Collect. Math. **48**, 1–2 (1997), 115–136

Computing integral points on Mordell's elliptic curves

J. Gebel, A. Pethö and H. G. Zimmer[1]

Fachbereich 9 Mathematik, Universität des Saarlandes,
Postfach 15 11 50, D-66041 Saarbrücken, Germany
E-mail address: zimmer@math.uni-sb.de

Abstract

We use Mordell's elliptic curves E_k (see below) to illustrate our algorithm for computing all integral points on *any* given elliptic curve over the rationals (see [5]) and apply it to determine the integral points on E_k for k within the range $|k| \leq 10,000$. Actually, the calculations can be extended to $|k| \leq 100,000$. In this larger range Hall's conjecture holds with $c_\epsilon = 5$.

1. Introduction

Siegel [12] proved in 1929 that the number of integral points on an elliptic curve E over an algebraic number field K is finite, and Mahler [9] generalized this result in 1934 to S-integral points. In 1978, Lang (and Demjanenko, see [8]) conjectured that the number of integral points on a quasi-minimal model of E over K is bounded by a constant depending only on K and the rank r of E over K, and this conjecture easily carries over to the number of S-integral points with a bound depending on r, K and S. Indeed, Silverman [13] proved these conjectures in 1981 for elliptic curves E over K with integral j-invariant.

Moreover, beginning with the pioneering work of Baker [1], several authors derived bounds for the size of the coordinates of integer points on elliptic curves E over K. Since we are interested in computing all integral points on the elliptic curve defined by Mordell's equation (by abuse of language, we shall speak of Mordell's elliptic curve)

$$E_k : \quad y^2 = x^3 + k \quad (0 \neq k \in \mathbb{Z}),$$

[1] The lecture was delivered by the last author.

we mention here only the bounds obtained for this equation by Stark [17]:

$$\max\{|x|,|y|\} < \exp\{c_\epsilon |k|^{1+\epsilon}\},$$

with an effectively computable constant $c_\epsilon > 0$ depending on a given $\epsilon > 0$, and by Sprindžuk [16], p. 113,

$$\max\{|x|,|y|\} < \exp\{c|k|(1+ln|k|)^6\},$$

with a computable absolute constant $c > 0$.

Some numerical data led Hall [7] to make the

Conjecture.

$$|x| < c_\epsilon |k|^{2+\epsilon}$$

with a constant $c_\epsilon > 0$ depending only on $\epsilon > 0$.

Yet the coordinates of integer points on E_k can be quite large in comparison to k. For instance,

$$233,387,325,399,875^2 = 3,790,689,201^3 + 28,024.$$

We shall not employ our numerical results to estimate the constants in the theorems of Stark and Sprindžuk here. Rather we shall use Mordell's elliptic curves E_k to illustrate our algorithm for computing all integral points on *any* given elliptic curve over the rationals (see [5]) and apply it to determine the integral points on E_k for k within the range $|k| \leq 10,000$. Actually, the calculations can be extended to $|k| \leq 100,000$. In this larger range Hall's conjecture holds with $c_\epsilon = 5$.

One ingredient of our algorithm is an explicit lower bound for linear forms in elliptic logarithms. In fact, by considering also linear forms in p-adic elliptic logarithms as in [15], we are even able to determine all S-integral points on Mordell's elliptic curve E_k for any finite set of primes $S = \{\infty, p_1, \ldots, p_n\}$ of the rational number field $\mathbb{Q}$. In the final section, we shall list our results for $S = \{\infty, 2, 3, 5\}$ and $|k| \leq 10,000$.

An extended version of this paper will appear elsewhere.

2. Basic steps of the algorithm

By Mordell's theorem [11], the group of rational points of E_k over $\mathbb{Q}$ is

$$E_k(\mathbb{Q}) \cong E_{k,tors}(\mathbb{Q}) \oplus \mathbb{Z}^r,$$

where $E_{k,tors}(\mathbb{Q})$ is the (finite) torsion group and r is the rank of E_k over $\mathbb{Q}$. Let

$$\{P_1, \ldots, P_r\} \text{ be a basis of } E_k(\mathbb{Q})$$

or, more precisely, of the free part of $E_k(\mathbb{Q})$.

Then, every point $P \in E_k(\mathbb{Q})$ admits a unique representation of the form

$$P = \sum_{\nu=1}^{r} n_\nu P_\nu + P_{r+1} \quad (n_\nu \in \mathbb{Z}), \tag{2.1}$$

where $P_{r+1} \in E_{k,tors}(\mathbb{Q})$ is a torsion point.

Our aim is to find a positive integer N such that, for all *integral* points $P \in E_k(\mathbb{Q})$,

$$|n_\nu| \leq N \quad (\nu = 1, \ldots, r). \tag{2.2}$$

This aim is reached essentially in *three steps* (see [5]):

1. Determine the torsion group, the rank and a basis of the Mordell-Weil group $E_k(\mathbb{Q})$ (see [6]).
2. Compute a lower bound for linear forms in elliptic logarithms (see [3]).
3. Reduce the bound N obtained in this way by numerical diophantine approximation techniques (see [18]).

3. Determination of the Mordell-Weil group (Step 1)

The torsion group is small and can be easily computed. We have (see [4])

Proposition 3.1

Let $k = m^6 k_0$, *with* $m, k_0 \in \mathbb{Z}$, $m > 0$, k_0 *free of 6-th power prime factors. Then*

$$E_{k,tors}(\mathbb{Q}) = \begin{cases} \mathbb{Z}/6\mathbb{Z} & \text{if } k_0 = 1 \\ \mathbb{Z}/3\mathbb{Z} & \text{if } k_0 \neq 1 \text{ is a square or } k_0 = -432 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } k_0 \neq 1 \text{ is a cube} \\ \{0\} & \text{otherwise.} \end{cases}$$

Moreover, any torsion point $P = (x, y) \in E_{k,tors}(\mathbb{Q})$ has coordinates $x, y \in \mathbb{Z}$ such that

$$y = 0 \quad \text{or} \quad y \mid 3k.$$

Rank and basis of the group $E_k(\mathbb{Q})$ are much more difficult to determine. We follow the procedure developed in [6]. It relies on a theorem of Manin [10] and originally depends on the truth of the conjecture of Birch and Swinnerton-Dyer, but our results concerning the curves E_k can be verified afterwards without the assumption of any conjectures.

At first we need to introduce the height functions on $E_k(\mathbb{Q})$. For a rational point with coordinates written in simplest fraction representation

$$\mathcal{O} \neq P = \left(\frac{\xi}{\zeta^2}, \frac{\eta}{\zeta^3}\right) \in E_k(\mathbb{Q}) \text{ with } \xi, \eta, \zeta \in \mathbb{Z},\ \zeta > 0,\ (\xi, \zeta) = (\eta, \zeta) = 1,$$

we recall the definition of the *ordinary height* or *Weil height*

$$h(P) = \left\{ \begin{array}{ll} \frac{1}{2}\ \log\ \max\{|\xi|, \zeta^2\} & \text{if } P \neq \mathcal{O} \\ 0 & \text{if } P = \mathcal{O} \end{array} \right\}.$$

But instead, we shall use the *modified ordinary height* (see [21])

$$d(P) = \left\{ \begin{array}{ll} \frac{1}{2}\ \log\ \max\{|\sqrt[3]{k}\zeta^2|, |\xi|\} & \text{if } P \neq \mathcal{O} \\ \frac{1}{2}\ \log\ |\sqrt[3]{k}| & \text{if } P = \mathcal{O} \end{array} \right\}$$

in our derivation of bounds for the elliptic logarithms. Both functions can be taken to define the *canonical height* or *Néron-Tate height*

$$\hat{h}(P) = \lim_{n \to \infty} \frac{h(2^n P)}{2^{2n}} = \lim_{n \to \infty} \frac{d(2^n P)}{2^{2n}}.$$

We list here the basic properties of these height functions.

(1) There are only finitely many points of bounded (ordinary or canonical) height in $E_k(\mathbb{Q})$.

(2) $\hat{h}$ is a positive-semidefinite quadratic form on $E_k(\mathbb{Q})$, i.e.

$$\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q) \text{ for } P, Q \in E_k(\mathbb{Q}),$$
$$\hat{h}(P) \geq 0 \text{ for } P \in E_k(\mathbb{Q}),$$

and $\hat{h}$ has null space $E_{k,tors}(\mathbb{Q})$, i.e.

$$\hat{h}(P) = 0 \text{ if and only if } P \in E_{k,tors}(\mathbb{Q}).$$

(3) $\hat{h}$ extends to a positive-definite quadratic form on the factor group

$$\tilde{E}_k(\mathbb{Q}) = E_k(\mathbb{Q})/E_{k,tors}(\mathbb{Q})$$

with associated nondegenerate symmetric bilinear form

$$\hat{h}(\tilde{P}, \tilde{Q}) = 2(\hat{h}(\tilde{P} + \tilde{Q}) - \hat{h}(\tilde{P}) - \hat{h}(\tilde{Q})) \text{ for } \tilde{P}, \tilde{Q} \in \tilde{E}_k(\mathbb{Q}).$$

(4) $\hat{h}$ induces a Euclidean norm $\sqrt{2\hat{h}}$ on the r-dimensional real space

$$\mathcal{E}_k(\mathbb{Q}) = E_k(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$$

via the natural injective embedding

$$\tilde{E}_k(\mathbb{Q}) \hookrightarrow \mathcal{E}_k(\mathbb{Q}).$$

(5) The absolute value of the determinant

$$R = |\det(\hat{h}(P_\mu, P_\nu))_{\mu,\nu=1,\ldots,r}|,$$

where $\{P_1, \ldots, P_r\}$ is a basis of $E_k(\mathbb{Q})$ modulo torsion, is an invariant, called the *regulator* of $E_k/\mathbb{Q}$.

(6) The difference between the ordinary height d (or h) and the canonical height $\hat{h}$ is bounded by a constant depending only on k:

$$|d(P) - \hat{h}(P)| < \delta_k \text{ for } P \in E_k(\mathbb{Q}).$$

In fact, one can choose (see [20] - [22])

$$\delta_k = \frac{1}{6} \log |k| + \frac{5}{3} \log 2. \tag{3.1}$$

More precisely, we have (see [21], [22])

$$-\frac{5}{6} \log 2 \leq d(P) - \hat{h}(P) \leq \frac{1}{6} \log |k| + \frac{5}{3} \log 2. \tag{3.2}$$

In terms of the ordinary height h, these estimates read

$$-\frac{1}{6} \log |k| - \frac{5}{6} \log 2 \leq h(P) - \hat{h}(P) \leq \frac{1}{6} \log |k| + \frac{5}{3} \log 2.$$

Silverman [14] established the bounds

$$-\frac{1}{6}\ \log\ |k| - 1.576 \le h(P) - \hat{h}(P) \le \frac{1}{6}\ \log\ |k| + 1.48.$$

A comparison shows that Silverman's constants are slightly weaker than ours, but their dependence on k is the same.

A basis $P_1, \ldots, P_r$ of the free part of $E_k(\mathbb{Q})$ is now determined by applying the method of successive minima from geometry of numbers to the r-dimensional Euclidean space

$$\mathcal{E}_k(\mathbb{Q}) = E_k(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}\,.$$

This method requires the knowledge of the rank r of E_k over $\mathbb{Q}$. The rank can be obtained by computing suitable derivatives of the L-series $L(s, E_k/\mathbb{Q})$ at $s = 1$ and assuming the Birch and Swinnerton-Dyer conjecture to be true. We use the following important theorem due to Manin [10].

Theorem 3.2

Put

$$B = \delta_k + \frac{2^{2r}}{\gamma_r^2} R'^2\ \max\{1, h'^{2(1-r)}\},$$

where δ_k is the bound mentioned above, r is the rank of $E_k/\mathbb{Q}$, γ_r is the volume of the r-dimensional unit ball, $R' \ge R$ is an upper bound for the regulator of $E_k/\mathbb{Q}$ and $h' > 0$ is a lower bound for the canonical height on nontorsion points in $E_k(\mathbb{Q})$:

$$0 < h' < \hat{h}(P) \quad \text{for } P \in E_k(\mathbb{Q}) \setminus E_{k,tors}(\mathbb{Q}).$$

Then the set

$$\{P \in E_k(\mathbb{Q});\ h(P) \le B\}$$

generates a subgroup of $\widetilde{E}_k(\mathbb{Q})$ of finite index $\le r!$

The quantities in Manin's bound B can be determined as follows. Put

$$M_k := \{P \in E_k(\mathbb{Q}) \setminus E_{k,tors}(\mathbb{Q});\ h(P) \le 2\delta_k\}.$$

Then

$$h' = \left\{ \begin{array}{l} \delta_k \text{ if } M_k = \emptyset \\ \min\{\hat{h}(P);\ P \in M_k\} \text{ if } M_k \ne \emptyset \end{array} \right\}.$$

The quantity γ_r is taken from tables. A bound for the difference between the ordinary height and the canonical height on $E_k(\mathbb{Q})$ is chosen according to (3.1). The determination of the rank r and the upper bound R' for the regulator is based on the (see [2])

Conjecture of Birch and Swinnerton-Dyer.

(i) *The L-series $L(s, E_k/\mathbb{Q})$ of $E_k/\mathbb{Q}$ has a zero of order r at $s = 1$, where r is the rank of $E_k/\mathbb{Q}$.*

(ii) $\lim_{s\to 1} \frac{L(s, E_k/\mathbb{Q})}{(s-1)^r} = \frac{\Omega \cdot \sharp \text{III}_k \cdot R}{(\sharp E_{k,tors}(\mathbb{Q}))^2} \prod_{p|\mathcal{N}} c_p,$

where

$\Omega =$ *$m\omega_1$ with the real period ω_1 of E_k (computed by the arithmetic-geometric mean method of Gauss) and the number m of connected components of $E_k(\mathbb{R})$,*

$\text{III}_k =$ *Tate-Shafarevich group of $E_k/\mathbb{Q}$,*

$R =$ *regulator of $E_k/\mathbb{Q}$,*

$c_p =$ *p-th Tamagawa number of $E_k/\mathbb{Q}$ and*

$\mathcal{N} =$ *conductor of $E_k/\mathbb{Q}$ (computed by Tate's algorithm).*

Taking this conjecture for granted, we can compute the rank r of $E_k/\mathbb{Q}$ on the basis of the relation

$$r = \min\{\rho \in \mathbb{Z};\ \rho \geq 0,\ L^{(\rho)}(1, E_k/\mathbb{Q}) \neq 0\}.$$

Of course, the problem here is to decide whether or not $L^{(\rho)}(1, E_k/\mathbb{Q}) = 0$. But assuming that the ρ-th derivative is $\neq 0$ at $s = 1$ and hence that $r = \rho$, and starting a sieving procedure with the bound B in Manin's theorem, one can either verify by contradiction that $L^{(\rho)}(1, E_k/\mathbb{Q}) = 0$ or figure out that this derivative is $\neq 0$.

Once the rank r is known, we are able to compute the upper bound for the regulator

$$R' = \frac{L^{(r)}(1, E_k/\mathbb{Q})(\sharp E_{k,tors}(\mathbb{Q}))^2}{\Omega r! \prod_{p|\mathcal{N}} c_p} \geq R$$

in crudely estimating the order of the Tate-Shafarevich group by one:

$$\sharp\ \text{III}_k \geq 1.$$

By virtue of Manin's theorem, a basis of $E_k(\mathbb{Q})$ is then determined in five steps.

(i) Compute the bound B.

(ii) Determine the set $\{P \in E_k(\mathbb{Q}) \setminus E_{k,tors}(\mathbb{Q});\ h(P) \leq B\}$ by a suitable sieving procedure.

(iii) By repeated divisions by 2, compute a complete set of representatives in $E_k(\mathbb{Q})$ of the factor group $E_k(\mathbb{Q})/2E_k(\mathbb{Q})$.

(iv) Determine a generating system of points for $E_k(\mathbb{Q})$ by the infinite descent method.

(v) Compute a basis from the generating system by applying the (modified) *LLL*-algorithm.

4. Elliptic logarithms (Step 2)

The elliptic curve $E_k/\mathbb{Q}$ can be parametrized by Weierstrass' $\wp$-function corresponding to the lattice $\Omega = \langle \omega_1, \omega_2 \rangle$ generated by the real and complex period ω_1 and ω_2 of $E_k/\mathbb{C}$, respectively. Indeed we have the analytic isomorphism

$$\begin{aligned} \mathbb{C}/\Omega \quad &\xrightarrow{\sim} E_k(\mathbb{C}) \\ u + \Omega \ &\longmapsto P = (\wp(u), \wp'(u)) = \Big(\frac{\xi}{\zeta^2}, \frac{\eta}{\zeta^3}\Big). \end{aligned}$$

For integer points $P \in E_k(\mathbb{Q})$, we thus obtain

$$\xi = \wp(u), \ \eta = \wp'(u).$$

The real period admits an integral representation

$$\omega_1 = 2 \int_\alpha^\infty \frac{dx}{\sqrt{x^3 + k}},$$

where $\alpha = \sqrt[3]{k} \in \mathbb{R}$ is the real root of $x^3 + k$, and the *elliptic logarithm* u of an integer point $P = (\xi, \eta) = (\wp(u), \wp'(u))$ admits the integral representation

$$u = \frac{1}{\omega_1} \int_\xi^\infty \frac{dx}{\sqrt{x^3 + k}} \ (\text{mod } \mathbb{Z}), \tag{4.1}$$

provided that $\xi \geq |\sqrt[3]{k}|$. We shall normalize the elliptic logarithm to

$$u \in \,]-\frac{1}{2}, +\frac{1}{2}].$$

It can be computed by Gauss' arithmetic-geometric mean method or by an algorithm of Zagier [19].

Let $\{P_1, \ldots, P_r\}$ be the basis of the infinite part of $E_k(\mathbb{Q})$ computed in Step 1. Denote by $\lambda_1 \in \mathbb{R}$, $\lambda_1 > 0$, the smallest eigenvalue of the regulator matrix

$$\big(\hat{h}(P_\mu, P_\nu)\big)_{\mu,\nu=1,\ldots,r}$$

associated with the bilinear form $\hat{h}$. Then, any point $P \in E_k(\mathbb{Q})$ in its representation (2.1) in terms of the basis has canonical height

$$\hat{h}(P) = \hat{h}\Big(\sum_{\nu=1}^{r} n_\nu P_\nu + P_{r+1}\Big) \geq \lambda_1 N^2 \tag{4.2}$$

for

$$N = \max_{\nu=1,\dots,r} \{|n_\nu|\} \tag{4.3}$$

in accordance with (2.2). For *integral* points $P = (\xi, \eta) \in E_k(\mathbb{Q})$ whose first coordinate is sufficiently large compared to k, viz.

$$|\xi| > |\sqrt[3]{k}|,$$

we derive from (3.2) and (4.2) the lower estimate

$$\frac{1}{2}\ \log\ |\xi| \geq \hat{h}(P) - \frac{5}{6}\ \log\ 2 \geq \lambda_1 N^2 - \frac{5}{6}\ \log\ 2.$$

We wish to translate this inequality into an upper estimate for the elliptic logarithm u of P. To this end we put

$$\xi_0 = \kappa |\sqrt[3]{k}| \quad \text{with } \kappa = \left\{ \begin{array}{ll} 2 & \text{if } k < 0 \\ \dfrac{2\sqrt[3]{2} - 1}{\sqrt[3]{2} - 1} & \text{if } k > 0 \end{array} \right\}. \tag{4.4}$$

Then, for

$$\xi > \xi_0, \tag{4.5}$$

the following inequality holds:

$$\int_\xi^\infty \frac{dx}{\sqrt{x^3 + k}} < \frac{2\sqrt{2}}{\sqrt{\xi}}.$$

Observing (4.1) and assuming (4.5), we now arrive at the desired upper estimate for the elliptic logarithm u of the given integral point $P = (\xi, \eta) = (\wp(u), \wp'(u)) \in E_k(\mathbb{Q})$:

$$\log |u| < \log(2\sqrt{2}) - \log\ \omega_1 - \lambda_1 N^2 + \frac{5}{6} \log\ 2$$

or

$$|u| < c_1' \exp(-\lambda_1 N^2) \tag{4.6}$$

for

$$c_1' = \frac{2^{\frac{7}{3}}}{\omega_1}.$$

For the sake of simplicity, we eliminate the torsion point in (2.1) by multiplying this representation by the order g of the torsion group. This number g is explicitly known from proposition 3.1. For the point $P' = gP$, the representation (2.1) becomes

$$P' = \sum_{\nu=1}^{r} n_\nu' P_\nu \quad (n_\nu' = g n_\nu \in \mathbb{Z})$$

and this translates into the equation

$$u' = n_0' + \sum_{\nu=1}^{r} n_\nu' u_\nu$$

for the (normalized) elliptic logarithms

$$u' = gu \text{ of } P' \text{ and } u_\nu \text{ of } P_\nu \quad (\nu = 1, \ldots, r).$$

The inequality (4.6) now becomes

$$|u'| < g c_1' \exp(-\lambda_1 N^2). \tag{4.7}$$

On combining this upper bound with an explicit lower bound obtained by S. David [3], we arrive at the desired estimates for the elliptic logarithm of any integer point in $E_k(\mathbb{Q})$. We use the following notation.

Let $\tau = \frac{\omega_2}{\omega_1}$ be such that $\mathrm{im}\,(\tau) > 0$, choose $V_\nu \in \mathbb{R}$ such that

$$\log\ V_\nu \geq \max\left\{\hat{h}(P_\nu),\ \log\ |4k|,\ \frac{3\pi|u_\nu|^2}{\omega_1^2\ \mathrm{im}(\tau)}\right\} \quad (\nu = 1, \ldots, r)$$

and put[2] (cf. [3])

$$C = 2.9 \cdot 10^{6+6r} \cdot 4^{2r^2} \cdot (r+1)^{2r^2+9r+12.3}.$$

[2] This constant is a corrected version of the constant originally given by David.

Theorem 4.1

The elliptic logarithm

$$u = n_0 + \sum_{\nu=1}^{r} n_\nu u_\nu + u_{r+1}$$

of an integer point

$$P = (\wp(u), \wp'(u)) = (\xi, \eta) = \sum_{\nu=1}^{r} n_\nu P_\nu + P_{r+1}$$

with first coordinate of absolute value

$$|\xi| > \xi_0$$

satisfies the inequalities

$$\exp\Big\{-C\ \log^{r+1}|4k|\Big(\log\big(\frac{r+1}{2}gN\big)+1\Big)\Big(\log\ \log\big(\frac{r+1}{2}gN\big)+1\Big)^{r+1}\prod_{\nu=1}^{r}\log V_\nu\Big\}$$
$$\leq |gu| < gc_1'\ \exp(-\lambda_1 N^2)$$

with N from (4.3), ξ_0 from (4.4), c_1' from (4.6) and

$$g = \sharp E_{k,tors}(\mathbb{Q}).$$

Since, for sufficiently large N, the left hand bound exceeds the right hand bound, we can now derive from theorem 4.1 an upper estimate for N and hence, by (4.3), for the coefficients n_ν in the representation (2.1) of all integer points in terms of the basis of $E_k(\mathbb{Q})$.

To achieve this, we introduce the quantities

$$c_1 = \max\Big\{1, \frac{\log(gc_1')}{\lambda_1}\Big\} \quad \text{with } c_1' = \frac{2^{\frac{7}{3}}}{\omega_1}$$

and

$$c_2 = \max\Big\{10^9, \frac{C}{\lambda_1}\Big\}\Big(\frac{\log\ |4k|}{2}\Big)^{r+1}\prod_{\nu=1}^{r}\log\ V_\nu.$$

Then theorem 4.1 tells us that

$$N^2 < c_1 + c_2\ \log^{r+2} N^2.$$

The largest solution of this inequality satisfies

$$N_0 < N_1 = 2^{r+2}\sqrt{c_1c_2}\log^{\frac{r+2}{2}}\left(c_2(r+2)^{r+2}\right),$$

where, in addition, N_1 is subject to the condition

$$N_1 > \max\left\{e^e, (6r+6)^2, \sqrt{\frac{\log(2gc_1')}{\lambda_1}}\right\}.$$

The upper bound for N is the following.

Theorem 4.2

For an integer point

$$P = (\xi, \eta) = \sum_{\nu=1}^{r} n_\nu P_\nu + P_{r+1} \quad (n_\nu \in \mathbb{Z})$$

with first coordinate of absolute value

$$|\xi| > \xi_0,$$

where ξ_0 is defined by (4.4), the maximum

$$N = \max_{\nu=1,\ldots,r}\{|n_\nu|\}$$

satisfies the inequality

$$N \leq N_2 := \max\left\{N_1, \frac{2V}{r+1}\right\} \quad \textit{for } V = \max_{\nu=1,\ldots,r}\{V_\nu\}.$$

5. Reduction of the bound (Step 3)

The bound N_2 for N obtained in theorem 4.2 is very large so that a search for integer points $P \in E_k(\mathbb{Q})$ with coefficients $|n_\nu| \leq N$ is not feasible. That is why we need to reduce this bound N_2. The reduction is accomplished by a numerical diophantine approximation technique due to de Weger [18].

Let therefore C_0 be a suitable positive integer, specifically

$$C_0 \sim N_2^{r+1}.$$

Consider the lattice

$$\Gamma := \langle \underline{e}_1, \ldots, \underline{e}_r, (\lfloor C_0 u_1 \rfloor, \ldots, \lfloor C_0 u_r \rfloor, C_0) \rangle \subseteq \mathbb{R}^{r+1},$$

where $\underline{e}_\nu$ denotes the ν-th unit vector in $\mathbb{R}^{r+1}$. Designate by $l(\Gamma)$ the Euclidean length of the shortest vector in Γ. Then de Weger shows the following. Regard (cf. (4.6))

$$\big| n_0 + \sum_{\nu=1}^{r} n_\nu u \big| < c_1' \ \exp(-\lambda_1 N^2), \qquad N \le N_2 \tag{5.1}$$

as a homogeneous diophantine approximation problem.

Proposition 5.1

If $\hat{N} \in \mathbb{N}$ is such that

$$\hat{N} \le \frac{l(\Gamma)}{\sqrt{r^2 + 5r + 4}},$$

then the diophantine approximation problem (5.1) cannot be solved for $N \in \mathbb{Z}$ within the range

$$\sqrt{\frac{1}{\lambda_1} \log \frac{2^{\frac{7}{3}} C_0}{\omega_1 \hat{N}}} < N \le \hat{N}.$$

The proposition leads to the

Reduction algorithm with starting value $N = N_2$. (Here the symbol $\sim$ means order of magnitude.)

(i) Choose a sufficiently large integer C_0 ($\sim N_2^{r+1}$ or larger).

(ii) Compute an LLL-reduced basis $\{\underline{b}_1, \ldots, \underline{b}_{r+1}\}$ of the lattice Γ.

(iii) Put

$$\hat{N} = 2^{-\frac{r}{2}} ||\underline{b}_1|| / \sqrt{r^2 + 5r + 4}$$

and

$$N_1 = \sqrt{\frac{1}{\lambda_1} \ \log \frac{2^{\frac{7}{3}} C_0}{\omega_1 \hat{N}}}.$$

(iv) If $N_1 \geq \hat{N}$, then choose another (larger) C_0 and go to (ii).
(v) If $N_1 < \hat{N}$, then $N = N_1$ and go to (i).
(vi) Output (N). Stop.

After a sufficient number of reductions, N cannot be reduced any further. It then remains to test all linear combinations

$$P = n_1 P_1 + \cdots + n_r P_r + P_{r+1}$$

with

$$n_\nu \in \mathbb{Z},\ |n_\nu| \leq N\ (\nu = 1, \ldots, r) \text{ and } P_{r+1} \in E_{k,tors}(\mathbb{Q})$$

for integrality of $P \in E_k(\mathbb{Q})$.

An extra search - by sieving - is necessary in order to find all integral points

$$P = (\xi, \eta) \in E_k(\mathbb{Q}) \quad \text{with } \xi \leq \xi_0.$$

As pointed out above, if we employ also p-adic elliptic logarithms we are able to produce all S-integral points on E_k for any finite set S of places (including the infinite one) of $\mathbb{Q}$.

6. Examples and tables

EXAMPLE 1: $E:\ y^2 = x^3 + 108$

rank: 1
basis: (6, 18)
regulator: 0.1501068952
torsion: $\mathcal{O}$
set of primes: $S = \{2,\ 3,\ 5,\ \infty\}$
$12 = 6 \cdot 2$ S-integral points

1. $(6,\ 18) = (6,\ 18)$
2. $(-3,\ 9) = 2 \cdot (6,\ 18)$
3. $(-2,\ 10) = -3 \cdot (6,\ 18)$
4. $(366,\ 7002) = 5 \cdot (6,\ 18)$
5. $(33/4,\ 207/8) = -4 \cdot (6,\ 18)$
6. $(109/25,\ 1727/125) = 6 \cdot (6,\ 18)$

EXAMPLE 2: $E:\ y^2 = x^3 + 225$

rank: 2
basis: $(-6,\,3),\ (-5,\,10)$
regulator: 1.3890930394
torsion: $\mathcal{O},\ (0,\,15),\ (0,\,-15)$
set of primes: $S = \{2,\,3,\,5,\,\infty\}$
$44 = 22 \cdot 2$ S-integral points

1. $(0,\,15) = (0,\,15)$
2. $(-6,\,3) = (-6,\,3)$
3. $(10,\,35) = (0,\,-15) - (-6,\,3)$
4. $(15,\,60) = (0,\,-15) + (-6,\,3)$
5. $(336,\,6159) = -2 \cdot (-6,\,3)$
6. $(180,\,2415) = (-6,\,3) - (-5,\,10)$
7. $(-5,\,10) = (-5,\,10)$
8. $(6,\,21) = (0,\,-15) - (-5,\,10)$
9. $(30,\,165) = (0,\,-15) + (-5,\,10)$
10. $(60,\,465) = -(-6,\,3) - (-5,\,10)$
11. $(4,\,17) = (0,\,15) + (-6,\,3) + (-5,\,10)$
12. $(351,\,6576) = (0,\,-15) + (-6,\,3) + 2 \cdot (-5,\,10)$
13. $(720114,\,611085363) = (0,\,15) - 3 \cdot (-6,\,3) - 2 \cdot (-5,\,10)$
14. $(9/4,\,123/8) = (0,\,15) - (-6,\,3) + (-5,\,10)$
15. $(-15/4,\,105/8) = (0,\,15) - (-6,\,3) - (-5,\,10)$
16. $(385/16,\,7615/64) = -2 \cdot (-5,\,10)$
17. $(105/64,\,7755/512) = (0,\,15) + 2 \cdot (-6,\,3)$
18. $(-20/9,\,395/27) = (0,\,15) + (-6,\,3) - (-5,\,10)$
19. $(550/9,\,12905/27) = (0,\,-15) + 2 \cdot (-6,\,3) + (-5,\,10)$
20. $(130/81,\,11035/729) = (0,\,-15) - (-6,\,3) - 2 \cdot (-5,\,10)$
21. $(99/25,\,2118/125) = (0,\,-15) - 2 \cdot (-6,\,3) - (-5,\,10)$
22. $(2146/25,\,99431/125) = (0,\,-15) - (-6,\,3) + 2 \cdot (-5,\,10)$

EXAMPLE 3: $E: \ y^2 = x^3 + 1025$

rank: 3
basis: (10, 45), (−5, 30), (−10, 5)
regulator: 1.1945306597
torsion: $\mathcal{O}$
set of primes: $S = \{2, 3, 5, \infty\}$
$70 = 35 \cdot 2$ S-integral points

1. $(20, 95) = -(10, 45) + (-5, 30)$
2. $(166, 2139) = 2 \cdot (10, 45) - (-5, 30)$
3. $(10, 45) = (10, 45)$
4. $(-5, 30) = (-5, 30)$
5. $(-4, 31) = -(10, 45) - (-5, 30)$
6. $(3730, 227805) = (10, 45) + 2 \cdot (-5, 30)$
7. $(64, 513) = -(-5, 30) + (-10, 5)$
8. $(446, 9419) = -2 \cdot (10, 45) + (-10, 5)$
9. $(-10, 5) = (-10, 5)$
10. $(4, 33) = -(10, 45) - (-10, 5)$
11. $(155, 1930) = -2 \cdot (10, 45) - (-10, 5)$
12. $(-1, 32) = (10, 45) - (-5, 30) - (-10, 5)$
13. $(40, 255) = -(-5, 30) - (-10, 5)$
14. $(50, 355) = (10, 45) + (-5, 30) + (-10, 5)$
15. $(920, 27905) = -2 \cdot (-10, 5)$
16. $(3631, 218796) = -(10, 45) - 2 \cdot (-5, 30) - 2 \cdot (-10, 5)$
17. $(25/4, 285/8) = -(10, 45) + (-10, 5)$
18. $(985/4, 30915/8) = -(10, 45) + 2 \cdot (-5, 30) + (-10, 5)$
19. $(1/16, 2049/64) = 2 \cdot (10, 45) + (-5, 30) + (10, 5)$
20. $(185/16, 3245/64) = -2 \cdot (-5, 30)$
21. $(-575/64, 8865/512) = -2 \cdot (10, 45) + (-5, 30) - (-10, 5)$
22. $(8201/4096, 8425499/262144) = -2 \cdot (10, 45) + 2 \cdot (-5, 30) + 2 \cdot (-10, 5)$
23. $(10/9, 865/27) = (10, 45) - (-5, 30) + (-10, 5)$
24. $(46/9, 919/27) = 2 \cdot (-5, 30) + (-10, 5)$
25. $(-80/9, 485/27) = 2 \cdot (10, 45)$
26. $(295/9, 5140/27) = (10, 45) + (-5, 30) - (-10, 5)$
27. $(2260/81, 109945/729) = -(10, 45) + (-5, 30) + 2 \cdot (-10, 5)$
28. $(3715/729, 669610/19683) = -2 \cdot (10, 45) - 2 \cdot (-5, 30) - (-10, 5)$
29. $(7114/729, 870137/19683) = -3 \cdot (10, 45) + (-5, 30) - (-10, 5)$
30. $(194380/729, 85701635/19683) = (10, 45) - 3 \cdot (-5, 30)$
31. $(-74/25, 3951/125) = (-5, 30) + 2 \cdot (-10, 5)$

EXAMPLE 3: (continued)

32. $(-206/25,\ 2697/125) = (10,\ 45) - 2 \cdot (-5,\ 30)$
33. $(-215/36,\ 6155/216) = -(10,\ 45) - (-5,\ 30) - 2 \cdot (-10,\ 5)$
34. $(1481/100,\ 65371/1000) = -(10,\ 45) + (-5,\ 30) - 2 \cdot (-10,\ 5)$
35. $(-342614/50625,\ 304585741/11390625) = -3 \cdot (10,\ 45) - (-5,\ 30) + (-10,\ 5)$

EXAMPLE 4: $E:\ y^2 = x^3 + 2089$

rank: 4
basis: $(-4,\ 45),\ (-10,\ 33),\ (8,\ 51),\ (-12,\ 19)$
regulator: 17.5653394266
torsion: $\mathcal{O}$
set of primes: $S = \{2,\ 3,\ 5,\ \infty\}$
$94 = 47 \cdot 2$ S-integral points

1. $(60,\ 467) = (-4,\ 45) - (8,\ 51)$
2. $(183,\ 2476) = -(-4,\ 45) + (-10,\ 33)$
3. $(-4,\ 45) = (-4,\ 45)$
4. $(-10,\ 33) = (-10,\ 33)$
5. $(18,\ 89) = -(-4,\ 45) - (-10,\ 33)$
6. $(8,\ 51) = (8,\ 51)$
7. $(129968,\ 46854861) = 2 \cdot (-4,\ 45) + (8,\ 51)$
8. $(3,\ 46) = -(-10,\ 33) - (8,\ 51)$
9. $(170,\ 2217) = (-4,\ 45) + (-10,\ 33) + (8,\ 51)$
10. $(9278,\ 893679) = (-4,\ 45) + (-10,\ 33) - (8,\ 51) + (-12,\ 19)$
11. $(698,\ 18441) = -(-10,\ 33) + (-12,\ 19)$
12. $(80,\ 717) = -(-4,\ 45) + (-12,\ 19)$
13. $(-12,\ 19) = (-12,\ 19)$
14. $(71,\ 600) = -(-4,\ 45) - (8,\ 51)$
15. $(-15/4,\ 361/8) = -(-4,\ 45) - (8,\ 51)$
16. $(65/4,\ 639/8) = -(8,\ 51) + (-12,\ 19)$
17. $(-39/16,\ 2915/64) = -(-4,\ 45) + (8,\ 51) + (-12,\ 19)$
18. $(425/16,\ 9237/64) = -(-4,\ 45) - (-12,\ 19)$
19. $(42417/64,\ 8735977/512) = (-4,\ 45) + 2 \cdot (-10,\ 33) + (8,\ 51) - (-12,\ 19)$
20. $(-12823/1024,\ 366837/32768) = 2 \cdot (-4,\ 45) - (8,\ 51)$
21. $(-5/9,\ 1234/27) = (-4,\ 45) + (-10,\ 33) - (-12,\ 19)$
22. $(214/9,\ 3365/27) = (-10,\ 33) - (8,\ 51)$
23. $(232/9,\ 3743/27) = (-4,\ 45) + (8,\ 51) - (-12,\ 19)$
24. $(250/9,\ 4141/27) = (-10,\ 33) + (8,\ 51) + (-12,\ 19)$
25. $(191362/9,\ 83711197/27) = (-4,\ 45) - (-10,\ 33) - 2 \cdot (-12,\ 19)$

EXAMPLE 4: (continued)

26. $(-752/81,\ 26171/729) = -(-4,\ 45) + (8,\ 51) - (-12,\ 19)$
27. $(52/729,\ 899623/19683) = 2 \cdot (-10,\ 33) + (-12,\ 19)$
28. $(559/729,\ 899720/19683) = (-4,\ 45) + (-10,\ 33) + 2 \cdot (8,\ 51)$
29. $(12594790/729,\ 44697825539/19683)$
$= -(-4,\ 45) + (-10,\ 33) - 2 \cdot (8,\ 51) + (-12,\ 19)$
30. $(174/25,\ 6157/125) = (-4,\ 45) + (-10,\ 33) + (-12,\ 19)$
31. $(164/25,\ 6087/125) = -(8,\ 51) - (-12,\ 19)$
32. $(-289/25,\ 2916/125) = -(-4,\ 45) - (-10,\ 33) + (8,\ 51)$
33. $(-306/25,\ 1997/125) = (-4,\ 45) - (-10,\ 33) - (-12,\ 19)$
34. $(306/25,\ 7829/125) = (-10,\ 33) + (8,\ 51) - (-12,\ 19)$
35. $(9134/25,\ 872973/125) = -(-10,\ 33) - 2 \cdot (8,\ 51)$
36. $(20319/25,\ 2896372/125) = -2 \cdot (-4,\ 45) - (-10,\ 33) - (8,\ 51) + (-12,\ 19)$
37. $(84116/25,\ 24395961/125) = 2 \cdot (-4,\ 45) - (8,\ 51) - (-12,\ 19)$
38. $(10946/625,\ 1349631/15625) = (-4,\ 45) - (-10,\ 33) + (8,\ 51)$
39. $(37470434/625,\ 229368135873/15625)$
$= -(-4,\ 45) - (-10,\ 33) - (8,\ 51) - 2 \cdot (-12,\ 19)$
40. $(172033/36,\ 71353889/216) = -2 \cdot (8,\ 51) - (-12,\ 19)$
41. $(-60679/6400,\ 18005619/512000) = (-4,\ 45) + 2 \cdot (8,\ 51) - (-12,\ 19)$
42. $(2691681/160000,\ 5296996079/64000000) = -2 \cdot (-10,\ 33) - 2 \cdot (-12,\ 19)$
43. $(1864/225,\ 173987/3375) = -2 \cdot (-4,\ 45)$
44. $(-2876/225,\ 2557/3375) = (-4,\ 45) + 2(-10,\ 33) + (8,\ 51)$
45. $(9160098049/94478400,\ 877702508470657/918330048000)$
$= 2 \cdot (-4,\ 45) + 2 \cdot (-10,\ 33) - 2 \cdot (8,\ 51)$
46. $(5226209/409600,\ 16920395823/262144000)$
$= (-4,\ 45) + 2 \cdot (-10,\ 33) + 2 \cdot (8,\ 51) + (-12,\ 19)$
47. $(83521/8100,\ 41143681/729000) = (-4,\ 45) + 2 \cdot (-10,\ 33) - (8,\ 51)$

6.1 Determination of all S-integral points on Mordell's Equation

$$E_k:\ y^2 = x^3 + k \qquad (k \in \mathbb{Z})$$

for $S = \{2,\ 3,\ 5,\ \infty\}$ and $0 < |k| \leq 10,000$.

S-integral points on Mordell's equation (Summary)

number of S-integral points	curves with rank $r=0$	curves with rank $r=1$	curves with rank $r=2$	curves with rank $r=3$	curves with rank $r=4$	all curves
0	6459	4425	86			10970
1	24					24
2	45	4352	841			5238
4		640	886	6		1532
5	4	7				11
6		67	615	19		703
7		3				3
8		20	419	37		476
10		13	263	48		324
11		3				3
12		9	151	42		203
13		1				1
14		5	66	52		124
16		2	30	53		85
18			24	54		79
20			9	44		53
22			13	30		43
24			5	16		21
26			3	16		19
28			2	14		16
30			1	5		6
32				6	2	7
34			3	5	2	10
36			1	5	1	7
38				6	1	5
40				3	2	5
42				4		4
44			1	2	1	5
46				5	1	6
48			1	1	1	3

S-integral points on Mordell's equation (Summary)

(continued)

number of S-integral points	curves with rank r=0	curves with rank r=1	curves with rank r=2	curves with rank r=3	curves with rank r=4	all curves
52				1	1	2
54				1		1
56					1	1
58				1		1
62					1	1
64					1	1
66					1	1
70				1	1	2
72					1	1
94					1	1
	6532	9547	3426	477	18	20000

6.2 Total and average number of points

Integer points:						
	r=0	r=1	r=2	r=3	r=4	all curves
total number	134	5810	8228	2724	228	17124
average	0.021	0.607	2.402	5.699	12.667	0.856

S-integral points (S $=\{2,3,5,\infty\}$):						
	r=0	r=1	r=2	r=3	r=4	all curves
total number	134	12268	19624	8506	928	41460
average	0.021	1.285	5.728	17.832	51.556	2.073

References

1. A. Baker, The diophantine equation $y^2 = ax^3 + bx^2 + cx + d$, *J. London Math. Soc.* **43** (1968), 1–9.
2. B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves I, II, *J. Reine Angew. Math.* **212** (1963), 7–25, **218** (1965), 79–108.
3. S. David, Minorations de formes linéaires de logarithmes elliptiques, *Publ. Math. Univ. Pierre et Marie Curie* **106**, Problèmes diophantiens 1991-1992, exp. no. 3.
4. R. Fueter, Über kubische diophantische Gleichungen, *Comment. Math. Helv.* **2** (1930), 69–89.
5. J. Gebel, A. Pethö and H. G. Zimmer, Computing integral points on elliptic curves, *Acta Arith.* **68** (1994), 171–192.
6. J. Gebel and H. G. Zimmer, Computing the Mordell-Weil group of an elliptic curve over $\mathbb{Q}$. In: *Elliptic Curves and Related Topics, Eds.*: H. Kisilevsky and M. Ram Murty, CRM Proceed. and *Lect. Notes, Amer. Math. Soc.*, Providence, RI 1994, 61–83.
7. M. Hall, The Diophantine equation $x^3 - y^2 = k$. In: *Computers in Number Theory, Eds.* A. O. L. Atkin and B. J. Birch, Academic Press, London 1971, 173–198.
8. S. Lang, *Elliptic Curves: Diophantine Analysis*, Grundl. Math. Wiss. 231, Springer-Verlag, Berlin 1978.
9. K. Mahler, Über die rationalen Punkte auf Kurven vom Geschlecht Eins, *J. Reine Angew. Math.* **170** (1934), 168–178.
10. Yu. I. Manin, Cyclotomic fields and modular curves, *Russian Math. Surveys* **26** (1971), 7–78.
11. L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, *Proc. Cambr. Philos. Soc.* **21** (1922), 179–192.
12. C. L. Siegel, Über einige Anwendungen diophantischer Approximationen, *Abh. Preuss. Akad. Wiss.* (1929), 1–41.
13. J. H. Silverman, A quantitative version of Siegel's theorem, *J. Reine Angew. Math.* **378** (1981), 60–100.
14. J. H. Silverman, The difference between the Weil height and the canonical height on elliptic curves, *Math. Comp.* **55** (1990), 723–743.
15. N. Smart, S-integral points on elliptic curves, *Proc. Cambr. Phil. Soc.* **116** (1994), 391–399.
16. V. G. Sprindžuk, *Classical Diophantine Equations*, Lect. Notes in Math. 1559, Springer-Verlag, Berlin 1993.
17. H. M. Stark, Effective estimates of solutions of some Diophantine equations, *Acta Arith.* **24** (1973), 251–259.
18. B. M. M. de Weger, *Algorithms for diophantine equations*, PhD Thesis, Centr. for Wiskunde en Informatica, Amsterdam 1987.
19. D. Zagier, Large integral points on elliptic curves, *Math. Comp.* **48** (1987), 425–436.
20. H. G. Zimmer, On the difference of the Weil height and the Néron-Tate height, *Math. Z.* **147** (1976), 35–51.

21. H. G. Zimmer, Generalization of Manin's conditional algorithm. SYMSAC '76. Proc. 1976 ACM Sympos. on Symb. Alg. Comp. Ed. R. D. Jenks, Yorktown Heights, N.Y. 1976, 285–299.
22. H. G. Zimmer, A limit formula for the canonical height of an elliptic curve and its application to height computations. In: *Number Theory*, Ed. R. A. Mollin, W. de Gruyter, Berlin 1990, 641–659.