Computing S-integral points on elliptic curves

Jesef Gebel, Attila Pethö and Horst G. Zimmer

1. Introduction

In [GPZ 1] we describe a method, due to Lang and Zagier, for computing all integral points on an elliptic curve E over the field $\mathbb{Q}$ of rational numbers. The method requires the knowledge of the Mordell-Weil group $E(\mathbb{Q})$ and relies on height calculations and on estimating linear forms in complex elliptic logarithms. The corresponding algorithm, implemented in the computer algebra package SIMATH, works quite well for curves E over $\mathbb{Q}$ of rank $r \leq 7$ (see [G]). In [GPZ 2] the algorithm is applied to Mordell's elliptic curves

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

for k within the range

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

Moreover, some interesting numerical experiments relating to Hall's conjecture are carried through. A report about these endeavors is given in [GPZ 3]. In that report we also point out that the algorithm can be extended to yield all S-integral points on E over $\mathbb{Q}$, when S is chosen as a finite set of places of $\mathbb{Q}$ including the infinite place. Some tables of S-integral points are exhibited there for $S = \{2, 3, 5, \infty\}$, but the extended procedure based on p-adic elliptic logarithms in addition to the complex logarithm is not elaborated on.

In the present report, we outline the p-adic method and list some new tables concerning S-integral points on elliptic curves. The results are achieved by means of the implementation of the extended algorithm in the SIMATH package.

Basically, for the p-adic case, we shall follow the line of thought as described in [Sm]. However, our approach differs from the one taken in [Sm] in two respects. First, we use different height estimates and second, in the case of rank at most two curves, we rely on an explicit bound for linear forms in two p-adic elliptic logarithms which was recently established by Rémond and Urfels [R-U]. The crucial idea is to establish an inequality for two functions on the maximum N of the coefficients of S-integral points (see (2) below) of which the lower function exceeds the upper one for sufficiently large N thus leading to an upper bound for N.

2. Height estimates

Let

$$E:\ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \qquad (a_i \in \mathbb{Z})$$

be the given elliptic curve over $\mathbb{Q}$ with Tate's quantities

$$b_2 = a_1^4 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4,\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

$E/\mathbb{Q}$ has discriminant

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

and absolute invariant

$$j = \frac{c_4}{\Delta} =: \frac{j_1}{j_2} \qquad (j_i \in \mathbb{Z},\ gcd(j_1, j_2) = 1).$$

The invariant differential is

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2 + a_4 - a_1y}.$$

By Mordell's theorem, the group $E(\mathbb{Q})$ of rational points on E is finitely generated:

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r,$$

where $E(\mathbb{Q})_{tors}$ is the *torsion group* and r the *rank* of E over $\mathbb{Q}$. Suppose that a basis $P_1, \ldots, P_r \in E(\mathbb{Q})$ of the free part of $E(\mathbb{Q})$ is known. Then every rational point $P \in E(\mathbb{Q})$ has a unique representation

$$P = n_1P_1 + \cdots + n_rP_r + P_{r+1} \qquad (n_i \in \mathbb{Z}) \tag{1}$$

with a torsion point $P_{r+1} \in E(\mathbb{Q})_{tors}$.

We fix an arbitrary finite set S of places of $\mathbb{Q}$ (including the infinite one):

$$S := \{p_1, \ldots, p_{s-1}, \infty\}.$$

Our aim is to find an upper bound N_2 for the coefficients n_i in the representation (1) of S-integral points $P \in E(\mathbb{Q})$:

$$N := \max_{i=1,\ldots,r}\{|n_i|_\infty\} \le N_2. \tag{2}$$

To this end we start by estimating heights. The multiplicative height of a rational point $P = (x, y) \in E(\mathbb{Q})$ is defined as the following product over all primes p of $\mathbb{Q}$ (including $p = \infty$):

$$H(P) := \prod_p \max\{1, |x|_p\}$$

where $|\ |_p$ are the normalized multiplicative absolute values of $\mathbb{Q}$ corresponding to the places p and satisfying the product formula. The ordinary additive height is then

$$h(P) := \frac{1}{2}\ \log\ H(P)$$

and the canonical additive height

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

From Theorem 5 in [Z], one readily derives the inequality

$$h(P) \geq \hat{h}(P) - C_1 \quad \text{for } P \in E(\mathbb{Q})$$

with the constant

$$C_1 := \frac{1}{2}(\log\ 2 + \mu_\infty)$$

in which

$$\mu_\infty := \log\ \max\{|b_2|_\infty, |b_4|_\infty^{\frac{1}{2}}, |b_6|_\infty^{\frac{1}{3}}, |b_8|_\infty^{\frac{1}{4}}\}.$$

As explained in [GPZ 1], this leads to a lower estimate

$$h(P) \geq \lambda_1 N^2 - C_1 \tag{3}$$

involving the smallest eigenvalue λ_1 of the regulator matrix associated with the basis points $P_1, \ldots, P_r \in E(\mathbb{Q})$ via the canonical height $\hat{h}$.

Let now $P = (x, y) \in E(\mathbb{Q})$ be an S-integral point and choose $p \in S$ in such a way that

$$|x|_p = \max\{|x|_{p_1}, \ldots, |x|_{p_{s-1}}, |x|_\infty\}.$$

Then we conclude that

$$H(P) \leq |x|_p^s \qquad \text{for } s := \sharp S$$

and hence that

$$h(P) \leq \frac{s}{2}\ \log\ |x|_p. \tag{4}$$

Combining (3) and (4) yields (cf. [G])

$$\frac{1}{|x|_p^{1/2}} \leq C_2\ \exp\left(-C_3 N^2\right) \tag{5}$$

with

$$C_2 := \exp\left(\frac{C_1}{s}\right),\ C_3 := \frac{\lambda_1}{s}.$$

3. Elliptic logarithms

A lower bound for $|x|_p^{-\frac{1}{2}}$ to supplement the upper bound (5) is now obtained by estimating a linear form in elliptic logarithms. Two cases are to be distinguished, the classical case of $p = \infty$ and the p-adic case. In both cases it is convenient to transform the above long Weierstrass equation for E over $\mathbb{Q}$ into short Weierstrass form:

$$E: \quad Y^2 = X^3 + aX + b \qquad (a, b \in \mathbb{Z}).$$

Note that the canonical height $\hat{h}$ is invariant under the corresponding birational transformation over $\mathbb{Q}$ (cf. Theorem 1 in [Z]).

Case 1: $p = \infty \in S$. In this case S. David [D] computed a lower bound for linear forms in complex elliptic logarithms. The elliptic curve E, now assumed to be given in short Weierstrass form over $\mathbb{Q}$, is parametrized by the Weierstrass function $\wp(u)$ and its derivative $\wp'(u)$. The complex argument $u \in \mathbb{C}$ of a rational point

$$P = (x, y) = (\wp(u), \wp'(u)) \in E(\mathbb{Q})$$

is called the *elliptic logarithm* of P. David's lower bound involves the following quantities:

$$g := E(\mathbb{Q})_{tors}, \text{ the order of the torsion group,} \tag{6}$$

$$C := 2.9 \cdot 10^{6r+6} \cdot 4^{2r^2}(r+1)^{2r^2+9r+12.3}, \tag{7}$$

$$h := \log \max\{4|aj_2|_\infty, 4|bj_2|_\infty, |j_1|_\infty, |j_2|_\infty\},$$

and some numbers $V_i \in \mathbb{R}$ satisfying

$$\log V_i \geq \max\{\hat{h}(P_i), h, \frac{3\pi|u_i|^2}{\omega_1^2}\mathrm{im}(\tau)^{-1}\} \quad (i = 1, \ldots, r)$$

where $u_i \in \mathbb{R}$ are the elliptic logarithms of the generating points P_i of $E(\mathbb{Q})$, ω_1, ω_2 denote the real and complex period of E, respectively, and $\tau = \frac{\omega_2}{\omega_1}$ is the quotient of ω_1, ω_2. The desired lower bound complementing (5) is then

$$\begin{aligned} &\tfrac{\omega_1}{g\sqrt{8}} \exp\{-Ch^{r+1}(\log(\tfrac{r+1}{2}gN) + 1)(\log\,\log(\tfrac{r+1}{2}gN) + 1)^{r+1} \\ &\cdot \prod_{i=1}^{r} \log\, V_i)\} \leq \frac{1}{|x|_\infty^{1/2}}. \end{aligned} \tag{8}$$

Of course, the inequalities (5) and (8) for $|x|_\infty^{1/2}$ have an analogue for the elliptic logarithm $u' = gu \in \mathbb{R}$ of the g-fold multiple $P' = (x', y') = gP = g(x, y)$ of our S-integral point $P \in E(\mathbb{Q})$ (see the proposition on page 179 in [GPZ 1]).

Case 2 $p = p_i \in S$ (for some $i \in \mathbb{N}$ such that $1 \leq i \leq s-1$).
Here we use p-adic elliptic logarithms (cf. [G], [S], [Sm]). Unfortunately, an explicit lower bound similar to (8) in the complex case exists only for $r = 2$.

We explain in some detail how one proceeds in the p-adic case. Let $\mathbb{Q}_p$ be the p-adic completion of $\mathbb{Q}$ and $\mathbb{Z}_p$ its ring of p-adic integers. Denote by

$$E_1(\mathbb{Q}_p) := \{P \in E(\mathbb{Q}_p) \mid \tilde{P} = \tilde{O}\}$$

the kernel of the reduction map modulo p, where E is regarded as a curve over $\mathbb{Q}_p$ and $\tilde{P}$, $\tilde{\mathcal{O}}$ are the reduced points $P, \mathcal{O}$ modulo p. Designate by $\mathcal{E}(p\mathbb{Z}_p)$ the formal group associated to E (cf. [S]). We consider the isomorphism

$$\begin{array}{ccc} \mathcal{E}(p\mathbb{Z}_p) & \longrightarrow & E_1(\mathbb{Q}_p) \\ z & \longmapsto & \left\{ \begin{array}{ll} 0 & \text{if } z = 0 \\ (\frac{z}{w(z)}, -\frac{1}{w(z)}) & \text{if } z \neq 0 \end{array} \right\}, \end{array}$$

where

$$z = -\frac{x}{y},\ w(z) = -\frac{1}{y}.$$

The equation for $w = w(z)$ entailed from the long Weierstrass equation for $E/\mathbb{Q}$ becomes

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 = f(z, w).$$

A recursive procedure based on this equation (see [S]) leads to the power series

$$\begin{array}{rl} w = & z^3 + a_1z^4 + (a_1^2 + a_2)z^5 + (a_1^3 + 2a_1a_2 + a_3)z^6 \\ & +(a_1^4 + 3a_1^2a_2 + 3a_1a_3 + a_2^2 + a_4)z^7 + \cdots \\ & \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[z]]. \end{array}$$

This is the unique power series in z satisfying the relation

$$w(z) = f(z, w(z)).$$

¿From it we also get the Laurent series for x and y, viz.

$$\begin{array}{rcccl} x(z) & = & \frac{z}{w(z)} & = & \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3z - (a_4 + a_1a_3)z^2 - \cdots, \\ y(z) & = & -\frac{1}{w(z)} & = & -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1a_3)z + \cdots. \end{array} \tag{9}$$

The invariant differential has the expansion

$$\begin{array}{rl} \omega(z) = & (1 + a_1z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1a_2 + a_3)z^3 \\ & +(a_1^4 + 3a_1^2a_2 + 6a_1a_3 + a_2^2 + 2a_4)z^4 + \cdots)dz. \end{array}$$

Note that in these expansions the coefficients of the powers of z each have the same weight depending on the exponent of z.

The p-adic elliptic logarithm is now the homomorphism to the additive group $\hat{G}_a$ (over the p-adic analogue $\mathbb{C}_p$ of the complex numbers $\mathbb{C}$) defined as follows:

$$\begin{array}{lcl} \psi_p:\ E_1(\mathbb{Q}_p) & \longrightarrow & \hat{G}_a \\ P = (x, y) & \longmapsto & \int \omega(z) = z + \frac{d_1}{2}z^2 + \frac{d_2}{3}z^3 + \cdots. \end{array}$$

In particular, the p-adic logarithm ψ_p has the properties

$$\psi_p(P + Q) = \psi_p(P) + \psi_p(Q) \tag{10}$$

and

$$|\psi_p(P)|_p = |z|_p = |-\frac{x}{y}|_p.$$

Let $\tilde{E}$ be the reduced curve E modulo p and denote by $\mathcal{N}_p = \sharp\tilde{E}(\mathbb{F}_q)$ the number of rational points on $\tilde{E}/\mathbb{F}_p$. With the order g of the torsion group introduced in (6), we define the number

$$m := lcm(g, \mathcal{N}_p).$$

Then, we have, from the Lutz filtration of E,

$$mP_i =: P_i' \in E_1(\mathbb{Q}_p) \quad (i = 1, \ldots, r)$$

for the generating points p_i of $E(\mathbb{Q})$ and

$$mP_{r+1} = \mathcal{O}$$

for the torsion points $P_{r+1} \in E(\mathbb{Q})_{tors}$.

The representation (1) of an S-integral point $P = (x, y) \in E(\mathbb{Q})$ gives rise to the representation

$$P' = n_1' P_1 + \cdots + n_r' P_r = n_1 P_1' + \cdots n_r P_r' \quad (n_i' := mn_i \in \mathbb{Z}) \tag{11}$$

of its m-multiple $P' = (x', y') = mP \in E_1(\mathbb{Q}_p)$. In analogy to (9), we then have the Laurent series

$$x' = \frac{z'}{w(z')} = \frac{1}{z'^2} - \frac{a_1}{z'} - a_2 - a_3 z' - (a_4 + a_1 a_3) z'^2 - \cdots$$

and this expansion entails the estimate

$$|x'|_p \leq \frac{1}{|z'|_p^2} = \frac{1}{|t'|_p^2}, \tag{12}$$

where we use the abbreviating notation $t' := \psi_p(P')$ for the elliptic logarithm of P'.

On combining the inequalities (5) and (12) and observing that $|x'|_p \geq |x|_p$, we end up with the upper estimate for the p-adic elliptic loarithm $t' = \psi(P')$ of the point $P'(x', y') = mP = m(x, y)$:

$$|t'|_p \leq \frac{1}{|x'|_p^{1/2}} \leq \frac{1}{|x|_p^{1/2}} \leq C_2 \ \exp(-C_3 N^2). \tag{13}$$

This is the p-adic analogue of the right hand inequality exhibited in the proposition on page 179 of [GPZ 1]. In analogy to the left hand inequality in that proposition and to (8), what we need here is an explicit lower estimate for the p-value of the p-adic elliptic logarithm t' of P'. As mentioned above, to date such an estimate is available only for $r \leq 2$.

¿From (10) and (11), we have the relation

$$t' = n_1' t_1 + \cdots + n_r' t_r = n_1 t_1' + \ldots + n_r t_r' \quad (n_i' = mn_i \in \mathbb{Z}) \tag{14}$$

between the elliptic logarithms $t' = \psi_p(P')$ of P', $t_i = \psi_p(P_i)$ of the generating points P_i and $t_i' = \psi_p(P_i')$ of their m-multiples $P_i' = mP_i \in E(\mathbb{Q})$.

As in the complex case, we again suppose E to be given in short Weierstrass form with coefficients $a, b \in \mathbb{Z}$.

An implicitly given lower bound is known for arbitrary ranks r from a theorem of Bertrand [B]. Put

$$B := \log \max\{|n_1|_\infty, \ldots, |n_r|_\infty\}$$

and

$$H := \max\{\hat{h}(P_1), \ldots, \hat{h}(P_r)\}.$$

Then, for CM elliptic curves, Bertrand establishes the inequality

$$\exp\{-c(p \log(m^2 H)^{16r^2} (\log B)^{8r}\} < |t'|_p$$

for $t' = \psi(P')$, where

$$c = c(a, b, r) \in \mathbb{R}_{>0}$$

is a constant depending only on the coefficients a, b of the short Weierstrass form and on the rank r of E over $\mathbb{Q}$. What we require, however, is an explicit form of this constant c comparable to David's constant C in (7) and (8). We trust that D. Bertrand or M. Waldschmidt will encourage a graduate student to work out the explicit form of this constant. A first step in this direction was already taken by Rémond and Urfels [R-U] in the special case of forms in $r = 2$ logarithms. In fact they obtained the following analogue of (8).

On dividing (14) by n_2 and changing the sign, the linear form for $r = 2$ reads

$$\Lambda = nt'_1 - t'_2,$$

where

$$n = \frac{n_1}{n_2} \in \mathbb{Q} \text{ satisfies } |n|_p \leq 1$$

(without loss of generality). We introduce the auxiliary quantities:

$$\begin{array}{rcl} \alpha_i & := & \max\{1, \hat{h}(P_i)\} \quad (i = 1, 2) \\ h(n) & := & \log \max\{|m_1|_\infty, |m_2|_\infty\}, \end{array}$$

where $n = \frac{m_1}{m_2}$ is the simplest fraction representation of n,

$$\begin{array}{rcl} h(E) & := & \log \max\{1, |a|_\infty, |b|_\infty\}, \\ \sigma & := & \rho \max\{|t_1|_p, |t_2|_p\}^{-1}, \end{array}$$

where

$$\rho := p^{-\lambda_p} \quad \text{for } \lambda_p := \left\{ \begin{array}{cc} \frac{1}{p-1} & \text{if } p > 2 \\ 3 & \text{if } p = 2 \end{array} \right\},$$

$$\beta := \max\{h(n), h(E), \hat{h}(P_1), \hat{h}(P_2), \delta\},$$

where

$$\delta := \max\{1, (\log \sigma)^{-1}\},$$

and

$$\gamma := \max\{1, h(E), \log \beta\}.$$

Rémond and Urfels [R-U] now proved that $\Lambda \neq 0$ implies the inequality

$$\exp\{-5.7 \cdot 10^{26} \cdot \alpha_1 \cdot \alpha_2 \cdot \beta \cdot \gamma^3 \cdot \delta^6 \cdot \log\ \sigma\} \leq |\Lambda|_p.$$

For any sufficiently large N, this inequality can be turned into

$$\frac{1}{N}\ \exp\{-C' \cdot \log\ N \cdot (\log\ \log\ N)^3\} \leq |t'|_p, \tag{15}$$

with an explicitly computable constant C' depending on $\hat{h}(P_i)$, $h(E)$, ρ and $|t_i|_p$. The estimate (15) is the analogue of the lower estimate for the complex elliptic logarithm given in the proposition on page 179 of [GPZ 1].

4. De Weger reduction

Comparing the lower bound (8) for the square root of the absolute value of the x-coordinate of our given S-integral point $P = (x, y) \in E(\mathbb{Q})$ with the upper bound in (5) leads in case 1 ($p = \infty$) to the inequality

$$\begin{aligned} \tfrac{\lambda_1}{s} N^2 < Ch^{r+1}(\log(\tfrac{r+1}{2} gN) + 1)(\log\ \log(\tfrac{r+1}{2} gN) + 1)^{r+1} \\ \cdot \prod_{i=1}^{r} \log\ V_i + \log\ \sqrt{8} g C_2 - \log\ \omega_1. \end{aligned} \tag{16}$$

Similarly, comparing the lower bound (15) for the p-value of the p-adic elliptic logarithm $t' = \psi_p(P')$ of the point $P' = mP \in E(\mathbb{Q})$ (where $P = (x, y) \in E(\mathbb{Q})$ is the given S-integral point) with the upper bound in (13) leads in case 2 (the p-adic case) to the inequality

$$\frac{\lambda_1}{s} N^2 < \log\ N(1 + C'(\log\ \log\ N)^3) + \log\ C_2 \tag{17}$$

with the above explicitly computable constant C'.

In both cases, for sufficiently large N, the left hand side of (16) and (17) each exceeds the right hand side. Hence we obtain the desired upper bound

$$N \leq N_2$$

for the maximum, defined by (2), of the absolute values of the coefficients in the basis representation (1) of our S-integral points $P \in E(\mathbb{Q})$.

In case 1, we may choose (cf. [G], [GPZ 1])

$$N_2 := \max\{N_1, \frac{2V}{r+1}, \frac{1}{\lambda_1} \log(g \frac{2^{7/3}}{\omega_1})\},$$

where

$$V := \max_{i=1,\ldots,r} \{V_i\}$$

and

$$N_1 := 2^{r+2} \sqrt{d_1 d_2}\ \log^{\frac{r+2}{2}}(d_2(r+2)^{r+2})$$

for

$$\begin{aligned} d_1 &:= \max\{1, \tfrac{1}{\lambda_1} \log(g\tfrac{2^{7/3}}{\omega_1})\}, \\ d_2 &:= \max\{10^9, \frac{1}{\lambda_1} C\}(\frac{h}{2})^{r+1} \prod_{i=1}^{r} \log\, V_i \end{aligned}$$

with $g = \sharp\, E(\mathbb{Q})_{tors}$ as before in (6) and C as in (7).

In case 2, analogous bounds can be derived from (17) if E has rank $r \leq 2$ over $\mathbb{Q}$. Otherwise, we carry through our computations with an assumed bound

$$N_2 \approx 10^{40}$$

and hope to find all S-integral points on E over $\mathbb{Q}$ in this way.

However, the bound N_2 is by far too large to facilitate the determination of all S-integral points. For instance, we may come up with (see [GPZ 1])

$$N_2 \approx 10^{126}.$$

It is here where de Weger reduction (see [dW]) based on the LLL-algorithm comes into play. This recursive procedure reduces the bound to

$$N_2 \approx 10.$$

Then the search for all S-integral points on $E/\mathbb{Q}$ becomes feasible by means of an efficient sieving method (see [G]).

The application of de Weger reduction is described in detail in [G], [GPZ 1], [Sm] in case 1 ($p = \infty$) and in [G], [Sm] in case 2 ($p \neq \infty$). We refrain therefore from presenting the reduction method here.

The extended algorithm for determining all S-integral points on elliptic curves E over $\mathbb{Q}$ has been implemented by the first author [G] in the computer algebra package SIMATH. In the tables below we list some new examples.

In fact we computed the number of S-integral points for a varying set S of places of $\mathbb{Q}$ on Mordell's curves for

$$10,000 < |k| < 100,000\,,$$

but we selected only those curves which have either rank $r = 5$ or rank $r = 4$ and a large number of S-integral points.

Mordell-Weil group

k	r	t	basis
-92712	5	1	$(46, 68),\ (58, 320),\ (106, 1048),\ (\frac{478}{9}, \frac{6452}{27}),\ (\frac{313}{4}, \frac{4973}{8})$
-43847	5	1	$(38, 105),\ (56, 363),\ (62, 441),\ (36, 53),\ (\frac{177}{4}, \frac{1655}{8})$
-28279	5	1	$(34, 105),\ (40, 189),\ (70, 561),\ (32, 67),\ (50, 311)$
32977	4	1	$(14, 189),\ (-28, 105),\ (98, 987),\ (-6, 181)$
54225	4	1	$(-30, 165),\ (30, 285),\ (15, 240),\ (90, 885)$
66265	5	1	$(-6, 257),\ (-24, 229),\ (24, 283),\ (54, 473),\ (-9, 256)$
81077	5	1	$(47, 430),\ (83, 808),\ (\frac{17}{4}, \frac{2279}{8}),\ (\frac{41}{4}, \frac{2293}{8}),\ (\frac{-89}{9}, \frac{7642}{27})$
92025	4	1	$(-30, 255),\ (30, 345),\ (60, 555),\ (-45, 30)$
94636	5	1	$(-10, 306),\ (-18, 298),\ (110, 1194),\ (45, 431),\ (125, 1431)$

r = rank of E/Q

t = order of the torsion group

Number of integral and S-integral points

k	S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
-92712	16	28	56	74	82	96	112	128	134
-43847	36	50	72	106	126	144	176	202	220
-28279	42	58	80	118	146	176	192	226	246
32977	30	46	66	96	106	126	148	170	184
54225	48	68	84	98	120	146	166	188	204
66265	20	28	64	98	104	138	150	166	180
81077	8	28	56	70	80	94	102	104	128
92025	38	58	76	90	112	132	148	174	188
94636	26	52	72	108	126	156	172	200	216

where $S_0 = \{\infty\}$

$S_1 = \{2, \infty\}$

$S_2 = \{2, 3, \infty\}$

$S_3 = \{2, 3, 5, \infty\}$

$S_4 = \{2, 3, 5, 7, \infty\}$

$S_5 = \{2, 3, 5, 7, 11, \infty\}$

$S_6 = \{2, 3, 5, 7, 11, 13, \infty\}$

$S_7 = \{2, 3, 5, 7, 11, 13, 17, \infty\}$

$S_8 = \{2, 3, 5, 7, 11, 13, 17, 19, \infty\}$

References

[B] D. Bertrand, Approximations diophantiennes p-adiques sur les courbes elliptiques admettant und multiplication complexe. Comp. Math. **37** (1978), 21-50.

[D] S. David, Minorations de formes linéaires de logarithmes elliptiques. To appear in Mém. Soc. Math. France.

[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, Saarbrücken 1996.

[GPZ 1] J. Gebel, A. Pethö and H.G. Zimmer, Computing integral points on elliptic curves. Acta Arith. **68** (1994), 171-192.

[GPZ 2] J. Gebel, A. Pethö and H.G. Zimmer, On Mordell's equation. To appear.

[GPZ 3] J. Gebel, A. Pethö and H.G. Zimmer, Computing integral points on Mordell's elliptic curves. To appear in Proc. Journées Arithmétiques, Barcelona 1995.

[R-U] G. Rémond and F. Urfels, Approximation diophantienne de logarithmes elliptiques p-adiques. To appear in J. Numb. Th.

[S] J.H. Silverman, The Arithmetic of Elliptic Curves. Grad. Texts in Math. **106**, Springer-Verlag, Heidelberg 1986.

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

[S-T] R.J. Stroeker and 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. PhD Thesis. Amsterdam 1987.

[Z] H.G. Zimmer, A Limit Formula for the Canonical Height of an Elliptic Curve and its Application to Height Computations. "Number Theory". Proc. First Conf. CNTA, ed. by R. Mollin. W. de Gruyter, Berlin 1990, 641-659.