Z}^6$. Given a solution $m_0, m_1, \ldots, m_5$ of (36) with $M \le M_0$, we consider the lattice point

$$\mathcal{A}(m_1,m_2,m_3,m_4,m_5,m_0)^\top = (m_1,m_2,m_3,m_4,m_5,\lambda)^\top.$$

While on the one hand, by the very definition of d, this lattice point satisfies the inequality

$$d^2 \le m_1^2 + \ldots + m_5^2 + \lambda^2 \le 5M_0^2 + \lambda^2, \tag{37}$$

on the other hand, because by definition λ is an approximation to $-CL(P)$, we have

$$|\lambda + CL(P)| \le \tfrac{1}{2}(|m_1| + \ldots + |m_5| + |m_0| + 1) \le 5M_0 + \tfrac{1}{2}. \tag{38}$$

Thus, using inequalities (36), (37) and (38), we reach a reduced upper bound M_1 for M, namely

$$M_1 = \left\lfloor \sqrt{\frac{1}{2c_1}\left(\log C + 13.5713 - \log\left(\sqrt{d^2 - 5M_0^2} - (5M_0 + \frac{1}{2})\right)\right)} \right\rfloor .$$

Naturally, this is a valid expression only for $d > \sqrt{30M_0^2 + 5M_0 + \frac{1}{4}}$. By heuristic argument, a lattice of dimension dim and determinant det should have $d \approx \det^{1/\dim}$, and therefore, our present d should be approximately $C^{1/6}$. This suggests we should take $C \approx M_0^6$, but large enough. Then we can expect the reduced bound to be $M_1 \approx \sqrt{\log C} \approx \sqrt{\log M_0}$.

We start the reduction procedure with $C = 10^{890}$ and compute $d = 1.27678\cdots \times 10^{148}$, which leads to $M_1 = 42$. On putting $M_0 = 42$, we repeat the process. With $C = 10^{15}$ we find $d = 293.455\ldots$ and $M_1 = 6$. All integral points with coefficients below the final bound of 6 can be recovered without any trouble by direct search. As a matter of fact the values of $|m_i|$ $(i = 1,\ldots,5)$ corresponding to an integral point never exceed 1. This completes the proof. □

It might be of interest to mention the computation times. They were as follows: mrank (see [Cr92]) used 7.2 seconds to compute the rank, findinf used 3.8 seconds to compute the points of small height, it took about 17 seconds on a Pentium 75 PC to show that the Mordell-Weil basis basis has an optimal c_1-value, Pari 1.39.03 used about 38.5 minutes on a Pentium 75 PC for the reduction process, and Apecs 4.2 under Maple V.4 used about 1 hour and 55 minutes on a Pentium 75 PC to find the small solutions.

We continue with yet another binomial equation, namely

$$\binom{n}{k} = \binom{n-1}{k+2},$$

and we can show that it has only the rather trivial solutions $\binom{3}{0} = \binom{2}{2} = 1$ and $\binom{0}{0} = \binom{-1}{2} = 1$. Getting rid of denominators will introduce new solutions with negative k. Renaming k by u and n by v for reasons of uniformity, the following equation emerges:

$$u^3 - 2u^2v + 3uv^2 - v^3 + 3u^2 - 3uv + 3v^2 + 2u = 0, \tag{39}$$

and we can formulate the theorem

Theorem 3. *The only integral solutions of the diophantine equation* (39) *are* $(u, v) = (-2, -2), (-2, -1), (-2, 0), (-1, -1), (-1, 0), (-1, 1), (0, 0), (0, 3)$.

The proof is in many respects similar to the previous one, but much simpler. The present elliptic curve has rank 1, trivial torsion and a generator for the Mordell-Weil group is found without any difficulty.

Our next example is very much of twin type. Apart from the trivial $\binom{3}{0} = \binom{1}{1} = 1$ and $\binom{1}{1} = \binom{-1}{2} = 1$, we can prove that the equation

$$\binom{n}{k} = \binom{n-2}{k+1}$$

has only one nontrivial solution, namely $\binom{6}{1} = \binom{4}{2} = 6$. Again, by getting rid of denominators new solutions are introduced, some with a negative value of k, others as the result of multiplication by 0. Replacing k by u and n by v yields the equation

$$u^3 - 3u^2v + 4uv^2 - v^3 + 3u^2 - 7uv + 4v^2 + 2u - 3v = 0. \tag{40}$$

We can prove

Theorem 4. *The only integral solutions of the diophantine equation* (40) *are* $(u, v) = (-2, 0), (-1, -1), (-1, 0), (-1, 1), (0, 0), (0, 1), (0, 3), (1, 1), (1, 6)$.

Observe that $(u, v) = (0, 0)$ suggests equality in $1 = \binom{0}{0} \neq \binom{-2}{1} = -2$, and similarly $(u, v) = (0, 1)$ suggests equality in $1 = \binom{1}{0} \neq \binom{-1}{1} = -1$, each caused by multiplying both sides of the original equation by 0.

Once more, there are no remarkable facts to be mentioned; the elliptic curve has rank 1, a generator for the Mordell-Weil group is quite obvious, and its torsion subgroup is of order 2. The solution process runs along very much like it does in the previous examples. In this case we again work with $2L(P)$ instead of $L(P)$ which makes dealing with 2-torsion easier.

The final two examples of this section also form a pair. The first equation tells us that no positive integer of the form $\binom{m}{3}$ $(m \in \mathbb{Z}, m \geq 3)$ is at the same time a product of six consecutive integers, and the second equation says the same for integers of the form $\binom{m}{6}$ where m is an integer ≥ 6. To be more precise, we can show that the diophantine equation

$$x(x-1)(x-2)(x-3)(x-4)(x-5) = \binom{m}{3} \tag{41}$$

has no integral solutions (x, m) but those belonging to the set $\{0, 1, 2, 3, 4, 5\} \times \{0, 1, 2\}$, and the elements (x, m) of the set $\{0, 1, 2, 3, 4, 5\} \times \{0, 1, 2, 3, 4, 5\}$ are the only integral solutions of the diophantine equation

$$x(x-1)(x-2)(x-3)(x-4)(x-5) = \binom{m}{6}. \tag{42}$$

On putting $u = m - 1$ and $v = \frac{1}{2}x^2 - \frac{5}{2}x + 3$ in (41) this equation takes the form

$$u^3 - u = 48v^3 - 192v^2 + 144v \tag{43}$$

and we have

Theorem 5. *The integral solutions* (u, v) *of the diophantine equation* (43) *are precisely those that belong to the set* $\{-1, 0, 1\} \times \{0, 1, 3\}$.

Similarly, putting $u = \frac{1}{2}x^2 - \frac{5}{2}x + 3$ and $v = \frac{1}{2}m^2 - \frac{5}{2}m + 3$ in (42) transforms this equation into

$$720u^3 - 2880u^2 + 2160u = v^3 - 4v^2 + 3v \tag{44}$$

and hence we can prove that

Theorem 6. *All integral solutions* (u, v) *of the diophantine equation* (44) *are given by* $(u, v) \in \{0, 1, 3\} \times \{0, 1, 3\}$.

It should not come as a surprise that both proofs are similar. Both elliptic curves have trivial torsion and are of rank 4, but finding a certified Mordell-Weil basis for each is not a trivial matter. In both cases Siksek's index trick (see page 14 and the reference cited there) proves sufficient, but in case of equation (44) some extra sieving is required. See the next section (page 22) for more details in a similar case.

7.2 Examples 2(b)

The cubic equations of this final section are characterized by having three distinct asymptotes.
We have chosen two examples, both closely associated with so-called binary Krawtchouk polynomials. These polynomials, and especially the occurrence of integral zeroes, have a background in combinatorics and coding theory; see [HS93] and [KL96] and the references cited there. The nth binary Krawtchouk polynomial is defined by

$$k_n^N(x) = \sum_{j=0}^{n} (-1)^j \binom{N-x}{n-j} \binom{x}{j} \tag{45}$$

with parameters n, N. For $n = 1, 2, 3$ the zeroes of $k_n^N(x)$ are rather trivial, but for $n = 4, 5, 6, 7$ the equation $k_n^N(x) = 0$ can be directly associated with an elliptic curve, so that the problem of determining all integral zeroes of these polynomials can be solved by finding all integral points on the corresponding elliptic curves. For $n = 8$ the equation $k_n^N(x) = 0$ does not correspond to a curve of genus 1, but to a curve of genus 3 which makes a generalization of our approach quite unlikely. In [SdW98] we provide more information on the background of this problem and there we give the full details of the case $n = 6$. Here we shall suffice with giving most of the details of the other open case $n = 7$. But first we shall formulate precise statements of the results obtained.

If we put $n = 6$ in (45) and substitute $u = N$ and $v = (N - 2x)^2$, then equation $k_6^N(x) = 0$ may be rewritten as

$$-15u^3 + 45u^2v - 15uv^2 + v^3 + 90u^2 - 210uv + 40v^2 - 120u + 184v = 0. \qquad (46)$$

This equation is clearly not of Weierstraß or shifted Weierstraß type, and we can prove the following result.

Theorem 7. *The diophantine equation* (46) *has the integral solutions* (u, v) *as given in the table below. There are no other integral solutions. In addition the table also gives the corresponding values of* x *and* N*. Because of symmetry about* $x = N/2$ *we may restrict* x *to* $x \leq N/2$*.*

Solutions (u,v) of (46), $u = N$, $v = (N-2x)^2$								
(u,v)	x	N	(u,v)	x	N	(u,v)	x	N
$(-14,-56)$			$(3,1)$	1	3	$(9,25)$	2	9
$(-4,-20)$			$(3,9)$	0	3	$(12,4)$	5	12
$(-1,-9)$			$(4,0)$	2	4	$(12,36)$	3	12
$(0,0)$	0	0	$(4,4)$	1	4	$(12,100)$	1	12
$(1,1)$	0	1	$(4,16)$	0	4	$(16,144)$	2	16
$(2,-14)$			$(5,1)$	2	5	$(25,9)$	11	25
$(2,0)$	1	2	$(5,9)$	1	5	$(67,25)$	31	67
$(2,4)$	0	2	$(5,25)$	0	5	$(345,1225)$	155	345
$(3,-5)$								

Proof. See [SdW98]. □

For $n = 7$, $u = N - 1$ and $v = (N - 2x)^2 - 1$ in (45), equation $k_n^N(x) = 0$ reduces to

$$-105u^3 + 105u^2v - 21uv^2 + v^3 + 630u^2 - 462uv + 52v^2 - 840u + 360v = 0. \qquad (47)$$

This equation is again not of Weierstraß or shifted Weierstraß type, and we have the following result.

Theorem 8. *The diophantine equation* (47) *has the integral solutions* (u, v) *as given in the table below and no others. In addition the table also gives the corresponding values of* x *and* N*. Because of symmetry about* $x = N/2$ *we may restrict* x *to* $x \leq N/2$*.*

Solutions (u,v) of (47), $u=N-1$, $v=(N-2x)^2-1$								
(u,v)	x	N	(u,v)	x	N	(u,v)	x	N
$(-22,-132)$			$(3,-7)$			$(5,35)$	0	6
$(-6,-42)$			$(3,3)$	1	4	$(8,8)$	3	9
$(-3,-25)$			$(3,15)$	0	4	$(13,15)$	5	14
$(0,0)$	0	1	$(4,0)$	2	5	$(13,63)$	3	14
$(1,3)$	0	2	$(4,8)$	1	5	$(13,143)$	1	14
$(2,-18)$			$(4,24)$	0	5	$(16,80)$	4	17
$(2,0)$	1	3	$(5,3)$	2	6	$(21,255)$	4	22
$(2,8)$	0	3	$(5,15)$	1	6	$(1028,1368)$	496	1029

Proof. The birational transformations

$$(u,v)=\left(\tfrac{-128280X-9540Y+58379700}{53X^2-98482X-2220Y+28565297},\tfrac{487200X-22260Y-82369140}{53X^2-98482X-2220Y+28565297}\right), \tag{48}$$
$$(X,Y)=\left(\tfrac{17479u-3051v-44520}{7u-3v},\tfrac{2496599u^2+186858uv-68001v^2-6820800u-1795920v}{(7u-3v)^2}\right)$$

relate equation (47) to the global minimal Weierstrass model

$$Y^2+XY+Y=X^3-X^2-722882X+185853889. \tag{49}$$

We make a further transformation by

$$(X,Y)=(\tfrac14 x+\tfrac14,\tfrac18 y-\tfrac18 x-\tfrac58),\quad (x,y)=(4X-1,8Y+4X+4)$$

which leads to the short Weierstraß form

$$y^2=x^3-11566107x+11883082806.$$

By Apecs we compute the particulars of this elliptic curve, and we find that its torsion subgroup is trivial. Further, by Cremona's program mrank we obtain that the rank is 4, and we quickly find the four independent rational points $P_1=(1297,37151)$, $P_2=(-383,20351)$, $P_3=(247,4601)$, and $P_4=(697,4151)$, with regulator $R=1.47916\ldots$. We calculate $\hat{h}(P_1)=0.447230\ldots$, and we intend to show that there are no rational points of smaller canonical height. Silverman's and Siksek's bounds on the difference between the naive and canonical heights, as computed by Apecs, read

$$-5.11697<\hat{h}(P)-\tfrac12 h(X(P))<5.75713 \tag{50}$$

for any rational point P. Consequently, $h(X(P))<11.1285$ for any P with $\hat{h}(P)<\hat{h}(P_1)$. With Cremona's findinf we searched for all such points, showing that if $h(X(P))<11.1285$ then $P=\mathcal{O}$ or $\hat{h}(P)\geq\hat{h}(P_1)$. Therefore we may take $\lambda=0.447230$ in Siksek's upper bound for the index of the group generated by P_1, P_2, P_3, P_4 in the full Mordell-Weil group, giving

$$\text{index} \leq \sqrt{R}\frac{2}{(2\lambda)^2} = 3.04\ldots.$$

This implies that in order to prove that P_1, P_2, P_3, P_4 form a basis for the full group of rational points we merely need to show that the index cannot be equal to 3, because information from mrank tells us that the index must be odd. Siksek sieving (cf. [Sik95]) with $p = 3$ and $v = 23, 41, 67, 89$ gives the relation matrix

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

in which each column represents a prime v. As its rank is 4, the index is 1, and hence the four points P_i $(i = 1, 2, 3, 4)$ form a basis for the Mordell-Weil group.

Next we checked that amongst all possible bases, this basis has the property that the least eigenvalue of the Néron-Tate height pairing matrix (see [ST97]) is as large as possible. This optimal value is $c_1 = 0.260469\ldots$. We shall need this number later.

From the birational transformations (48) we deduce

$$\frac{\mathrm{d}v}{-315u^2 + 210uv - 21v^2 + 1260u - 462v - 840} = -\frac{1}{2}\frac{\mathrm{d}X}{2Y + X + 1} = -\frac{1}{2}\frac{\mathrm{d}x}{y}. \tag{51}$$

There are three asymptotes $v = \alpha u + \beta$, where α is one of the three roots of equation

$$\alpha^3 - 21\alpha^2 + 105\alpha - 105 = 0,$$

and $\beta = -\frac{1}{6}(6 + 3\alpha + \alpha^2)$. Further, the corresponding points at infinity, given in (X, Y)-coordinates, are

$$Q_0 = (X_0, Y_0) = \left(\frac{17479 - 3051\alpha}{7 - 3\alpha}, \frac{2496599 + 186858\alpha - 68001\alpha^2}{(7 - 3\alpha)^2}\right).$$

The numerical values of the α's, β's and Q_0's are gathered in the table below.

i	α_i	β_i	$Q_{0,i}$
1	$1.33265\ldots$	$-1.96231\ldots$	$(4467.98\ldots, 291646\ldots)$
2	$5.60155\ldots$	$-9.03033\ldots$	$(-39.6414\ldots, 15316.1\ldots)$
3	$14.0657\ldots$	$-41.0073\ldots$	$(722.660\ldots, -6403.62\ldots)$

Note that $Q_0 \in E(\mathbb{K})$, where $\mathbb{K} = \mathbb{Q}(\alpha)$ is a cubic number field. We now distinguish six (u,v)-ranges, 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 branches of (47) we see that $u = u(v)$ is a strictly increasing function of v. On each branch let $F : \mathbb{R} \longrightarrow \mathbb{R}$ be given by

$$F(v) = \frac{17479u(v) - 3051v - 44520}{7u(v) - 3v},$$

where $u(v)$ is the unique solution on that branch implicitly given by the equation (47). Then $X = F(v)$. For each of the six ranges, the unique v-interval and its X-image under F are as follows:

$$\begin{array}{lllll}
1_1: & I = [v, \infty) & \longrightarrow & J = [X, X_{0,1}) & \\
1_2: & I = (-\infty, v] & \longrightarrow & J = (X_{0,1}, X] & \\
2_1: & I = [v, \infty) & \longrightarrow & J = [X, X_{0,2}) & \text{if } v \geq 14 \\
2_2: & I = (-\infty, v] & \longrightarrow & J = (X_{0,2}, X] & \text{if } v \leq -3 \\
3_1: & I = [v, \infty) & \longrightarrow & J = [X, X_{0,3}) & \\
3_2: & I = (-\infty, v] & \longrightarrow & J = (X_{0,3}, X] & \text{if } v \leq -20
\end{array}$$

In some cases we need extra conditions to ensure the bijective correspondence of intervals. Observe that in the cases 1_1, 1_2, 3_1 and 3_2 we land on $E_0(\mathbb{R})$, while in the remaining cases 2_1 and 2_2 we land on $E_C(\mathbb{R})$. In all cases we have by (51) that

$$\int_I \frac{\mathrm{d}v}{-315u^2 + 210uv - 21v^2 + 1260u - 462v - 840} = \pm\tfrac{1}{2} \int_J \frac{\mathrm{d}X}{2Y + X + 1} = \pm\tfrac{1}{2} \int_{J'} \frac{\mathrm{d}x}{y}, \tag{52}$$

where J' is an obvious linear adjustment of the interval J. Provided $v \leq -20$ or $v \geq 14$ we find by explicitly solving (47) for $u = u(v)$ the inequality

$$-315u^2 + 210uv - 21v^2 + 1260u - 462v - 840 \geq 5.31119v^2.$$

Hence

$$\int_I \frac{\mathrm{d}v}{-315u^2 + 210uv - 21v^2 + 1260u - 462v - 840} < 0.188282 \int_I \frac{\mathrm{d}v}{v^2} = 0.188282\, \frac{1}{|v|}. \tag{53}$$

After this preliminary work, we consider an arbitrary point P on the curve with integral (u,v)-coordinates relative to (47). Then $P = m_1P_1 + m_2P_2 + m_3P_3 + m_4P_4$ for certain integers m_i $(i = 1,2,3,4)$. Let M be the absolute maximum of these coefficients, so $M = \max_{1\le i\le 4}|m_i|$.

Let the ϕ-function be properly adjusted. Then

$$\int_{J'} \frac{\mathrm{d}x}{y} = \pm\omega(\phi(Q_{0,i}) - \phi(P)). \tag{54}$$

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 $m_0 \in \mathbb{Z}$ such that all ϕ-values belong to $[0,1)$. This clearly implies that $|m_0| \le 4M$. Put $u_1 = \omega\phi(P_1) = 0.0289846\ldots$, $u_2 = \omega\phi(P_2) = 0.0344552\ldots$, $u_3 = \omega\phi(P_3) = 0.00957876\ldots$, $u_4 = \omega\phi(P_4) = 0.0474580\ldots$, $u_{0,1} = \omega\phi(Q_{0,1}) = 0.0150135\ldots$, $u_{0,2} = \omega\phi(Q_{0,2}) = 0.0247808\ldots$, $u_{0,3} = \omega\phi(Q_{0,3}) = 0.0636683\ldots$. 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 by (52), (53) and (54) it follows that

$$|L(P)| < 0.376564\,\frac{1}{|v|}. \tag{55}$$

If $v \le -1$ or $v \ge 234$ then $|X| > 1$. Considering the solution $u(v)$, implicitly given by (47), it follows by elementary calculus that

$$h(X(P)) \le \log|17479u - 3051v - 44520| < 10.8115 + \log|v|, \tag{56}$$

We emphasize that in the derivation we need the fact that u and v are integral.

Finally we have

$$\hat{h}(P) \ge c_1M^2. \tag{57}$$

Recall that $c_1 = 0.260469$.

Putting it all together, by (55), (56), (50) and (57), and under the condition $v \le -20$ or $v \ge 234$, we obtain that

$$|L(P)| < \exp(21.3491 - 0.520938M^2). \tag{58}$$

Next we apply David's result [D95] to the linear form in elliptic logarithms $L(P)$. Note that $\omega\phi(P_i)$ and $\omega\phi(Q_{0,i})$ are indeed elliptic logarithms, but that the coordinates of the associated points are in a field of degree 9. Thus we obtain

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

Here we have $c_4 = 3.20626\cdots \times 10^{225}$, $c_5 = 1+\log 9$, $c_6 = c_5 + 38.7112\ldots$. Combined with (58) this result of David yields an absolute upper bound $M_0 = 9.73642 \times 10^{119}$ for M.

In order to find all the solutions below this very large upper bound we use several rounds of LLL-reduction. 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 rational. Using the LLL-algorithm we compute $d = \min_{\boldsymbol{x}} |\mathcal{A}\boldsymbol{x} - \boldsymbol{y}|$. For a solution m_0, m_1, m_2, m_3, m_4 of (58) with $M \leq M_0$, we 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 definition of d, this lattice point satisfies the inequality

$$d^2 \leq m_1^2 + m_2^2 + m_3^2 + m_4^2 + \lambda^2 \leq 4M_0^2 + \lambda^2, \tag{59}$$

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

$$|\lambda - CL(P)| \leq \frac{1}{2}(|m_1| + |m_2| + |m_3| + |m_4| + |m_0| + 1) \leq 4M_0 + \tfrac{1}{2}. \tag{60}$$

On combining inequalities (58), (59) and (60), we reach a reduced upper bound M_1 for M, namely

$$M_1 = \left\lfloor \sqrt{\frac{1}{2c_1}\left(\log C + 19.1305 - \log\left(\sqrt{d^2 - 4M_0^2} - (4M_0 + \tfrac{1}{2})\right)\right)} \right\rfloor.$$

Clearly this bound is meaningful only if $d > \sqrt{20M_0^2 + 4M_0 + \frac{1}{4}}$. As in a previous remark, we expect d to be approximately $\det^{1/\dim}$. Therefore, in the present case $d \approx C^{1/5}$ so that we should take $C \approx M_0^5$, and large enough. The reduced bound can then be expected to be $M_1 \approx \sqrt{\log C} \approx \sqrt{\log M_0}$.

First we apply this procedure with $C = 10^{608}$ and find $d = 1.01729\cdots \times 10^{121}$, which leads to $M_1 = 46$. Next we replace M_0 by M_1, i.e. we put $M_0 = 46$, and repeat the process. With $C = 10^{14}$ we find $d = 288.781\ldots$ and $M_1 = 9$. We could not reach further improvement. Below this reduced bound 9 for M it is straightforward to find all solutions by direct search. We point out that for all solutions the corresponding coefficients $|m_i|$ are never larger than 2.

This completes the proof. $\square$

The computation times were as follows: mrank used about 36 hours and 7 minutes on a Sun Sparcstation 4 to compute the rank, findinf used about 4 minutes and 37 seconds on a Sun Sparcstation 4 to find the points of small height, the Siksek sieving used about 1 second on a Pentium 75 PC, it took 0.9 seconds on a Pentium 75 PC to find the basis with the optimal c_1-value, Pari 1.39.03 used about 11 minutes and 35 seconds on a Pentium 75 PC for the reduction procedure, and Apecs 4.2 under Maple V.4 used about 1 hour and 36 minutes on a Pentium 75 PC to find the small solutions. These computations were completed a while ago, so we expect significant improvements in the computation times by more up-to-date versions of the software we used.

References

[BC70] A. Baker and J. Coates, "Integer points on curves of genus 1", *Proc. Camb. Phil. Soc.* **67** (1970), 595–602.

[BH96] Yu. Bilu and G. Hanrot, "Solving Thue equations of high degree", *J. of Number Th.* **60** (1996), 373–392.

[BH98] Yu. Bilu and G. Hanrot, "Solving superelliptic diophantine equations by Baker's method", *Compositio Math.* **112** (1998), 273–312.

[BST97] A. Bremner, R.J. Stroeker and N. Tzanakis, "On sums of consecutive squares", *J. Number Th.* **62** (1997), 39–70.

[Co97] 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.

[Cr92] J. E. Cremona, "Algorithms for modular elliptic curves", Cambridge Un. Press, 1992. The programs mrank, mwrank, findinf may be downloaded from John Cremona's ftp site euclid.ex.ac.uk/pub/cremona.

[D95] S. David, "Minorations de formes linéaires de logarithmes elliptiques", *Mémoires Soc. Math. France (N.S)*, **62** (1995), iv + 143 pp.

[GZ94] J. Gebel and H.G. Zimmer, "Computing the Mordell-Weil group of an elliptic curve over $\mathbb{Q}$", CRM Proc. & Lect. Notes Vol. 4 (1994), 61–83.

[GPZ94] J. Gebel, A. Pethő and H.G. Zimmer, "Computing integral points on elliptic curves", *Acta Arith.* **68** (1994), 171–192.

[GPZ97] J. Gebel, A. Pethő and H.G. Zimmer, "Computing integral points on Mordell's elliptic curves", *Collect. Math.* **48** No.1-2 (1997), 115-136.

[HS93] Laurent Habsieger and Dennis Stanton, "More zeros of Krawtchouk polynomials", *Graphs and Combinatorics* **9** (1993), 163–172.

[HP98] L. Hajdu and Á. Pintér, "Combinatorial Diophantine Equations", preprint.

[H97] G. Hanrot, "Résolution effective d'équations diophantiennes: algorithmes et applications", Thèse, Université Bordeaux 1, 1997.

[KL96] Ilia Krasikov and Simon Litsyn, "On integral zeros of Krawtchouk polynomials", *J. Comb. Theory* Ser. A **bf 74** (1996), 71–99.

[N28] T. Nagel, "Sur les propriétés des cubiques planes du premier genre", *Acta Math.* **52** (1928), 93–126.

[Sch92] Wolfgang M. Schmidt, "Integer points on curves of genus 1", *Compositio Math.* **81** (1992), 33–59.

[Sie29] C.L. Siegel, "Über einige Anwendungen diophantischer Approximationen", *Abh. Preuss. Akad. Wiss.* (1929), 1–41.

[Sil86] J. H. Silverman, "The arithmetic of elliptic curves", Springer-Verlag, New York, 1986.

[Sil88] J. H. Silverman, "Computing heights on elliptic curves", *Math. Comp.* **51** (1988), 339–358.

[Sil90] J. H. Silverman, "The difference between the Weil height and the canonical height on elliptic curves", *Math. Comp.* **55** (1990), 723–743.

[Sik95] Samir Siksek, "Infinite descent on elliptic curves", *Rocky Mountain J. Math.* **25** (1995), 1501–1538.

[Sm94] N.P. Smart, "S-integral points on elliptic curves", *Math. Proc. Camb. Phil. Soc.* **116** (1994), 391–399.

[St95] R. J. Stroeker, "On the sum of consecutive cubes being a perfect square", *Compositio Math.* **97** (1995), 295–307.

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

[ST97] R. J. Stroeker and N. Tzanakis, "On the elliptic logarithm method for elliptic diophantine equations: Reflections and an improvement", to appear in *Experimental Math.*

[SdW96] R.J. Stroeker and B.M.M. de Weger, "On a quartic diophantine equation", *Proc. Edinburgh Math. Soc* **39** (1996), 97–114.

[SdW97] R.J. Stroeker and B.M.M. de Weger, "Elliptic binomial diophantine equations", to appear in *Math. Comp.*

[SdW98] R.J. Stroeker and B.M.M. de Weger, "On integral zeroes of binary Krawtchouk polynomials", in preparation.

[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.

[TdW89] N. Tzanakis and B.M.M. de Weger, "On the practical solution of the Thue equation", *J. of Number Th.* **31**(2) (1989), 99–132.

[dW89] B. M. M. de Weger, "Algorithms for Diophantine equations", CWI Tract 65, Stichting Mathematisch Centrum, Amsterdam, 1989.

[Z87] D. Zagier, "Large integral points on elliptic curves, *Math. Comp.* **48** (1987), 425–436.