On Mordell's Equation

Josef Gebel[1*], Attila Pethő[2†], Horst G. Zimmer[3]

November 28, 2009

[1] Department of Computer Science and Engineering, Concordia University, Montréal PQ H5G 1M8, Canada. e-mail: sebp@cs.concordia.ca
[2] University of Medicine, Laboratory of Informatics, Nagyerdei Krt. 98, H-4032 Debrecen, Hungary. e-mail: pethoe@peugeot.dote.hu
[3] Universität des Saarlandes, Fachbereich 9 Mathematik, D-66041 Saarbrücken, Germany. e-mail: zimmer@math.uni-sb.de

Summary

In an earlier paper we developed an algorithm for computing all integral points on elliptic curves over the rationals $\mathbb{Q}$. Here we illustrate our method by applying it to Mordell's equation $y^2 = x^3+k$ for $0 \neq k \in \mathbb{Z}$ and draw some conclusions from our numerical findings. In fact we solve Mordell's equation in $\mathbb{Z}$ for all integers k within the range $0 < |k| \leq 10\,000$ and partially extend the computations to $0 < |k| \leq 100\,000$. For these values of k, the constant in Hall's conjecture turns out to be $C = 5$. Some other interesting observations are made concerning large integer points, large generators of the Mordell-Weil group and large Tate-Shafarevič groups. Three graphs illustrate the distribution of integer points in dependence on the parameter k. One interesting feature is the occurrence of lines in the graphs.

*Research partly supported by the DFG
†Research supported in part by Hungarian National Foundation for Scientific Research Grant No. 16791/95.

1 Introduction

Mordell's equation

$$E: \; y^2 = x^3 + k, \quad 0 \neq k \in \mathbb{Z}, \tag{1}$$

has a long history. Various methods have been applied to solve it or to prove some assertions about its number of solutions. An illuminating account of these endeavors is given in Mordell's book [Mo].

We are interested in finding all integer solutions of Mordell's equation for a large range of parameters k. The numerical results obtained are then used to estimate the constant in Hall's conjecture and to illustrate in three graphs the distribution of integer points.

Until recently, Mordell's equation could be completely solved in rational integers only for parameters $k \in \mathbb{Z}$ within the range (see [LF])

$$|k| \leq 100$$

and – with certain exceptions – within the range (see [SM])

$$100 < k \leq 200$$

as well as for some special higher values of k, e.g. $k = -999$ (see [Ste]). "Small" solutions, i.e. solutions with $|y| \leq 10^{10}$ were computed for the much larger range

$$|k| \leq 10\,000$$

(see [LJB]).

However, recent progress in the theory, the availability of very efficient algorithms based on the theory and advanced computer technology enable us meanwhile to completely solve Mordell's equation in rational integers for

$$|k| \leq 10\,000$$

and for almost all $k \in \mathbb{Z}$ within the interval

$$|k| \leq 100\,000.$$

Here 'almost all' means for all but about 1000 curves for which we could not find any integer point with first coordinate less than 10^{28} in absolute value.

This range of the parameter k is already large enough to provide suitable data to test the constants in Hall's conjecture [Ha]. Our theoretical findings lead to a bound for the coordinates of integer points which is exponentially worse than the bound established by Stark ([Sta], cf. also [Sp]). That is why we do not elaborate on this topic here.

The method for determining all integer points on elliptic curves over the rationals is based on ideas of Lang and Zagier [Za] and was described already in our paper [GPZ1]. In this article, we use Mordell's equation to illustrate our method, and we briefly explain the point search by sieving, not explained in [GPZ1]. The determination of all integer points has two ingredients. The first is an efficient and unconditional algorithm for computing the rank and a basis of the group of rational points $E(\mathbb{Q})$ of an elliptic curve E over the rationals $\mathbb{Q}$ developed in [GZi]. The second is an explicit lower bound for linear forms in elliptic logarithms established by David [Dav]. We mention that essentially the same method was also used by Stroeker and Tzanakis [STz]. However, they do not employ Manin's conditional algorithm described in [GZi].

The numerical results obtained include curves with large Tate-Shafarevič groups, curves with large generators and curves with large integer points. In his review of the paper [LJB] (see MR 33#91), Cassels claims that the largest integer solutions within the range $|k| \leq 10\,000$ are (for $k > 0$ or $k < 0$, respectively)

$$1\,775\,104^3 - 2\,365\,024\,826^2 = -5\,412,$$
$$939\,787^3 - 911\,054\,064^2 = 307.$$

However, we found the larger solutions

$$6\,369\,039^3 - 16\,073\,515\,093^2 = -7\,670,$$
$$110\,781\,386^3 - 1\,166\,004\,406\,095^2 = 8\,569.$$

One experimental observation derived from the tables is that the rank r of Mordell's curves grows according to

$$r = O(\log|k|/|\log\log|k||^{\frac{2}{3}}).$$

Three graphs illustrate the distribution of integer points for different parameters k. The graphs give rise to some interesting theoretical observations.

For lack of space, not all of the numerical data we obtained could be reproduced here[1].

We have extended our algorithm and calculations to S-integral points on Mordell's equation. A preliminary report on this is given in [GPZ2]. (See also [G].)

Acknowledgment. We wish to thank the referee for many valuable suggestions.

2 Determination of a Basis

In this section we will introduce an algorithm to determine the torsion group, the rank and a basis of the free part of the Mordell–Weil group $E(\mathbb{Q})$. The algorithm is conditional in that it is based on the truth of the conjecture of Birch and Swinnerton-Dyer [BSD].

However, by the work of Coates-Wiles, Greenberg, Gross-Zagier, Rubin and Kolyvagin (see [CW], [Gre] [GZa], [Ru1], [Ru2], [Ko1], [Ko2]) for ranks $r = 0$ and $r = 1$, the conjecture is a theorem provided the curve in question is modular. The Mordell curves have complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$ and thus are, a fortiori, modular. On the other hand, Cremona [Cr] has developed a method to determine the rank of an elliptic curve over $\mathbb{Q}$, if the 2-part of the Tate-Shafarevič group is trivial. With these results, we were able to show that the ranks conjecturally obtained by our algorithm are the true ranks for all parameters k within the range $|k| \leq 10\,000$ with the exception of two curves. The exceptions are the curves (1) for $k = -7\,954$ and $8\,206$. In these cases, the conjectured rank of $E/\mathbb{Q}$ is 2 and the order of the Tate-Shafarevič group is conjectured to be 4. However, in these two cases, a 3-descent yields the correctness of the ranks (and the Tate-Shafarevič groups as well). Therefore, our numerical results for $|k| \leq 10\,000$ are in fact independent of any conjecture.

We will use an example (see section 2.1) taken from [BMG] to illustrate the execution of our algorithm. In the example we shall use throughout the type $\mathsf{sans\ serif}$. The floating point values will be given with an accuracy of eight decimal digits.

[1]Additional data can be obtained via ftp under the address ftp.math.uni-sb.de in /pub/simath/mordell

For an arbitrary elliptic curve E over $\mathbb{Q}$ we denote by

$\mathcal{N}$	the conductor,
R	the regulator,
Ш	the Tate–Shafarevič group,
ω_1	the real period,
c_p	the p-th Tamagawa number.

Conjecture of Birch and Swinnerton-Dyer

(i) The rank r of $E/\mathbb{Q}$ is equal to the order of the zero of the L-series $L(E,\,s)$ of $E/\mathbb{Q}$ at the argument $s = 1$.

(ii) The first non-zero term in the Taylor-expansion of the L-series is

$$\lim_{s\to 1}\frac{L(E,\,s)}{(s-1)^r} = \frac{\Omega\cdot\#\text{Ш}\cdot R}{(\#E_{\mathrm{tors}}(\mathbb{Q}))^2}\cdot\prod_{p\mid\mathcal{N}} c_p,$$

where $\Omega = c_\infty\cdot\omega_1$ with $c_\infty :=$ number of connected components of $E(\mathbb{R})$.

2.1 The Torsion Group

For computing the torsion subgroup of $E(\mathbb{Q})$ for Mordell's curve, we use the following proposition which is due to Fueter [Fu].

Proposition 1 *Let $k = m^6\cdot k_0$, where $m,\,k_0\in\mathbb{Z}$ and k_0 is free of sixth power prime factors. Then the torsion subgroup of $E:\ y^2 = x^3 + k$ over $\mathbb{Q}$ is*

$$E_{\mathrm{tors}}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/6\mathbb{Z} & \text{if } k_0 = 1,\\ \mathbb{Z}/3\mathbb{Z} & \text{if } k_0 \text{ is a square different from } 1, \text{ or } k_0 = -432,\\ \mathbb{Z}/2\mathbb{Z} & \text{if } k_0 \text{ is a cube different from } 1,\\ \{\mathcal{O}\} & \text{otherwise,}\end{cases}$$

the points of order 2 being $(-a,\,0)$ if $k = a^3$ and the points of order 3 being $(0,\,\pm b)$ if $k = b^2$ and $(12m^2,\,\pm 36m^3)$ if $k = -432m^6$.

Hence, the order of the torsion subgroup $E_{\mathrm{tors}}(\mathbb{Q})$ is

$$g \le 6.$$

Example: Let

$$E: \ y^2 = x^3 - 66\,688\,704. \tag{2}$$

We have the factorization

$$-66\,688\,704 = -2^6 \cdot 3^3 \cdot 38\,593$$

and thus, by Proposition 1, the torsion subgroup is $E_{\mathrm{tors}}(\mathbb{Q}) = \{\mathcal{O}\}$.

2.2 The Rank

From the first part of the Birch and Swinnerton–Dyer conjecture we conclude that the rank r of $E/\mathbb{Q}$ can be determined as

$$r = \min\{\rho \geq 0 \mid L^{(\rho)}(E,\, 1) \neq 0\}.$$

In order to compute the L-series and its derivatives at $s = 1$, we need to know the sign $C = \pm 1$ of the functional equation of $E/\mathbb{Q}$. It can be computed either by means of the Fricke involution (see [Cr]) or by evaluating the Hecke equation

$$F(z) = -\frac{C}{\mathcal{N} z^2} F\Big(-\frac{1}{\mathcal{N} z}\Big)$$

of the inverse Mellin transform

$$F(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i z}$$

of the L-series of $E/\mathbb{Q}$. If

$$F\left(\frac{i}{\sqrt{\mathcal{N}}}\right) \neq 0,$$

then $C = 1$; otherwise we evaluate the Hecke equation at a point $z \neq \frac{i}{\sqrt{\mathcal{N}}}$ and derive the value of C. Conjecturally,

$$C = (-1)^r$$

(cf. [BSt]).

Example: First, we determine the conductor

$$\mathcal{N} = 214\,476\,429\,456$$

by an algorithm of Tate [Ta]. After having evaluated $360\,000$ coefficients of the Fourier series $F(z)$ in our example we find the approximation

$$\tilde{F}(\frac{i}{\sqrt{\mathcal{N}}}) = 37\,647.904,$$

of $F(\frac{i}{\sqrt{\mathcal{N}}})$ so that the sign of the functional equation must be $C = +1$ (since $F(\frac{i}{\sqrt{\mathcal{N}}}) = 0$ if $C = -1$).

We also get the approximation $\tilde{L}$ of the L-series of $E/\mathbb{Q}$ at $s = 1$

$$\tilde{L}(E,\,1) \quad = \quad 0.00000009.$$

and we 'conclude' (see the remark below) that $L(E,\,1) = 0$.

For the first, second and third derivative of the L-series at $s = 1$ we obtain the approximations

$$\begin{aligned} \tilde{L}^{(1)}(E,\,1) &= 0.00000018 \\ \tilde{L}^{(2)}(E,\,1) &= 0.00000003 \\ \tilde{L}^{(3)}(E,\,1) &= 0.00000005 \end{aligned}$$

and, again, we conclude that $L^{(\rho)}(E,\,1) = 0$ for $\rho = 1,\,2,\,3$.

Our approximation of the fourth derivative of the L-series at $s = 1$ is

$$\tilde{L}^{(4)}(E,\,1) = 11\,576.437$$

Thus we conjecture that the rank of E over $\mathbb{Q}$ is $r = 4$. We then prove by general 2-descent that the rank is indeed $r = 4$.

Remark: In order to prove that the ρ-th derivative of the L-series of $E/\mathbb{Q}$ at $s = 1$ is zero we assume that $r = \rho$ is the rank of $E/\mathbb{Q}$ and insert the values for r and $L^{(r)}(E,\,1)$ into the estimate (4) given below for the regulator R. With this upper bound for R we try to compute a basis of $E(\mathbb{Q})$. If we are not able to find a basis, the rank must be larger than ρ and thus $L^{(\rho)}(E,\,1) = 0$.

In general, we use three different methods for computing the rank: the first part of the Birch and Swinnerton-Dyer conjecture, general 2-descent or 3-descent via isogeny. Our results are unconditional for $|k| \leq 10.000$. (For details, see [G]).

2.3 Determining a Basis of the Free Part

In the former section, we showed how to determine the rank r of $E/\mathbb{Q}$. Therefore, in the sequel, we may suppose that r is known. From the second part of the Birch and Swinnerton-Dyer conjecture, we derive an upper bound R' for the regulator R of $E/\mathbb{Q}$, assuming that Ш is finite.

Now, the algorithm for determining a basis of the Mordell-Weil group is based on the following fundamental theorem.

Theorem 1 (Manin)
Let

$$B := \frac{2^r}{\gamma_r} R'/(\mu_1 \ldots \mu_{r-1}) \leq \frac{2^r}{\gamma_r} R'/\mu_1^{r-1},$$

where γ_r denotes the volume of the r-dimensional unit ball and

$$0 < \mu_1 < \ldots < \mu_{r-1}$$

are the first $r-1$ successive minima of the lattice $E(\mathbb{Q})$ in $E(\mathbb{Q}) \otimes_Z \mathbb{R}$ (see [Ma]). Then the set

$$\{P \in E(\mathbb{Q}) \backslash E_{\mathrm{tors}}(\mathbb{Q}) \mid \hat{h}(P) < B\}$$

generates a subgroup $\tilde{E}(\mathbb{Q})$ of $\hat{E}(\mathbb{Q}) := E(\mathbb{Q})/E_{\mathrm{tors}}(\mathbb{Q})$ of finite index.

Proof: See [Ma].

Note that μ_1 can be replaced by a lower bound $0 < \mu_1' \leq \mu_1$ defined by

$$\mu_1' = \begin{cases} \delta, \text{ if } M_\delta := \{P \in E(\mathbb{Q}) \backslash E_{\mathrm{tors}}(\mathbb{Q}) \mid h(P) < 2\delta\} \text{ is empty} \\ \mu_1 = \min\{\hat{h}(P) \mid P \in M_\delta\} \text{ otherwise,} \end{cases}$$

where δ is an upper bound for the difference between the Weil height h and the Néron–Tate height $\hat{h}$ on $E(\mathbb{Q})$, i.e. (cf. [GPZ1])

$$|h(P) - \hat{h}(P)| < \delta \quad \forall P \in E(\mathbb{Q}).$$

The symmetric bilinear form associated with the Néron-Tate height on $E(\mathbb{Q})$ will also be denoted by $\hat{h}$.

If we want to apply the above theorem, we have to find all points of bounded Néron-Tate height $\hat{h}(P) < B$ on $E/\mathbb{Q}$. At first sight, this seems to be impossible since we do not know where to search for these points nor when we have found them all. This is where the ordinary Weil height $h(P)$ defined below comes into play. It is very easy to find all the points of bounded (ordinary) Weil height and, since the difference between the two height functions is bounded by a constant δ which does not depend on $P \in E(\mathbb{Q})$, we are also able to find all points of bounded Néron–Tate height $\hat{h}(P) < B$ and thus a generating set of $\tilde{E}(\mathbb{Q})$:

- We find (by a sieving procedure, cf. section 4) all the points
$$P = (\frac{\xi}{\zeta^2}, \frac{\eta}{\zeta^3})$$
such that
$$h(P) = \log(\max\{|\xi|,\ \zeta^2) < B + \delta.$$
- We keep those points P with
$$h(P) < B + \delta \quad \text{ and } \quad \hat{h}(P) < B.$$

The bound δ can be computed by using a method of Zimmer ([Zi1], [Zi2], [Zi3]) or Silverman ([Si]). For Mordell's equation, we derive from [Zi2], [Zi3]) the estimate
$$\delta \le \frac{1}{3}\log|k| + \frac{10}{3}\log 2 \tag{3}$$
which is slightly better than Silverman's bound cf. [Si]
$$\delta \le \frac{1}{3}\log|k| + 2.96.$$
Note that the Néron-Tate height $\hat{h}$ that we use is twice the Néron-Tate height in Silverman's paper.

In order to compute the bound B we need to know an upper bound R' for the regulator R of $E/\mathbb{Q}$. To this end, we apply the second part of the Birch and Swinnerton–Dyer conjecture. Assuming $\infty > \#Ш \ge 1$, we have
$$R' = \frac{L^{(r)}(E,\,1)\cdot(\#E_{\text{tors}}(\mathbb{Q}))^2}{r!\cdot\Omega\cdot\prod_{p|\mathcal{N}} c_p} \ge R. \tag{4}$$
The real period ω_1 of $E/\mathbb{Q}$ can be computed by a very efficient method developed by D. Grayson [Gra] using the Gaussian arithmetic-geometric

mean. The Tamagawa numbers c_p are also obtained by Tate's algorithm [Ta] for determining the conductor $\mathcal{N}$ of $E/\mathbb{Q}$.

Example: By Tate's algorithm we get

$$\mathcal{N} = 214\,476\,429\,456 = 2^4 \cdot 3^2 \cdot 38\,593^2$$

and

$$c_2 = 1,\ c_3 = 2,\ c_{38\,593} = 1.$$

The algorithm also returns a global minimal equation

$$E' : \quad y'^2 = x'^3 - 1\,042\,011$$

for E which is different from our model (2). Since, in the course of the algorithm, it is more convenient to work with a minimal model of E, we will continue our computations with the model E' of our curve. When we have a basis on the minimal model, we only need to transform the basis points back to the original model via the birational transformation $x' = (\frac{1}{2})^2 x,\ y' = (\frac{1}{2})^3 y$.

By (3) we compute

$$\delta = 6.92937829$$

whereas the method of Silverman yields $\delta = 7.57888769$ for the difference between the Néron-Tate height and the Weil height on the minimal model E'.

By the method of Grayson, we compute the real period

$$\omega_1 = 0.24120501.$$

Since the discriminant $\Delta = -469\,059\,951\,220\,272$ of (the minimal model of) our curve is negative, $E(\mathbb{R})$ has only one connected component and thus

$$\Omega = \omega_1.$$

We insert all these values in (4) and obtain

$$R' = \frac{11\,576.437 \cdot 1^2}{4! \cdot 0.241 \cdot 1 \cdot 2 \cdot 1} = 999.879$$

By a sieving procedure we find the point $P_1 \in E(\mathbb{Q})$ listed below and hence

$$\mu_1 = \mu_1' = \hat{h}((255,\ 3\,942)) = 4.13154139.$$

Combining these results yields

$$B := \frac{2^4 \cdot 999.879}{\frac{\pi^2}{2} \cdot 4.13^3} = 46.02$$

and

$$B + \delta := 6.93 + 46.02 = 52.95.$$

Of course, this is only an upper bound for our search region. As soon as we have found r linearly independent points on the curve we stop the search procedure. The first four linearly independent points (and their Néron-Tate heights) that we find are

$$\begin{aligned}
&P_1 = (255,\ 3\,942), \quad \hat{h}(P_1) = 4.1315413974\\
&P_2 = (115,\ 692), \quad \hat{h}(P_2) = 5.2383463867\\
&P_3 = (409/4,\ 1\,315/8), \quad \hat{h}(P_3) = 6.5590924826\\
&P_4 = (25\,275/169,\ 3\,334\,176/2197), \quad \hat{h}(P_4) = 8.8809956275.
\end{aligned}$$

Next, we determine the regulator of the four points $P_1,\ P_2,\ P_3,\ P_4$

$$\mathrm{Reg}(P_1,\ P_2,\ P_3,\ P_4) = \det \hat{h}(P_\mu,\ P_\nu)_{1\le\mu,\nu\le 4} = 999.879$$

which is equal to the upper bound R' for the regulator R obtained by the conjecture of Birch and Swinnerton-Dyer. If $\{P_1,\ P_2,\ P_3,\ P_4\}$ were not a basis of $E(\mathbb{Q})$, then the size of regulator R of $E(\mathbb{Q})$ would be at most $R'/4 = 249.96970665$. By inserting this new upper bound for R and the values $\mu_i = \hat{h}(P_i), 1 \le i \le 3$, into formula (4) we find

$$B = 5.71;$$

but there are only 2 linearly independent points with Néron-Tate height less than 5.71 which is a contradiction to $\mathrm{rank}(E/\mathbb{Q}) = 4$. Thus, $\{P_1,\ P_2,\ P_3,\ P_4\}$ must be a basis of $E(\mathbb{Q})$.

We still have to transform the basis points back to the original model (2) of our curve:

$$\begin{aligned}
P_1 &\to (1\,020,\ 31\,536)\\
P_2 &\to (460,\ 5\,536)\\
P_3 &\to (409,\ 1\,315)\\
P_4 &\to (101\,100/169,\ 26\,673\,408/2\,197).
\end{aligned}$$

Note that the Néron-Tate height $\hat{h}$ is invariant under birational transformations.

Remark: We use the second part of the Birch and Swinnerton-Dyer conjecture to obtain an upper bound for the regulator, but once we have found a basis we can prove that these points really form a basis. Thus our calculations are eventually unconditional.

3 A bound for integer points

Let $E/\mathbb{Q}$ be an elliptic curve with rank r and basis $\{P_1, \dots, P_r\}$ of the infinite part of $E(\mathbb{Q})$. Then, any point $P \in E(\mathbb{Q})$ can be represented as

$$P = \sum_{i=1}^{r} n_i P_i + P_{r+1} \qquad (n_i \in \mathbb{Z}), \tag{5}$$

where $P_{r+1} \in E_{\mathrm{tors}}(\mathbb{Q})$ is a torsion point. Our aim is to find an upper bound $N \in \mathbb{N}$ such that

$$P \text{ is integral} \quad \Longrightarrow \quad |n_i| \le N \quad (\forall\, 1 \le i \le n).$$

3.1 Finding an initial bound

In this section we briefly describe the method presented in [GPZ1]. It is based on an explicit estimation of linear forms in elliptic logarithms.

Let r be the rank, $P_1, \dots, P_r$ be a basis and g be the order of the torsion subgroup of the elliptic curve $E/\mathbb{Q}$ defined by Mordell's equation (1).

Denote by ω_1 and ω_2 the real and complex period of E, respectively, define $\tau = \pm\dfrac{\omega_2}{\omega_1}$ such that $\operatorname{Im}\tau > 0$, and take λ_1 to be the smallest eigenvalue of the regulator matrix $(\hat{h}(P_\mu, P_\nu))_{1 \le \mu,\nu \le r}$ associated with the basis $P_1, \dots, P_r$. We designate by $u_i \in]-\frac{1}{2}, \frac{1}{2}]$ the elliptic logarithm of the point P_i.

Then, according to [GPZ1], we define

$$\xi_0 = \begin{cases} 2|k|^{\frac{1}{3}} & \text{if } k < 0 \\ ck^{\frac{1}{3}} & \text{if } k > 0, \text{ where } c = 5.85. \end{cases}$$

Let

$$P = (\xi, \eta) = (\wp(u), \wp'(u)) = \sum_{i=1}^{r} n_i P_i + P_{r+1} \in E(\mathbb{Q})$$

be any integer point on $E/\mathbb{Q}$ parameterized by the Weierstrass $\wp$-function and

$$u = n_0 + \sum_{i=1}^{r} n_i u_i + u_{r+1} \quad (n_i \in \mathbb{Z})$$

be its elliptic logarithm. In order to get rid of the torsion point, we consider the point $P' = g \cdot P$ and its elliptic logarithm $u' = gu$ in the corresponding representation

$$u' = n_0' + \sum_{i=1}^{r} n_i' u_i \quad (n_i' = g \cdot n_i).$$

The following proposition from [GPZ1] gives us lower and upper estimates for the elliptic logarithm of an integer point.

Proposition 2 *Let $P = (\xi, \eta) = (\wp(u), \wp'(u))$ with $\xi > \xi_0$ be an integer point on $E/\mathbb{Q}$ and put $P' = gP$. The elliptic logarithm $u' = gu$ of P' satisfies the estimate*

$$\begin{aligned} &\exp\left\{-Ch^{r+1}(\log(\frac{r+1}{2}gN)+1)(\log\log(\frac{r+1}{2}gN)+1)^{r+1}\prod_{i=1}^{r}\log V_i\right\} \\ &\qquad \le |g \cdot u| \\ &\qquad < \exp\left\{-\lambda_1 N^2 + \log(g \cdot c_1')\right\}, \end{aligned}$$

where the constant C (see [Dav]) is given by[2]

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

and

$$\begin{aligned} h &= \log 4|k|, \\ V_i &= \exp\max\left\{\hat{h}(P_i),\, h,\, \frac{3\pi u_i^2}{\omega_1^2 \mathrm{Im}\,\tau}\right\} \quad (1 \le i \le r), \\ V &= \max_{1\le i\le r}\{V_i\}, \\ c_1' &= \frac{2^{\frac{7}{3}}}{\omega_1}. \end{aligned}$$

The following theorem, also from [GPZ1], enables us to find an initial upper bound for N.

[2] This expression for C is a correction of the value of C used in [GPZ1]

Theorem 2 *Let*

$$P = (\xi,\, \eta) = \sum_{i=1}^{r} n_i P_i + P_{r+1} \in E(\mathbb{Q})$$

be an integer point on $E/\mathbb{Q}$ as in (5) with first coordinate $\xi > \xi_0$. Then, the number

$$N = \max_{1 \le i \le n} \{|n_i|\}$$

satisfies the inequality

$$N \le N_2 := \max\left\{N_1,\, \frac{2V}{r+1}\right\},$$

where

$$N_1 = 2^{r+2}\sqrt{c_1 c_2}\,\log^{\frac{r+2}{2}}\left(c_2(r+2)^{r+2}\right)$$

for

$$c_1 = \max\left\{\frac{\log(gc_1')}{\lambda_1},\, 1\right\}$$

and

$$c_2 = \max\left\{\frac{C}{\lambda_1}, 10^9\right\}\left(\frac{h}{2}\right)^{r+1}\prod_{i=1}^{r}\log V_i.$$

Example: Also by a method of Grayson, we compute the complex period

$$\omega_2 = 0.12060251 + 0.20888326\,i \quad \text{and the imaginary part} \quad \operatorname{Im}\tau = 0.86603868.$$

The smallest eigenvalue of the regulator matrix is

$$\lambda_1 = 3.20488705.$$

The elliptic logarithms of the basis points are

$$\begin{aligned} u_1 &= 0.26081931, \\ u_2 &= 0.41475763, \\ u_3 &= 0.47802466, \\ u_4 &= 0.34771489. \end{aligned}$$

Then, we have

$$\xi_0 = 2 \cdot 66\,688\,704^{\frac{1}{3}} = 811.04961324.$$

We will need ξ_0 to carry out an extra search for points with x-coordinate less than or equal to ξ_0, since the theorem is only valid for those points $P = (\xi, \eta)$ with $\xi > \xi_0$.

David's constant is

$$C = 2.9 \cdot 10^{6r+6} \cdot 4^{2r^2} \cdot (r+1)^{2r^2+9r+12.3} \sim 2.5 \cdot 10^{105}.$$

We also compute the values

$$\begin{aligned}
h &= \log(4 \cdot 66688704) \sim 19.40184050, \\
V_1 &= \exp(h) = \exp(19.40184050) \sim 2.7 \cdot 10^8, \\
V_2 &= \exp\left\{\frac{3\pi u_2^2}{\omega_1^2 \operatorname{Im}\tau}\right\} = \exp(32.17732563) \sim 9.4 \cdot 10^{13}, \\
V_3 &= \exp\left\{\frac{3\pi u_3^2}{\omega_1^2 \operatorname{Im}\tau}\right\} = \exp(42.75259814) \sim 3.7 \cdot 10^{19}, \\
V_4 &= \exp\left\{\frac{3\pi u_4^2}{\omega_1^2 \operatorname{Im}\tau}\right\} = \exp(22.61558126) \sim 6.6 \cdot 10^{9}, \\
V &= V_3, \\
c_1 &= \max\{0.93035703,\, 1\} = 1, \\
c_2 &\sim 4.0 \cdot 10^{115}.
\end{aligned}$$

Our initial bound N_2 can now be determined. We have

$$N_1 = 2^6 \cdot \sqrt{c_1 \cdot c_2} \cdot \log^3(c_2 \cdot 6^6) \sim 8.6 \cdot 10^{66}$$

and obtain

$$N_2 = \max\{N_1, 2 \cdot \frac{V}{5}\} = \max\{N_1, 1.5 \cdot 10^{19}\} = N_1 \sim 8.6 \cdot 10^{66}.$$

3.2 Reduction of the initial bound

Since, in general, the bound $N_2 \geq N$ is very large, we have to reduce it to an appropriate size. This is done by a method of de Weger ([dW]) which is based on LLL-reduction (see [LLL]).

In order to reduce the bound for N, we consider the two inequalities

$$\left| n_0' + \sum_{i=1}^{r} n_i' u_i \right| < g c_1' \exp\{-\lambda_1 N^2\} \tag{6}$$

and

$$N \leq N_2$$

as a homogeneous diophantine approximation problem. We will only give a brief description of de Weger's method and refer the reader to [GPZ1] or [dW] for more details .

Let C_0 be a suitable positive integer, viz. $C_0 \sim N_2^{r+1}$, and Γ be the lattice spanned by the $r+1$ vectors

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \lfloor C_0 u_1 \rfloor \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ \lfloor C_0 u_r \rfloor \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ C_0 \end{pmatrix},$$

where $\lfloor C_0 u_i \rfloor$ denotes the largest integer less than or equal to $C_0 u_i$ $(1 \leq i \leq r)$. The Euclidean length of the shortest non-zero vector of Γ is denoted by $l(\Gamma)$. Lemma 3.7 of [dW] states that if $\tilde{N}$ is a positive integer such that

$$l(\Gamma) \geq \sqrt{r^2 + 5r + 4} \cdot \tilde{N},$$

then (6) cannot hold for N within the range

$$\sqrt{\frac{1}{\lambda_1} \log \frac{2^{\frac{7}{3}} \cdot C_0}{\omega_1 \tilde{N}}} < N \leq \tilde{N}. \tag{7}$$

If $\{\underline{b}_1, \ldots, \underline{b}_{r+1}\}$ is an LLL-reduced basis for Γ, then we have

$$l(\Gamma) \geq 2^{-\frac{r}{2}} \|\underline{b}_1\|,$$

where $\|\underline{b}_1\|$ is the Euclidean length of the shortest vector $\underline{b}_1$. We take

$$\tilde{N} = 2^{-\frac{r}{2}} \|\underline{b}_1\| (\sqrt{r^2 + 5r + 4})^{-1}.$$

Then we replace N_2 by the left hand side of (7) and repeat this procedure recursively until no further reduction can be achieved.

The task remains to compute all linear combinations

$$\sum_{i=1}^{r} n_i P_i + P_{r+1}$$

for $|n_i| \le N$ and $P_{r+1} \in E_{\mathrm{tors}}(\mathbb{Q})$.

Example: Starting with $N_2 = 8.6 \cdot 10^{66}$ and $C_0 = 10^{335} \sim N_2^5$, we compute an LLL-reduced basis of Γ with

$$\|\underline{b}_1\| = 9.1 \cdot 10^{66}.$$

We also determine

$$\tilde{N} \sim 4.5 \cdot 10^{65}$$

and find the new upper bound $N_2 = 13$ for N.

Note that, since $C_0 = 10^{335}$, we have to approximate the elliptic logarithms u_i of the basis points P_i with an accuracy up to at least 335 digits.

A second reduction yields $N = N_2 = 2$ which cannot be reduced any further.

Since the torsion group is trivial, we only have to test all linear combinations

$$\sum_{i=1}^{4} n_i P_i \quad \text{for } |n_i| \le 2 \ (1 \le i \le 4).$$

We find the following 8 integer points

$$\begin{gathered}
(409,\ 1\,315) = P_3,\\
(409,\ -1\,315) = -P_3,\\
(460,\ 5\,536) = P_2,\\
(460,\ -5\,536) = -P_2,\\
(1\,020,\ 31\,536) = P_1,\\
(1\,020,\ -31\,536) = -P_1,\\
(606\,365\,857,\ 14\,931\,454\,281\,967) = 2 \cdot P_1 + P_3,\\
(606\,365\,857,\ -14\,931\,454\,281\,967) = -2 \cdot P_1 - P_3.
\end{gathered}$$

The extra search procedure for points (ξ, η) with $\xi \le \xi_0 = 811.04961324$ yields the four points

$$(409,\ \pm 1\,315) \quad \text{and} \quad (460,\ \pm 5\,536)$$

already found previously. Thus, the 8 points listed above are the only integer points on E over the rationals.

4 Sieving

The sieving procedure is not explained in [GPZ1]. That is why we discuss it briefly here.

In order to find a basis of the Mordell-Weil group, we have to determine all points

$$P = (x,\, y) = \left(\frac{\xi}{\zeta^2},\, \frac{\eta}{\zeta^3}\right), \quad \xi,\, \eta,\, \zeta \in \mathbb{Z},\ (\xi,\ \zeta) = 1 = (\eta,\ \zeta),$$

on the curve (1) such that[3]

$$d(P) = \log \max\{|\xi|,\ |\zeta^6 k|^{\frac{1}{3}}\} < B', \tag{8}$$

where

$$B' := B + \delta + \frac{1}{3}\log 4\,|k|.$$

Similarly, to find all integer points on E by the method presented we have to test for all pairs $(\xi,\, \eta) \in \mathbb{Z}^2$ with $|\xi| < \xi_0$ whether or not they lie on E.

After this remark we come back to equation (1) with the extra condition (8).

First, we change the rational equation

$$E:\ \left(\frac{\eta}{\zeta^3}\right)^2 = \left(\frac{\xi}{\zeta^2}\right)^3 + k$$

into an equation over the integers

$$E_\zeta:\ \eta^2 = \xi^3 + \zeta^6 k =: f_\zeta(\xi) \tag{9}$$

by multiplying the equation for E with ζ^6.

From (8) and (9), we see that we have to consider the equation

$$E_\zeta:\ \eta^2 = f_\zeta(\xi)$$

for each integer $\zeta \in [1,\ \lfloor\exp\{B'/2\}\rfloor]$ subject to the condition

$$\xi \in [\max\left\{\lfloor -\zeta^2|k|^{\frac{1}{3}}\rfloor,\ -\lfloor\exp B'\rfloor\right\},\ \lfloor\exp B'\rfloor].$$

Note that, by regarding (9) as an equation in the field of real numbers (i.e. 'modulo the infinite place'), we find that

$$f_\zeta(x) < 0$$

[3] Note that we have replaced the ordinary Weil height $h(P)$ by the modified Weil height $d(P)$ which is more convenient for our purposes.

for $x < -\zeta^2|k|^{\frac{1}{3}}$.

We will now show how the sieving of the equation

$$y^2 = x^3 + K, \quad K \in \mathbb{Z}, \tag{10}$$

in the interval $I = [x_0,\, x_1] \subseteq \mathbb{Z}$ is carried out. Here, for the sake of readability, we write K instead of $\zeta^6 k$ and keep this number fixed.

It is obvious that if $(x,\, y) \in \mathbb{Z}^2$ satisfies (10), then $(\tilde{x}, \tilde{y})$ is a solution of the congruence

$$Y^2 \equiv X^3 + K \pmod{m}$$

for every positive integer m, where $\tilde{x},\ \tilde{y}$ each denotes the smallest non-negative residue of the integers $x,\ y$ modulo m.

Choose some integers $m_1, \ldots, m_t$ composed of small powers of the first few prime numbers. (In our implementation we used $m_1 = 6624 = 2^5 \cdot 3^2 \cdot 23,\ m_2 = 8075 = 5^2 \cdot 17 \cdot 19,\ m_3 = 7007 = 7^2 \cdot 11 \cdot 13$.) If $x^3 + k$ is a square, then it is a square modulo each m_i. Hence, for each m_i we precompute the residue classes x for which $x^3 + k$ is not a square modulo m_i and remove from the interval under consideration all integers in any of these classes. With the above-mentioned choices of m_i, this eliminates about 99.9 % of all numbers in any long interval, and for the remaining small fraction we simply check directly whether $x^3 + k$ is a square.

Remark: Of course, this sieving procedure can be applied to any equation of the form

$$y^2 = f(x,\, z) \in \mathbb{Q}[x,\, z],$$

where we look only for solutions $x,\, y,\, z \in \mathbb{Z}$. For example, we applied a similar method to find points on the quartics

$$Q:\ y^2 = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4, \quad a,\, b,\, c,\, d,\, e \in \mathbb{Z},$$

which are the 2-coverings of elliptic curves $E/\mathbb{Q}$ in the method of general 2-descent (cf. [Cr]). We used these quartics to find large basis points (of Néron-Tate height larger than 20).

5 Tables

In this section we display some tables that result from our computations based on the above method.

We first applied this method to the Mordell curves

$$E:\ y^2 = x^3 + k, \quad 0 < |k| \le 10\,000.$$

Then, for $10\,000 < |k| \le 100\,000$, we proceeded as follows. Whenever we were able to compute a basis of $E/\mathbb{Q}$, we applied our algorithm for determining all integer points. For some curves, however, we were not able to find a basis. These curves have rank $r = 1$ and a large generator. Here 'large' means that the Néron-Tate height is larger than 70.

If there were any integer point $P = (x,\, y)$ on one of these curves, its Néron-Tate height must be at least as large as the height (≥ 70) of the (missing) generator.

Since, from (3), the upper bound for the difference between the Weil height and the Néron-Tate height on $E/\mathbb{Q}$ is

$$\delta = \frac{1}{3}\log|k| + \frac{10}{3}\log 2 \le \frac{1}{3}\log 100\,000 + \frac{10}{3}\log 2 \le 7 \qquad \text{(for all } |k| \le 100\,000\text{)}$$

such a point must have first coordinate of absolute value

$$|x| > \exp\{70 - 7\} = \exp\{63\} > 10^{28}.$$

But this is very unlikely since the x-coordinate of the largest integer point that we have found within the range $|k| \le 100\,000$ is less than $4 \cdot 10^{10}$.

An alternative approach for finding a generator is the method of Heegner points. Once this method is implemented all integer points will be found.

5.1 Conjectures and conclusions

The large amount of data obtained from our computations gives rise to some speculations.

From Tables 3 and 7 below, we see that the maximal rank of the Mordell curves $E/\mathbb{Q}$ for $|k| < 10\,000$ is 4, and 5 for $|k| < 100\,000$. Furthermore, for $|k| < 10,\ 100,\ 1000$ we find $\mathrm{rk}(E/\mathbb{Q}) \le 1,\ 2,\ 3$, respectively. This suggests that the rank of $E/\mathbb{Q}$ grows according to

$$\mathrm{rk}(E/\mathbb{Q}) = O(\log|k|).$$

Mestre [Me] found that the rank of any elliptic curve $E/\mathbb{Q}$ behaves like

$$\mathrm{rk}(E/\mathbb{Q}) = O\left(\frac{\log \mathcal{N}}{\log\log \mathcal{N}}\right),$$

where $\mathcal{N}$ denotes the conductor of $E/\mathbb{Q}$ (for Mordell's curves, we have $\mathcal{N} = O(k^2)$). For each rank $r > 0$ occurring in our tables we took the smallest positive and the greatest negative integer k such that $E:\ y^2 = x^3 + k$ has rank r:

r	$k > 0$	$k < 0$	$\min \lvert k \rvert$
1	2	-2	2
2	15	-11	11
3	113	-174	113
4	2089	-2351	2089
5	66265	-28279	28279

In order to find the approximate rate of growth for the rank we applied several functions to these values.

r	$\lvert k \rvert$	$\log \lvert k \rvert$	$\log \lvert k \rvert / \log\log \lvert k \rvert$	$\log 4k^2 / \log\log 4k^2$
1	2	0.693	-1.891	2.719
2	11	2.398	2.742	3.394
3	113	4.727	3.043	4.549
4	2089	7.644	3.758	5.926
5	28279	10.250	4.404	7.092

However, none of these functions seems to describe the growth rate. The most suitable function that we found is

r	$\lvert k \rvert$	$\log \lvert k \rvert / \lvert \log\log \lvert k \rvert \rvert^{\frac{2}{3}}$
1	2	1.353
2	11	2.622
3	113	3.525
4	2089	4.762
5	28279	5.836

Also, from these tables, we see that the average number of integer points

$$\Phi(r) = \frac{\#\text{integer points on all } E/\mathbb{Q} \text{ with } \mathrm{rk}(E/\mathbb{Q}) = r}{\#\text{curves } E/\mathbb{Q} \text{ with } \mathrm{rk}(E/\mathbb{Q}) = r}$$

on a Mordell curve E of rank r seems grow exponentially in r.

Another observation that we made concerns the distribution of the ranks of the Mordell curves. Until recently, the common opinion among specialists was that half of all elliptic curves have rank 0 and half rank 1, with higher ranks occurring asymptotically for only 0 % of all curves. However, numerical work of Zagier and Kramarz [ZK] calls this belief into question. They examined the family of elliptic curves

$$x^3 + y^3 = m, \quad m \in \mathbb{Z} \text{ cubefree.}$$

These curves are birationally equivalent to the Mordell curves

$$y^2 = x^3 - 432m^2.$$

For $0 < m \leq 70\,000$, and m cubefree, Zagier and Kramarz computed the value of $L(E, 1)$, and, for $0 < m \leq 20\,000$, m cubefree, also $L'(E, 1)$ when the sign of the functional equation was negative. They point out that

6 347 curves (38.145 %) have rank 0
8 141 curves (48.927 %) have rank 1
1 972 curves (11.852 %) have even rank ≥ 2
179 curves (1.076 %) have odd rank ≥ 3.

For this family of elliptic curves, the number of curves with rank 1 is considerably higher than the number of curves of rank 0, and the proportion of curves with rank greater than 1 is rather large.

Moreover, they detected a constancy of the proportion of curves with ranks larger than 1 over a large range of values of m, suggesting that these curves occur with positive density. Our computations for the Mordell curves $E/\mathbb{Q}$ in the range $|k| \leq 100\,000$ confirm their observation. We even found that the proportion of curves with ranks greater than 1 is still larger, especially for even ranks. The corresponding results are exhibited in tables 1^- and 1^+.

In tables 1^- and 1^+ we list the numbers (#) and percentages (%) of curves of ranks 0, 1, 2, 3, 4, and 5 for values of k ranging over growing intervals and we display them separately for negative and positive values of k.

Table 1^-

$0 > k \geq$		$r=0$	$r=1$	$r=2$	$r=3$	$r=4$	$r=5$
	#	3 625	4 435	1 702	228	10	0
$-10\,000$	%	36.250	44.350	17.020	2.280	0.100	0.000
	#	7 211	8 831	3 437	494	27	0
$-20\,000$	%	36.055	44.155	17.185	2.470	0.135	0.000
	#	10 851	13 222	5 121	757	48	1
$-30\,000$	%	36.170	44.073	17.070	2.523	0.160	0.003
	#	14 450	17 615	6 858	1 002	74	1
$-40\,000$	%	36.125	44.038	17.145	2.505	0.185	0.003
	#	18 050	22 008	8 601	1 243	96	2
$-50\,000$	%	36.100	44.016	17.202	2.486	0.192	0.004
	#	21 694	26 390	10 266	1 521	127	2
$-60\,000$	%	36.157	43.983	17.110	2.535	0.212	0.003
	#	25 324	30 758	11 969	1 799	148	2
$-70\,000$	%	36.177	43.940	17.099	2.570	0.211	0.003
	#	28 966	35 122	13 654	2 082	174	2
$-80\,000$	%	36.208	43.903	17.067	2.603	0.215	0.003
	#	32 653	39 489	15 296	2 363	197	2
$-90\,000$	%	36.281	43.877	16.996	2.626	0.219	0.002
	#	36 278	43 857	17 010	2 635	217	3
$-100\,000$	%	36.278	43.857	17.010	2.635	0.217	0.003

Table 1^+

$0 < k \leq$		$r=0$	$r=1$	$r=2$	$r=3$	$r=4$	$r=5$
	#	2 907	5 111	1 724	250	8	0
10 000	%	29.07	51.11	17.24	2.25	0.08	0.00
	#	5 889	10 147	3 398	531	35	0
20 000	%	29.445	50.735	16.990	2.655	0.175	0.000
	#	8 822	15 224	5 071	828	55	0
30 000	%	29.407	50.747	16.903	2.760	0.183	0.000

Table 1$^+$ (continued)

$0 < k \leq$		$r = 0$	$r = 1$	$r = 2$	$r = 3$	$r = 4$	$r = 5$
	#	11 755	20 290	6 754	1 118	83	0
40 000	%	29.387	50.725	16.885	2.795	0.207	0.000
	#	14 702	25 360	8 428	1 412	98	0
50 000	%	29.404	50.720	16.856	2.824	0.196	0.000
	#	17 641	30 411	10 119	1 706	123	0
60 000	%	29.402	50.685	16.865	2.843	0.205	0.000
	#	20 636	35 495	11 752	1 999	153	1
70 000	%	29.480	50.656	16.789	2.856	0.219	0.001
	#	23 557	40 550	13 439	2 276	177	1
80 000	%	29.446	50.688	16.799	2.845	0.221	0.001
	#	26 573	45 601	15 079	2 580	201	2
90 000	%	29.486	50.668	16.754	2.867	0.223	0.002
	#	29 523	50 659	16 706	2 874	235	3
100 000	%	29.523	50.659	16.706	2.874	0.235	0.003

As pointed out already, this statistics supports the observations made by Zagier and Kramarz.

Some other interesting observations can be made. Whereas for negative values of k the number of rank 0 curves is considerably higher than the number for positive values of k, the converse is true for rank 1 curves. This asymmetry remains true if we consider the distribution of even and odd ranks only for those k which are 6−th power free. We display the data in table 2.

Table 2

$k < 0$	$r = 0$	$r = 1$	$r = 2$	$r = 3$	$r = 4$	$r = 5$	r even	r odd
#	35 642	43 085	16 739	2 611	217	3	52 598	45 699
%	36.259	43.831	17.029	2.656	0.221	0.003	53.509	46.491
$k > 0$								
#	29 003	49 780	16 436	2 840	235	3	45 674	52 623
%	29.505	50.642	16.721	2.889	0.239	0.003	46.465	53.535

We also mention that Brumer [Br] has recently proved that the average rank of an elliptic curve, ordered accordingly to its Faltings height, is at most 2.3. This result is conditional in that it depends on the conjecture of Birch and Swinnerton-Dyer, the conjecture of Shimura, Taniyama and Weil and the Riemann hypothesis for the L-function of an elliptic curve. From Table 7 below the average rank of Mordell's curves with $|k| \leq 100\,000$ turns out to be 0.9.

Furthermore, Stewart and Top [StT] showed that there exist positive numbers C_1 and C_2 such that, if T is a real number larger than C_1, then the number of sixth- power-free integers k with $|k| \leq T$ for which Mordell's curve has rank at least 6 is at least

$$C_2 T^{1/27} / \log^2 T.$$

5.2 Mordell's equation for $|k| \leq 10\,000$

Tables 3 and 7 below reveal that rank 0 curves have at most 5 integral points. This is, of course, a consequence of Proposition 1 from which we know that $\#E_{\mathrm{tors}}(\mathbb{Q}) \leq 6$. It is remarkable that, in Tables 3 and 7, Mordell's curves of rank 1 with k free of 6-th powers have at most 12 integral points and equality is attained only for the curve with $k = 100$. If k is not free of 6-th powers the corresponding curves have up to 14 integer points in the range considered.

Table 3 summarizes the results of our computations with the Mordell curves

$$E: \; y^2 = x^3 + k \quad \text{for } 0 < |k| \leq 10\,000.$$

Table 3: Summary $|k| \leq 10\,000$

number of integer points	number of curves of rank 0	1	2	3	4	total number of curves
0	6459	6884	997	22		14362
1	24	3				27
2	45	2503	1462	108	1	4119
3		4				4
4		99	535	126		760
5	4	3				7
6		24	277	103	6	410
7		2				2
8		12	94	41	1	148
9		2				2
10		8	28	29	1	66
12		1	17	16	2	36
14		1	6	10	1	18
16			5	9		14
18			3	5	1	9
20				4	1	5
22			1	3	2	6
24				1	1	2
26			1			1
28					1	1
32				1		1
$\sum$	6532	9546	3426	478	18	20000

The total and average number of integer points

rank	0	1	2	3	4	all
$\sum$	134	5810	8228	2724	228	17124
$\Phi(r)$	0.021	0.609	2.402	5.699	12.722	0.856

5.2.1 Some curves with large generators

In this table we list the largest generators of rank 1 curves that we have found (for $|k| \leq 10\,000$). The points are represented in the following way:

$$P = (x,\, y) = \left(\frac{\xi}{\zeta^2},\, \frac{\eta}{\zeta^3}\right), \quad \xi,\, \eta,\, \zeta \in \mathbb{Z},\ \zeta > 0, \quad (\xi,\, \zeta) = (\eta,\, \zeta) = 1.$$

We also exhibit the Néron-Tate heights $\hat{h}(P)$ of the points P.

Table 4: Large generators

$k = -9353$	$\hat{h}(P) = 140.9808419298$
$\xi = 136345516255828512524796163737233563410839528658 91\backslash$ 946306347473	
$\eta = 492159014243045856727815228202728833424610915833 62\backslash$ 774789106258579533483727671785124888387815	
$\zeta = 4786471232792916550078534837 52$	
$k = -7365$	$\hat{h}(P) = 121.3392142866$
$\xi = 497677938538294961683649842550472349297427279765 45\backslash$ 161	
$\eta = 111025460745445483686646845995514015774047170415 73\backslash$ 939878410384242505241628396986	
$\zeta = 16415294927845750910775 3$	
$k = -8417$	$\hat{h}(P) = 120.5297630755$
$\xi = 128142859256420950913672776243910937650954896324 37\backslash$ 721	
$\eta = 162608862356173363733694191219195852784435208367 00\backslash$ 850006009902906211790360985 6	
$\zeta = 250460347892401233148858 45$	

	continued
$k = -7969$	$\hat{h}(P) = 111.8099458689$
$\xi = 2291157583928969147760088047142360067139443658017$	
$\eta = 2390047508063301126770382344695936751703026382114 5\backslash$	
$\quad 7566140166564962207643 3$	
$\zeta = 30420072310611037999365 4$	
$k = -4530$	$\hat{h}(P) = 110.3580688067$
$\xi = 847029141256762518733763780964312268229839867531$	
$\eta = 77955637625350263810470790602942158496257479823491\backslash$	
$\quad 828083070825513347123 9$	
$\zeta = 613551056925673863477$	
$k = -3881$	$\hat{h}(P) = 89.6692019429$
$\xi = 8133266424795962255589926343226661997 85$	
$\eta = 23173930488614936556981151794837639882707489217277\backslash$	
$\quad 709463851$	
$\zeta = 2516095125742235478$	

5.2.2 Order of the Tate-Shafarevič group

In Table 5 we list all orders of the Tate-Shafarevič groups that occurred for $|k| \leq 10\,000$ and the corresponding number of curves. In Table 6 we list those k for which the order of Ш is at least 16.

Table 5: Order of Ш

#Ш	total	$k<0$	$k>0$	$r=0$	$r=1$	$r=2$	$r=3$	$r=4$
1	17704	8522	9182	4662	9129	3417	478	18
4	1499	835	664	1210	287	2	–	–
9	703	568	135	566	130	7	–	–
16	74	57	17	74	–	–	–	–
25	12	10	2	12	–	–	–	–
36	8	8	–	8	–	–	–	–
Σ	20000	10000	10000	6532	9546	3426	478	18

Table 6: Curves with large order of Ш

$\#Ш = 16$				k			
-9941	-9649	-9565	-9458	-9410	-9262	-9086	-9054
-8872	-8781	-8566	-8529	-8438	-8170	-8169	-8080
-7773	-7729	-7542	-7458	-7169	-7045	-6981	-6945
-6854	-6757	-6506	-6373	-6170	-6117	-6009	-5869
-5830	-5693	-5505	-5461	-5442	-5218	-4929	-4749
-4560	-4469	-4462	-4329	-4102	-3949	-3893	-3713
-3390	-3013	-2374	-2194	-1753	-1494	-1221	3686
4010	4631	4694	5730	6395	6467	6493	7221
7683	8222	8726	8950	9237	9762	9951	9965
-4910	-8206						
$\#Ш = 25$				k			
-9789	-7745	-7638	-7134	-6702	-6674	-5090	-4777
-4686	-3930	8798	9834				
$\#Ш = 36$				k			
-9978	-9740	-9227	-9194	-9185	-8053	-5414	-2957

In all cases, the structure of the Tate-Shafarevič groups is

$$Ш \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \qquad \text{where } \#Ш = n^2,$$

with the two exceptions

$$Ш \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{ for } k = -4910 \text{ and } -8206.$$

Note that for $r \geq 2$, the orders of the Tate-Shafarevič groups are conjectural.

5.3 Mordell's equation for $|k| \leq 100\,000$

Table 7 summarizes the results of our computations with the Mordell curves

$$E: \; y^2 = x^3 + k \quad \text{for } 0 < |k| \leq 100\,000.$$

Here we assume that those rank 1 curves for which we were unable to find a generator (see the introductory remarks of this section) do not have any integer points. This is the case for about 1800 rank 1 curves.

Table 7: Summary $|k| \le 100\,000$

number of int. points	number of curves with rank 0	1	2	3	4	5	total number of curves
0	65 620	77 357	14 859	723	3		158 562
1	45	9					54
2	130	16 723	13 471	1 783	51		32 157
3		16					16
4		297	3 344	1 393	78		5 112
5	6	7	1				14
6		55	1 519	726	83		2 383
7		2	1				3
8		29	346	386	64	1	826
9		4	1				5
10		13	95	204	46		358
12		2	37	115	32		186
14		2	18	77	20		117
16			10	41	23	1	75
18			5	33	14		52
20			3	12	15	1	31
22			4	10	9		23
24				3	6		9
26			1		3	1	5
28					1		1
30			1	1	2		4
32				1			1
36				1		1	2
38					1		1
42						1	1
48					1		1
$\sum$	65 801	94 516	33 716	5 509	452	6	200 000

The total and average number of integer points							
rank	0	1	2	3	4	5	all
$\sum$	335	35 522	54 319	22 960	4 062	148	117 346
$\Phi(r)$	0.005	0.376	1.611	4.168	8.987	24.667	0.587

5.3.1 Some large integer points

In this table we list all integer points $P = (x, y)$ on

$$E: \; y^2 = x^3 + k \quad \text{for } 0 < |k| \leq 100\,000,$$

with $x \geq 5 \cdot 10^7$.

Table 8: Large integer points

k	rank	x_P	$\pm y_P$
28 024	4	3 790 689 201	233 387 325 399 875
-64 432	4	3 171 881 612	178 638 660 622 364
91 017	3	1 979 757 358	88 088 243 191 777
99 207	2	1 303 201 029	47 045 395 221 186
-88 688	3	1 053 831 624	34 210 296 678 956
-63 604	2	912 903 445	27 582 731 314 539
-44 678	3	890 838 663	26 588 790 747 913
30 788	2	428 895 712	8 882 343 339 054
14 857	3	390 620 082	7 720 258 643 465
14 668	4	384 242 766	7 531 969 451 458
-71 873	2	227 449 469	3 430 262 778 906
79 721	2	189 024 034	2 598 816 054 105
-37 071	3	184 151 166	2 498 973 838 515
11 492	2	154 319 269	1 917 035 856 801
55 441	4	144 185 972	1 731 348 576 567
-22 189	3	140 292 677	1 661 699 554 612
78 454	1	136 918 715	1 602 116 974 677
46 747	1	133 566 713	1 543 644 740 562
-43 084	3	128 694 365	1 459 954 419 179
-98 084	3	121 603 794	1 340 975 019 110
21 689	3	115 716 430	1 244 779 822 617
-58 295	3	114 932 466	1 232 151 436 201
69 760	3	112 749 404	1 197 212 884 968
8 569	2	110 781 386	1 166 004 406 095

continued			
k	rank	x_P	$\pm y_P$
20 961	3	108 997 072	1 137 947 555 953
-93 664	2	107 994 529	1 122 283 639 935
92 962	3	106 999 199	1 106 804 177 919
20 513	2	106 011 056	1 091 507 542 127
25 895	3	103 289 609	1 049 747 744 368
34 721	4	86 493 730	804 409 034 061
64 809	3	79 948 698	714 853 574 601
88 538	2	77 371 607	680 569 411 759
-57 059	3	70 078 487	586 647 298 662
28 676	2	69 830 432	583 535 246 338
89 750	3	61 429 931	481 470 897 421
-54 312	2	53 519 722	391 535 164 856
50 948	2	52 219 621	377 355 403 503

6 Graphs

In this section we give three graphical reproductions of the computations of the Mordell curves for $k = -10\,000$ to $10\,000$.[4] We ran a simple C-program on our files converting the values for k and the x-coordinates of the integer points into LaTeX-commands. For the sake of readability, we left out the very large integer points.

6.1 Mordell curves for $|k| \leq 10\,000$

In the first graph we put the values for k and x of all integer points $P = (x, y)$ on the curves $E: \ y^2 = x^3 + k$ for $-10,000 \leq k \leq 10,000$ into a coordinate system.

For lack of space, we had to limit the size of the x-coordinates of the integer points to $13\,000$; there are 136 points with $x > 13\,000$ which do not appear in the graph.

[4] This was suggested to us by Barry Mazur.

Graph 1

We observed at first sight that, for negative values of k, there are several series of points which appear to be placed on a line whereas this phenomenon does not seem to occur for positive k.

We shall show that there are indeed lines in the negative half plane of the graph. To this end, let us assume that in Mordell's equation x, y and k are polynomials in a variable z over the reals:

$$x,\ y,\ k \in \mathbb{R}[z].$$

If

$$k = k_1 x + k_2' \quad (k_1,\ k_2' \in \mathbb{R})$$

is linear in x, then, as polynomials in z, x has even degree and y has degree divisible by 3. Let us assume that x is quadratic in z. Without loss of generality, we may take

$$x = z^2 + a \quad (a \in \mathbb{R}).$$

Then

$$k = k_1 z^2 + k_2 \quad (k_1,\ k_2 \in \mathbb{R}),$$

and we put

$$y = z^3 + y_1 z^2 + y_2 z + y_3 \quad (y_1,\ y_2,\ y_3 \in \mathbb{R}).$$

Inserting these expressions for x, y and k in Mordell's equation (1) and comparing coefficients of z^ν for $\nu = 5,\ 4,\ 3,\ 2,\ 0$ yields

$$y_1 = 0,\ y_2 = \tfrac{3}{2}a,\ y_3 = 0,\ k_1 = -\tfrac{3}{4}a^2 \quad \text{and} \quad k_2 = -a^3.$$

Hence, we obtain the quantities x, y and k as polynomials over $\mathbb{Q}$ in two variables a and z:

$$x = z^2 + a,\ k = -a^2(\tfrac{3}{4}z^2 + a),\ y = z(z^2 + \tfrac{3}{2}a). \tag{11}$$

On specifying $a \in \mathbb{Z}$ as a fixed integer, we see that x depends linearly on k, namely $x = -\frac{4}{3a^2}(k + \frac{1}{4}a^3)$, and x, k and y attain integer values for all $z \in \mathbb{Z}$ if a is even, and for all $z \in 2\mathbb{Z}$, if a is odd. Moreover, k is negative for all sufficiently large values $|z|$.

However, for negative values of a, the constant k, as a function of z, attains positive values for (finitely many) parameters z of small absolute value $|z|$. In this case, there are lines which start in the positive half plane and go up to the negative half plane. However, they cannot be visualized in our graph.

The relation (11) reflects the general situation if x is a quadratic polynomial. By a more involved calculation, we obtain a similar result if x is a quartic rather than a quadratic polynomial in z.

Graph 2

In the above graph we depicted the lines

$$\alpha : \quad a = 1,\ k = -\tfrac{1}{4}(3x+1); \qquad \beta : \quad a = 2,\ k = -3x-2;$$

$$\gamma : \quad a = 3,\ k = -\tfrac{9}{4}(3x+3); \qquad \delta : \quad a = 4,\ k = -12x-4.$$

6.2 Hall's conjecture

We tried to illustrate M. Hall's conjecture [Ha] graphically. The conjecture states that, for any integer point $P = (x, y)$ on a Mordell curve $E:\ y^2 = x^3 + k$, the estimate

$$|x|^{\frac{1}{2}} < C|k|$$

holds with an absolute constant C. Lang [La] refers to the Hall conjecture in a weaker form, namely

$$|x|^{\frac{1}{2}} < C_\varepsilon |k|^{1+\varepsilon}$$

for any $\varepsilon > 0$, with C_ε depending only on ε.

In its original form, the Hall conjecture is best possible since Danilov [Dan] proved the existence of infinitely many integers x and y such that

$$|x^3 - y^2| < 216\sqrt{2|x|} - 1080.$$

In the following table we listed all Mordell curves for which $|x|^{\frac{1}{2}}/|k| > 1$.

Table 9: Hall's conjecture for $|k| \leq 100\,000$

k	x	$x^{\frac{1}{2}}/\lvert k\rvert$	k	x	$x^{\frac{1}{2}}/\lvert k\rvert$
1 090	28 187 351	4.87	14 668	384 242 766	1.34
17	5 234	4.26	14 857	390 620 082	1.33
225	720 114	3.77	8 569	110 781 386	1.23
24	8 158	3.76	11 492	154 319 269	1.08
−307	939 787	3.16	618	421 351	1.05
−207	367 806	2.93	297	93 844	1.03
28 024	3 790 689 201	2.20			

Hence, for the Mordell curves with $|k| \leq 100\,000$, Hall's conjecture is true for $C = 5$.

For our graphical illustration of Hall's conjecture, we used the Mordell curves with $-10\,000 \leq k \leq 10\,000$. We put the values for k on the vertical axis of the coordinate system (with a linear growth rate) and the values for $|x|$ with a quadratic rate of growth on the horizontal axis.

Graph 3

References

[BSt] B.J. Birch, N.M. Stephens: The parity of the rank of the Mordell-Weil group. Topology **5** (1966) 295-299.

[BSD] B.J. Birch, H.P.F. Swinnerton-Dyer: Notes on elliptic curves I and II. J. Reine Angew. Math., **212** (1963) 7-15, **218** (1965) 79-208.

[Br] A. Brumer: The average rank of elliptic curves I. Invent. Math. **109** (1992) 445-472.

[BMG] A. Brumer, O. McGuiness: The behavior of the Mordell-Weil group of elliptic curves. Bull. Amer. Math. Soc. (N.S.) **23** (1990) 375-382.

[Ca] J.W.S. Cassels: An introduction to the geometry of numbers. Die Grundlehren der mathematischen Wissenschaften Band **99**, Springer-Verlag, Berlin und New York.

[CW] J. Coates, A. Wiles: On the conjectures of Birch and Swinnerton-Dyer. Invent. Math. **39** (1977) 233-251.

[Cr] J.E. Cremona: Algorithms for modular elliptic curves. Cambridge University Press (1992).

[Dav] S. David: Minorations de formes linéaires de logarithmes elliptiques. Me'moires de la Societe' Mathe'matique de France Nume'ro 62, Nouvelle se'rie 1995. Supple'ment au Bulletin de la S.M.F. Tome 123, 1995, fascicule 3.

[Dan] L.V. Danilov: The diophantine equation $y^2 - x^3 = k$ and a conjecture of M. Hall. (Russian), Mat. Zametki **32** (1982) 273-275. Corr. **36** (1984) 457-458. Engl. transl.: Math. Notes **32** 617-618, **36** 726.

[EEPSS] W.J. Ellison, F. Ellison, F. Pesek, C.E. Stahl, D.S. Stall: The diophantine equation $y^2 + k = x^3$. J. Number Theory **2** (1970) 310-321.

[Fu] R. Fueter: Über kubische diophantische Gleichungen. Comm. Math.-Helv., **2** (1930) 69-89.

[G] J. Gebel: Bestimmung aller ganzen und S-ganzen Punkte auf elliptischen Kurven über den rationalen Zahlen mit Anwendung auf die Mordellschen Kurven. PhD Thesis, Universität des Saarlandes, Saarbrücken 1996.

[GPZ1] J. Gebel, A. Pethő, H.G. Zimmer: Computing integral points on elliptic curves. Acta Arith. **68** (1994) 171-192.

[GPZ2] J. Gebel, A. Pethő, H.G. Zimmer: Computing S-integral points on elliptic curves. To appear in Proceedings ANTS-II, Bordeaux 1996, Lecture Notes in Comp. Sci., Springer-Verlag.

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

[GM] B. Gordon, S.P. Mohanty: On a theorem of Delannay and some related results. Pacific J. Math. **68** (1977) 399-409.

[Gra] D.R. Grayson: The arithmetic-geometric mean. Arch. Math. **52** (1989) 507-512.

[Gre] R. Greenberg: On the Birch and Swinnerton-Dyer conjecture. Invent. Math. **72** (1983) 241-265.

[GZa] B. Gross, D. Zagier: Heegner points and derivatives of L-series. Invent. Math. **84** (1986) 225-320.

[Ha] M. Hall: The diophantine equation $x^3 - y^2 = k$. Computers in Number Theory, A.O.L. Atkin and B.J. Birch eds., Academic Press (1971) 173-198.

[Ko1] V.A. Kolyvagin: Finiteness of $E(\mathbb{Q})$ and Ш for a subclass of Weil curves. (Russian) Izv. Acad. Nauk USSR **52** (1988) 522-540.

[Ko2] V.A. Kolyvagin: Euler Systems. The Grothendieck Festschrift, vol. 2. Progr. in Math. **87**, (1990) 474-499, Birkhäuser Boston.

[LJB] M. Lal, M.F. Jones, W.J. Blundon: Numerical solutions of $y^3 - x^2 = k$. Math. Comp. **20** (1966), 322–325.

[La] S. Lang: Conjectured diophantine estimates on elliptic curves. Progr. in Math. **35** (1983) 155-171, Birkhäuser, Basel.

[LLL] A.K. Lenstra, H.W. Lenstra, L. Lovász: Factoring polynomials with rational coefficients. Math. Ann. **261** (1982) 515-534.

[LF] J. London, M. Finkelstein: On Mordell's equation $y^2 - k = x^3$. Bowling Green State University, Bowling Green, Ohio (1973).

[Ma] Y.I. Manin: Cyclotomic fields and modular curves. Russian Math. Surveys **26** (1971) no. 6, 7-78.

[Me] J.F. Mestre, Formules explicites et minorations de conducteurs de variétés algébriques. Compos. Math. **58** (1986), 209-232.

[Mo] L.J. Mordell: Diophantine equations. Academic Press (1969) 238-254.

[Ru1] K. Rubin: Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. Invent. Math. **64** (1981) 455-470.

[Ru2] K. Rubin: The work of Kolyvagin on the arithmetic of elliptic curves. Arith. of Compl. Manifolds, Proc., Lect. Notes in Math. **1399** (1988) 128-136, Springer-Verlag, Berlin und New York.

[Si] J.H. Silverman: The Difference between the Weil height and the canonical height on elliptic curves. Math. Comp. **55** (1990) 723-743.

[Sp] V.G. Sprindžuk: Classical diophantine equations. Lect. Notes in Math. **1559** (1993) p. 113, Springer-Verlag, Berlin und New York.

[Sta] H.M. Stark: Effective estimates of solutions of some diophantine equations, Acta Arith. **24** (1973) 251-259.

[Ste] R.P. Steiner: On Mordell's equation $y^2 - k = x^3$: a problem of Stolarsky. Math. Comp. **46** (1986) 703-714.

[SM] R.P. Steiner, S.P. Mohanty: On Mordell's equation $y^2 - k = x^3$. Indian J. Pure Appl. Math. **22** (1991) 13-21.

[StT] C.L. Stewart, J. Top: On ranks of twists of elliptic curves and power-free values of binary forms. J. Amer. Math. Soc. **8** (1995) 943-973.

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

[dW] B.M.M. de Weger: Algorithms for diophantine equations. Ph. D. Thesis, Centrum voor Wiskunde en Informatica, Amsterdam (1987).

[Ta] J. Tate: Algorithm for determining the type of a singular fiber in an elliptic pencil. Modular Functions in One Variable IV, Lect. Notes in Math. Vol. **476** (1975) 33-52, Springer-Verlag, Berlin und New York.

[Za] D. Zagier: Large integral points on elliptic curves. Math. Comp. **48** (1987) 425-436.

[ZK] D. Zagier, G. Kramarz: Numerical investigations related to the L-series of certain elliptic curves. J. Indian Math. Soc. **52** (1987), 51-60, (Ramanujan Centennary volume).

[Zi1] H.G. Zimmer: On Manin's conditional algorithm. Bull. Soc. Math. France, Mémoire N^o **49-50** (1977) 211-224.

[Zi2] H.G. Zimmer: Generalization of Manin's conditional algorithm. SYMSAC 76. Proc. ACM Sympos. Symbolic Alg. Comp., Yorktown Heights, N.Y. (1976) 285-299.

[Zi3] H.G. Zimmer: A limit formula for the canonical height of an elliptic curve and its application to height computations. Number Theory. Ed. R.A. Mollin, W. de Gruyter Verlag, Berlin and New York (1990) 641-659.