Basic algorithms for elliptic curves

Horst G. Zimmer[1]

Fachbereich 9 Mathematik
Universität des Saarlandes
Postfach 15 11 50
D-66041 Saarbrücken

1. Normal forms.

We present here some basic algorithms for elliptic curves developed for and implemented in our computer algebra package SIMATH (see [58]). The elliptic curves E are defined over a field K which will be specified either as an algebraic number field or as a finite field. In general, we shall therefore refer to E in long Weierstrass form:

$$(1.1) \qquad E: \quad Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \quad (a_i \in K).$$

To define the discriminant Δ and the modular invariant j of E, we require Tate's quantities

$$\begin{aligned} b_2 &= a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

and

$$c_4 = b_2^2 - 24b_4,\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

The discriminant is then

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

and the modular invariant

$$j = \frac{c_4^3}{\Delta}.$$

However, if E is defined over a number field K, we shall use the short Weierstrass form

$$(1.2) \qquad E: \quad Y^2 = X^3 + aX + b \quad (a, b \in K)$$

with discriminant

$$\Delta = -16(4a^3 + 27b^2) = -16\Delta_0$$

and modular invariant

$$j = 12^3\frac{4a^3}{\Delta_0}.$$

In the number field case, the D-twist E_D of E over K

$$E_D:\ Y^2 = X^3 + D^2aX + D^3b$$

for a square-free integer D in K also plays an important role. The discriminant of E_D is

$$\Delta_D = D^6\Delta$$

and the modular invariant

$$j_D = j.$$

Elliptic curves E defined over a number field K and having a 2-division point over K are usually given by the equation

$$(1.3) \qquad E: \quad Y^2 = X(X^2 + cX + d) \quad (c, d \in K)$$

[1] Research in part supported by the DFG and by the Siemens AG

so that the 2-division point is $P_0 = (0, 0)$. The discriminant becomes

$$\Delta = 16d^2(c^2 - 4d) = 16\Delta_0$$

and the modular invariant

$$j = 16^2 \frac{(c^2 - 3d)^3}{\Delta_0}.$$

These curves have D-twists

$$E_D : \quad Y^2 = X(X^2 + DcX + D^2 d)$$

for square-free integers D in K, and the discriminant and modular invariant are

$$\Delta_D = D^6 \Delta$$

and

$$j_D = j,$$

respectively.

2. Basic theorems and conjectures.

The algorithms we are going to report about are based on the theorems stated below and are relating to the subsequently quoted conjectures.

Let K be an algebraic number field of degree $n = [K : \mathbb{Q}]$ with ring of integers $\mathcal{O}_K$. We denote by $\mathcal{O}_S$ the subring of S-integers in K with respect to a finite set of places of K containing the infinite places.

Theorem 2.1 (Mordell-Weil, (cf., e.g. [55])). *The group of rational points $E(K)$ of an elliptic curve E over a number field K is finitely generated, i.e.*

$$E(K) \cong E_{tors}(K) \times \mathbb{Z}^r.$$

Here, $E_{tors}(K)$ designates the (finite) *torsion group* and $r \in \mathbb{Z}_{\geq 0}$ the *rank* of E over K.

Theorem 2.2 (Merel [36]). *The order of the torsion group of an elliptic curve E over a number field K of degree $n = [K : \mathbb{Q}]$ is bounded by a constant depending only on n:*

$$\sharp E_{tors}(K) \leq C(n).$$

This result corroborates the long-standing strong boundedness conjecture.

Theorem 2.3 (Siegel-Mahler, cf., e.g. [55]). *The number of S-integral points of an elliptic curve E over a number field K is finite:*

$$\sharp E(\mathcal{O}_S) < \infty.$$

Let $K = \mathbb{F}_q$ be a finite field with $q = p^m$ elements, where $p \in \mathbb{P}$ is a prime number.

Theorem 2.4 (Hasse [22], see also [68]). *The order $N_q = \sharp E(\mathbb{F}_q)$ of the group of rational points $E(\mathbb{F}_q)$ of an elliptic curve E over a finite field $\mathbb{F}_q$ satisfies the inequality*

$$|N_q - (q + 1)| \leq 2\sqrt{q}.$$

This is the analogue of the Riemann hypothesis in the function field case.

The following conjectures are closely related to the above Theorems 2.1 - 2.3.

Rank conjecture 2.1. *The rank of elliptic curves E over the rational number field $K = \mathbb{Q}$ is unbounded:*

$$\sup_{E/\mathbb{Q}} \mathrm{rk}_{\mathbb{Q}} E = \infty.$$

The rank conjecture 2.2 below is in contradiction with a conjecture of Honda (cf. [48], [53]):

Rank conjecture 2.2. *The rank of the D-twists of a fixed elliptic curve E over $K = \mathbb{Q}$ is unbounded:*

$$\sup_{D \in \mathbb{Z} \setminus \mathbb{Z}^2} \mathrm{rk}_{\mathbb{Q}} E_D = \infty.$$

An elliptic curve E over a number field K given in short Weierstrass form (1.2) is called *quasi-minimal* if it has coefficients $a, b \in \mathcal{O}_K$ subject to the condition that its discriminant Δ has norm of minimal absolute value in the isomorphism class of E over K:

$$|N_{K/\mathbb{Q}}(\Delta)| \text{ minimal.}$$

Conjecture 2.3 (Lang-Demjanenko [30], cf. also [56]). *The number of S-integral points on an elliptic curve E over a number field K given in quasi-minimal Weierstrass form, is bounded by a constant depending only on the rank $r = rk_{\mathbb{Q}}E$, the cardinality $s = \sharp S$ and the field K. More precisely,*

$$\sharp E(\mathcal{O}_S) \leq C^{r+s},$$

where the constant C depends only on K.

This conjecture was proved by Silverman [56] for elliptic curves with integral j-invariant. Silverman proved a (weaker) version of this conjecture for arbitrary elliptic curves E over K with a constant depending on K and the number of primes of K appearing in the denominator of j.

Conjecture 2.4 (Lang [31]). *The X-coordinate of an integer point $P = (x, y)$ on the elliptic curve E in short Weierstrass form (1.2) with coefficients $a, b \in \mathbb{Z}$ satisfies the estimate*

$$|x| \ll \max\{|a|^3, |b|^2\}^h$$

for some fixed real positive number h independent of the coefficients a, b.

On specializing the short Weierstrass form (1.2) for E over $\mathbb{Q}$ to $a = 0$ and $b = k \in \mathbb{Z}$, $k \neq 0$, one obtains *Mordell's equation*

$$E_k: \quad Y^2 = X^3 + k \quad (k \in \mathbb{Z}).$$

For this equation we have

Conjecture 2.5 (M. Hall [21]). *The integral points $P = (x, y) \in E(\mathbb{Z})$ of E_k for $k \in \mathbb{Z}$ satisfy the inequality*

$$\sqrt{|x|} < C\ |k|$$

with a constant C.

Following Stark and Trotter, S. Lang [31] refers to the following weaker version of Hall's conjecture.

Conjecture 2.5′ ([30], [31]). *The integral points $P = (x, y) \in E(\mathbb{Z})$ of E_k for $k \in \mathbb{Z}$ satisfy the inequality*

$$\sqrt{|x|} < C_\epsilon |k|^{1+\epsilon}$$

for any $\epsilon > 0$, where C_ϵ is a constant depending only on ϵ.

It is interesting to notice that the abc-conjecture implies this weak version of Hall's conjecture, but not the original strong version (see [41]).

3. Fundamental tasks.

Let K be an algebraic number field and E be an elliptic curve defined over K. Our interest focuses on the group of rational points or *Mordell-Weil group* $E(K)$ of E over K. We are going to deal with the following fundamental tasks which are closely related to the above theorems and have some impact on the conjectures quoted above.

Determine

(3.1) the torsion group $E_{tors}(K)$,

(3.2) the rank r and a basis of the free part of $E(K)$,

(3.3) all integral and S-integral points in $E(K)$.

Construct

(3.4) elliptic curves E over $\mathbb{Q}$ of high rank over suitably chosen multiquadratic extensions K of $\mathbb{Q}$,

(3.5) elliptic curves E of high rank over suitably chosen quadratic fields K.

Of course, such constructions have been carried through for curves E over the rational number field $K = \mathbb{Q}$. But we wish to perform similar constructions over proper extensions K of $\mathbb{Q}$.

Compute or estimate

(3.6) the 2-class rank of certain cubic number fields K in terms of the 2-Selmer group of the associated elliptic curves E.

Let now $K = \mathbb{F}_q$ be a finite field of $q = p^m$ elements, where $p \in \mathbb{P}$ is a prime number, and suppose that the elliptic curve E is defined over $\mathbb{F}_q$.

Construct

(3.7) elliptic curves E over suitably chosen fields $K = \mathbb{F}_q$ such that the group of rational points $E(\mathbb{F}_q)$ has large order:

$$N_q = \sharp E(\mathbb{F}_q) \gg 0.$$

For instance, one may want N_q to contain a large prime factor. This has cryptographic applications. The construction is based on Hasse's theorem and on class field theory.

4. Algorithms.

Let K be an algebraic number field.

4.1 Torsion groups.

For $K = \mathbb{Q}$, all possible torsion groups $E_{tors}(\mathbb{Q})$ are known from a theorem of Mazur [35]. For quadratic fields K, results of Kamienny ([23], [24], [25]) in combination with a conjecture and arguments of Kenku and Momose [26] yield all possible torsion groups, too. We restrict the task of determining all torsion groups $E_{tors}(K)$ of elliptic curves E over number fields K to

(a) fields K of degree $n = [K : \mathbb{Q}] \leq 4$ and

(b) curves E over K with *integral* modular invariant $j \in \mathcal{O}_K$.

With these constraints, all possible torison groups $E_{tors}(K)$ can be determined and in addition (with a few exceptions) all curves E and fields K such that $E_{tors}(K)$ has one of the given structures can be calculated (cf.[12], [37], [38], [42], [60], [67]. They are each finite in number. Of course, the curves are determined only up to isomorphism over K. In the case of fields K of degree $n = 4$ over $\mathbb{Q}$, one has to impose another condition, namely that K is a totally real or totally complex biquadratic field. The general degree-4-case has not been completely solved. Actually, one obtains the following more general result over a multiquadratic number field.

Theorem 4.1 (cf. [1]). *Let E be an elliptic curve defined over a multiquadratic field K, and suppose that E has $\mathfrak{p}$-integral j-invariant at all places $\mathfrak{p}$ of K lying over 2, 3 or 5. Then the torsion group $E_{tors}(K)$ has at most one of the following isomorphism types:*

$$\left\{ \begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & for\, m \in \{1,2,3,4,5,6,7,8,9,10,12,14,16,18,24,36\} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mu\mathbb{Z} & for\, \mu \in \{1,2,3,4,6,9\} \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\nu\mathbb{Z} & for\, \nu \in \{1,2,4\} \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\lambda\mathbb{Z} & for\, \lambda \in \{2,3\} \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} & \end{array} \right\}$$

However, if K is a totally complex or a totally real biquadratic field or a cyclic complex quartic field, the corresponding list of isomorphism types for $E_{tors}(K)$ is considerably smaller (see [1], [28], [60], [67]). In [67] we pointed out that, in the case of a totally real biquadratic field K, it remained an open question if there are elliptic curves E with integral j-invariant over K such that $E_{tors}(K)$ is of type $\mathbb{Z}/5\mathbb{Z}$. In the meantime however, it has been shown by A. Pethö (unpublished) that in fact there are infinitely many elliptic curves E with integral j-invariant over general quartic fields K such that the torsion group of E over K contains $\mathbb{Z}/5\mathbb{Z}$. Moreover, some examples of such curves over totally real biquadratic fields K have been constructed. The infinity result is in contrast to the class of elliptic curves with integral j over complex or totally real biquadratic fields K or number fields K of degree $n \leq 3$ (cf. [1], [42], [67]). In [60], some examples of curves E with integral j over totally real or general quartic fields K having torsion group of type $\mathbb{Z}/7\mathbb{Z}$ or $\mathbb{Z}/14\mathbb{Z}$ have been given, too. In the meantime, it could be shown that, in the case of totally real biquadratic fields, they are finite in number.

We mention that Merel's bound [36] for the order of the torsion group (see Theorem 2.2) is too large for the performance of feasible computations.

We give here some examples.

Table 1

$E_{tor}(K) \cong \mathbb{Z}/5\mathbb{Z}$

K	$\mathbb{Q}(\rho)$ with $\rho^4 = 148\rho^2 - 1$
IB	$\omega_1 = 1$
	$\omega + 2 = \rho$
	$\omega_3 = \frac{1}{5}\rho^2 + \frac{1}{5}$
	$\omega_4 = \frac{1}{5}\rho^3 + \frac{1}{5}\rho$
D_K	$12278016 = 2^8 \cdot 3^2 \cdot 73^2$
j	$-624456 - 7704288\omega_2 + 260280\omega_4$
	$-624456 + 52056\sqrt{146}$
$E : a$	$-323676 + 118260\sqrt{6} + 23976\sqrt{146} - 2180\sqrt{219}$
b	$132167700 - 52862220\sqrt{6} - 10716300\sqrt{146} + 8931060\sqrt{219}$
P	$(225 - 45\sqrt{6} - 9\sqrt{146} + 15\sqrt{219},\ -270\sqrt{6} - 54\sqrt{146})$
	is a point of order 5
j	$-290816 - 3563520\omega_2 + 118784\omega_4$
	$= -290816 - 118784\sqrt{6}$
$E : a$	$7344 - 3024\sqrt{6}$
b	$-1142640 + 466560\sqrt{6}$
P	$(60 - 24\sqrt{6},\ -540 + 216\sqrt{6})$
	is a point of order 5

Table 2

$E_{tor}(K) \geq \mathbb{Z}/7\mathbb{Z}$

K	$\mathbb{Q}(\rho)$ with $\rho^4 = 17\rho^3 - 8\rho^2 - 8\rho + 1$
IB	$\omega_1 = 1$
	$\omega_2 = \rho$
	$\omega_3 = \rho^2$
	$\omega_4 = \frac{1}{13}\rho^3 + \frac{7}{13}\rho^2 + \frac{7}{13}\rho + \frac{7}{13}$
D_K	$13725 = 3^2 \cdot 5^2 \cdot 61$
j	$-3528166975 - 6917966185\omega_2 - 10175422595\omega_3 + 5761666885\omega_4$
$E : a$	$-14093892\rho^3 + 7257735\rho^2 + 6891345\rho + 854928$
b	$1340374595580\rho^3 - 690225177852\rho^2 - 655400190942\rho - 81308491902$
P	$(33\rho^3 - 15\rho^2 - 18\rho,\ -108\rho^3 + 108\rho^2)$
	is a point of order 7

Table 3.1

$E_{tor}(K) \cong \mathbb{Z}/14\mathbb{Z}$

K	$\mathbb{Q}(\rho)$ with $\rho = \frac{3}{2} + \frac{3}{2}\sqrt{2} - \frac{1}{2}\sqrt{5} - \frac{1}{2}\sqrt{10}$
IB	$\omega_1 = 1$
	$\omega_2 = \rho$
	$\omega_3 = \rho^2$
	$\omega_4 = \frac{1}{13}\rho^3 + \frac{12}{13}\rho^2 + \frac{5}{13}\rho + \frac{5}{13}$
D_K	$1600 = 2^6 \cdot 5^2$
j	$3335168 + 6948864\omega_2 + 9350848\omega_3 - 7118592\omega_4$
	$= 1604192 + 1134016\sqrt{2} + 717600\sqrt{5} + 506688\sqrt{10}$
$E : a$	$-8 - \frac{11}{2}\sqrt{2} + 4\sqrt{5} + \frac{5}{2}\sqrt{10}$
b	$-\frac{105}{2} - 38\sqrt{2} + \frac{47}{2}\sqrt{5} + 17\sqrt{10}$
P	$(20 + \frac{29}{2}\sqrt{2} - 9\sqrt{5} - \frac{13}{2}\sqrt{10},\ 85 + \frac{123}{2}\sqrt{2} - 38\sqrt{5} - \frac{55}{2}\sqrt{10})$
	is a point of order 14

Table 3.2

$E_{tor}(K) \cong \mathbb{Z}/14\mathbb{Z}$

K	$\mathbb{Q}(\rho)$ with $\rho = \frac{5}{2} - \frac{3}{2}\sqrt{2} + \frac{1}{2}\sqrt{5} - \frac{1}{2}\sqrt{10}$
IB	$\omega_1 = 1$
	$\omega_2 = \rho$
	$\omega_3 = \rho^2$
	$\omega_4 = \frac{1}{13}\rho^3 + \frac{9}{13}\rho^2 + \frac{10}{13}\rho + \frac{11}{13}$
D_K	$1600 = 2^6 \cdot 5^2$
j	$10645120 - 5524480\omega_2 + 8889920\omega_3 - 6055296\omega_4$
	$= 1604192 + 1134016\sqrt{2} + 717600\sqrt{5} + 506688\sqrt{10}$
$E : a$	$-11 + \frac{17}{2}\sqrt{2} - 5\sqrt{5} + \frac{7}{2}\sqrt{10}$
b	$-\frac{171}{2} + \frac{121}{2}\sqrt{2} - \frac{75}{2}\sqrt{5} + \frac{53}{2}\sqrt{10}$
P	$(-21 + \frac{15}{2}\sqrt{2} - 10\sqrt{5} + 7\sqrt{10},\ -415 + \frac{587}{2}\sqrt{2} - 186\sqrt{5} + \frac{263}{2}\sqrt{10})$
	is a point of order 14

Table 3.3

$E_{tor}(K) \cong \mathbb{Z}/14\mathbb{Z}$

K	$\mathbb{Q}(\rho)$ with $\rho = \frac{7}{2} + 2\sqrt{2} + \frac{3}{2}\sqrt{5} + \sqrt{10}$
IB	$\omega_1 = 1$
	$\omega_2 = \rho$
	$\omega_3 = \rho^2$
	$\omega_4 = \frac{1}{13}\rho^3 + \frac{2}{13}\rho^2 + \frac{8}{13}\rho + \frac{9}{13}$
D_K	$1600 = 2^6 \cdot 5^2$
j	$-19456 - 24960\omega_2 + 9152\omega_3 + 26624\omega_4$
	$= 1604192 + 1134016\sqrt{2} + 717600\sqrt{5} + 506688\sqrt{10}$
$E : a$	$-37 - 27\sqrt{2} - 17\sqrt{5} - 12\sqrt{10}$
b	$-\frac{977}{2} - \frac{691}{2}\sqrt{2} - \frac{437}{2}\sqrt{5} - \frac{309}{2}\sqrt{10}$
P	$(-125 - \frac{177}{2}\sqrt{2} - 56\sqrt{5} - \frac{79}{2}\sqrt{10},\ -2397 - 1695\sqrt{2} - 1072\sqrt{5} - 758\sqrt{10})$
	is a point of order 14

The method of proving Theorem 4.1 and similar theorems in other cases, and for determining the corresponding curves E and fields K consist in

- applying reduction theory,

- using parametrizations,
- solving norm equations.

By reduction theory, the number of possible torsion groups can be considerably restricted. Note that the integrality condition on j leads to a bound for the order of torsion points which is independent of the curve but depends only on the field K. Then, for the torsion groups of small order, parametrizations of the corresponding elliptic curves come into play. The integrality of the j-invariant gives rise to some conditions on the parameter. These conditions are eventually transformed into norm equations. On solving the norm equations, one obtains in general a finite set of parameters by which both the elliptic curves E and the ground fields K such that $E_{tors}(K)$ has one of the given structures are fixed. The solutions of those norm equations are obtained in various different manners, e. g. by referring to intermediate fields, by using Groebner bases techniques and by employing Fibonacci and Lucas sequences (cf. [1], [12], [37], [42]).

4.2 Rank and basis.

Let E be an elliptic curve defined over an algebraic number field K. Then, according to Theorem 2.1, the Mordell-Weil group is finitely generated, and we wish to mention four algorithms for computing the rank r and a basis of the free part $E_{\mathrm{fr}}(K) \cong \mathbb{Z}^r$ of E over K:

(4.2.1) Manin's "conditional" algorithm (see [18], [34])

(4.2.2) Special 2-descent via 2-isogeny (following Tate, see [57])

(4.2.3) General 2-descent (following Birch and Swinnerton-Dyer, [2], [5], [6], [54])

(4.2.4) General 3-descent (following J. Quer, see [43])

4.2.1 Manin's algorithm. Let $\mathcal{M}_K$ be the set of all places $\mathfrak{p}$ of the number field K, and denote by $|\,|_\mathfrak{p}$ the corresponding multiplicative absolute values on K such that the product formula

$$\prod_{\mathfrak{p}\in\mathcal{M}_K} |a|_\mathfrak{p}^{n_\mathfrak{p}} = 1$$

is satisfied with local degrees

$$n_\mathfrak{p} = [K_\mathfrak{p} : \mathbb{Q}_p]$$

of the completion $K_\mathfrak{p}$ of K with respect to $\mathfrak{p}$ over the completion $\mathbb{Q}_p$ of $\mathbb{Q}$ with respect to p, where $\mathfrak{p}$ lies over a prime p of $\mathbb{Q}$ (including $p = \infty$). For a rational point $P = (x, y) \in E(K)$, we define the *ordinary height* of P by (see [66])

$$h(P) = \frac{1}{2}\log \prod_{\mathfrak{p}\in\mathcal{M}_K} \max\{1, |x|_\mathfrak{p}\}^{n_\mathfrak{p}}.$$

The *canonical height* is then the limit

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

There is a constant δ depending only on E and K such that (see [66])

$$|\hat{h}(P) - h(P)| < \delta.$$

The symmetric bilinear form corresponding to the quadratic form $\hat{h}$ on $E(K)$ is

$$\hat{h}(P, Q) = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)$$

for $P, Q \in E(K)$.

The *regulator* of $E(K)$ is defined in terms of a basis $P_1, \ldots, P_r \in E(K)$ of $E_{\mathrm{fr}}(K)$ as the absolute value of the determinant of the matrix $(\hat{h}(P_i, P_j))$:

$$R := |\det(\hat{h}(P_i, P_j))|_{i,j=1,\ldots,r}.$$

Let us consider the r-dimensional real vector space

$$\mathcal{E}(\mathbb{R}) = E(K) \otimes_{\mathbb{Z}} \mathbb{R}.$$

The bilinear form induces a norm

$$\|P\| = \sqrt{\hat{h}(P, P)}$$

on $\mathcal{E}(\mathbb{R})$ turning $\mathcal{E}(\mathbb{R})$ into a real Euclidean vector space. Manin's [34] algorithm consists in applying the *method of successive minima* (see [3]) to this space $\mathcal{E}(\mathbb{R})$.

The natural map

$$E(K) \longrightarrow \mathcal{E}(\mathbb{R})$$

has kernel $E_{tors}(K)$ so that the factor group

$$\hat{E}(K) = E(K)/E_{tors}(K)$$

is injectively embedded in the space $\mathcal{E}(\mathbb{R})$. Note that

$$P \in E_{tors}(K) \Leftrightarrow \hat{h}(P) = 0.$$

We recall that the *ν-th successive minimum* of the lattice $\hat{E}(K)$ in the space $\mathcal{E}(\mathbb{R})$ is the infimum h_ν over all real positive numbers h such that the set

$$\mathcal{N}(h) := \{P \in \mathcal{E}(\mathbb{R});\ \|P\| < h\}$$

contains ν linearly independent lattice points.

Minkowski's theorem now states that (see [3])

(a) $h_1 \ldots h_r \leq \frac{2^r}{c_r} R$,

where c_r stands for the volume of the r-dimensional unit ball,

(b) $\mathcal{N}(h_r)$ contains lattice points which generate a sublattice of $\hat{E}(K)$ of index $\leq r!$

Suppose now that upper bounds r' and R' for the rank r and the regulator R of E over K are known:

$$r \leq r', \quad R \leq R'.$$

Then Minkowski's theorem implies that

$$h_r \leq \frac{2^r}{c_r} \cdot R \frac{1}{h_1 \ldots h_{r-1}} \leq \frac{2^{r'}}{c_{r'}} \cdot R' \cdot \max\{1, h_1^{1-r'}\}.$$

Hence the set of non-torsion points $P \in E(K)$ of height

$$h(P) \leq 2\delta + \frac{2^{2r'}}{c_{r'}^2} {R'}^2 \max\{1, h_1^{2(1-r')}\}$$

generates a subgroup of $\hat{E}(K)$ of index $\leq r'!$ We call this bound for $h(P)$ the *Manin bound.*

In practice one applies an efficient sieving procedure for finding a sufficient number of independent rational points in $E(K)$ below a given bound (see [13]). Actually, assuming the rank r of $E(K)$ to be known, it suffices to find r independent points in $E(K)$. Then, the regulator of these points defines a bound for the height of generators which is sharper than the Manin bound. By minimizing the regulator, one ends up with r basis points.

The rank is computed by assuming the conjectures of Shimura-Taniyama-Weil (known to be true for semi-stable curves by work of Wiles) and of Birch and Swinnerton-Dyer (see [2], [17]). According to the latter conjecture, r is equal to the analytic rank of E over K, that is, to the least non-negative integer ρ such that the ρ-th derivative of the L-series $L(E/K;s)$ of E over K is non-zero at the argument $s = 1$. Of course, it is a problem to numerically decide whether or not $L^{(\rho)}(E/K;s)$ is zero at $s = 1$. However, on assuming that $L^{(\rho)}(E/K;1) \neq 0$, one inserts the value $r' = \rho$ in the Manin bound, where $L^{(r')}(E/K;1)$ occurs in the expression for R' (cf. [18], [34]), and tries to compute a basis of $E(K)$ with height below the new Manin bound. If one does not succeed, one must have $r > \rho$ and hence $L^{(\rho)}(E/K;1) = 0$.

Table 4

An elliptic curve E over $\mathbb{Q}$ of rank $r = 7$

$$E:\ Y^2 + 1641Y = X^3 - 168X^2 + 161X - 8$$

i	Generators P_i	Heights $\hat{h}(P_i)$
1	(103, -806)	3.9328739699
2	(102, -766)	3.9543450903
3	(101, -743)	3.9749799930
4	(120, -784)	3.9922302943
5	(100, -724)	3.9948505200
6	(99, -707)	4.0140191298
7	(122, -730)	4.0407915991

4.2.2 Special 2-descent via 2-isogeny.

Here we start out from the normal form (1.3) of E over K with $c, d \in \mathcal{O}_K$. This curve E has the rational 2-division point $P_0 = (0,0)$ and is isogenous to the elliptic curve

$$E': \quad Y^2 = X(X^2 + c'X + d') \quad (c', d' \in \mathcal{O}_K)$$

over K with coefficients

$$c' = -2c,\ d' = c^2 - 4d.$$

Let us suppose that K has class number one. The isogeny (cf. [6], [46], [47], [52], [53], [57], [61])

$$\Phi:\ E(K) \longrightarrow E'(K)$$

is given by

$$\begin{array}{ccll} \mathcal{O} & \longmapsto & \mathcal{O} & \\ P_0 & \longmapsto & \mathcal{O} & \\ P = (x,y) & \longmapsto & \left(\frac{y^2}{x^2}, \frac{y(x^2-d)}{x^2}\right) & \text{for } P \neq \mathcal{O}, P_0. \end{array}$$

Its dual isogeny

$$\Phi':\ E'(K) \longrightarrow E(K)$$

is analogously defined, and we have

$$\Phi' \circ \Phi = [2]_{E/K}, \quad \Phi \circ \Phi' = [2]_{E'/K}.$$

We also consider the group homomorphism

$$\begin{array}{rrcll} \alpha: & E(K) & \longrightarrow & K^*/K^{*2} & \\ & \mathcal{O} & \longmapsto & 1 \mod K^{*2} & \\ & P_0 & \longmapsto & d \mod K^{*2} & \\ & P=(x,y) & \longmapsto & x \mod K^{*2} & \text{for } P \neq \mathcal{O}, P_0 \end{array}$$

and the analogously defined homomorphism

$$\alpha' : E'(K) \longrightarrow K^*/K^{*2}.$$

Then the rank r of E over K is given by the formula (see [6], [47], [57])

$$(*) \qquad 2^r = \frac{\sharp \alpha E(K) \cdot \sharp \alpha' E'(K)}{2^2}.$$

The images $\alpha E(K)$ and $\alpha' E'(K)$ can be explicitly described as follows (see [6]). Let $K_2(d)$ denote a set of integers d_1 in K^*, belonging to distinct classes in K^*/K^{*2}, such that the additive normalized value $v_{\mathfrak{p}}(d_1)$ is even at all finite places $\mathfrak{p}$ of K which do not divide d. Then we have the finite sets

$$\begin{array}{lcl} \alpha E(K) & \cong & \{d_1 \in K_2(d);\quad y^2 = d_1 x^4 + cx^2 + \frac{d}{d_1} \text{ has a rational point over } K\}. \\ \alpha' E'(K) & \cong & \{d_1' \in K_2(d');\quad y^2 = d_1' x^4 + c' x^2 + \frac{d'}{d_1'} \text{ has a rational point over } K\}. \end{array}$$

These sets can be used to compute the rank r of E over K.

To this end we need also the well-known exact sequences involving the Selmer groups $S^{(\Phi)}(E/K)$, $S^{(\Phi')}(E'/K)$ and the Tate-Shafarevich groups

$$\text{III}(E/K)[\Phi], \quad \text{III}(E'/K)[\Phi'].$$

One starts out from the exact sequence

$$0 \longrightarrow E(\overline{K})[\Phi] \longrightarrow E(\overline{K}) \xrightarrow{\Phi} E'(K) \longrightarrow 0$$

of G-modules with respect to the absolute Galois group $G = \mathrm{Gal}(\overline{K}/K)$ of K ($\overline{K}$ being the algebraic closure of K), where $E(\overline{K})[\Phi]$ denotes the kernel of Φ. This sequence gives rise to the long exact cohomology sequence

$$\begin{array}{c} 0 \longrightarrow E(K)[\Phi] \longrightarrow E(K) \xrightarrow{\Phi} E'(K) \xrightarrow{\partial} H^1(G, E(\overline{K})[\Phi]) \\ \longrightarrow H^1(G, E(\overline{K})) \xrightarrow{\Phi} H^1(G, E'(\overline{K})), \end{array}$$

where ∂ is the connecting map. By factoring out the kernel on the left hand side and passing to the image on the right hand side, we obtain the exact sequence

$$0 \longrightarrow E'(K)/\Phi E(K) \xrightarrow{\partial} H^1(G, E(\overline{K})[\Phi]) \longrightarrow H^1(G, E(\overline{K}))[\Phi] \longrightarrow 0$$

and, analogously,

$$0 \longrightarrow E(K)/\Phi' E'(K) \xrightarrow{\partial} H^1(G, E'(\overline{K}))[\Phi'] \longrightarrow H^1(G, E'(\overline{K}))[\Phi'] \longrightarrow 0.$$

¿From these sequences one readily derives the desired exact sequences for the Selmer groups and the Tate-Shafarevich groups

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/\Phi' E'(K) & \longrightarrow & S^{(\Phi')}(E'/K) & \longrightarrow & \text{III}(E'/K)[\Phi'] & \longrightarrow & 0, \\ 0 & \longrightarrow & E'(K)/\Phi E(K) & \longrightarrow & S^{(\Phi)}(E/K) & \longrightarrow & \text{III}(E/K)[\Phi] & \longrightarrow & 0. \end{array}$$

Here the Selmer groups are given by

$$\begin{array}{lcl} S^{(\Phi')}(E'/K) & \cong & \{d_1 \in K_2(d);\ y^2 = d_1x^4 + cx^2 + \frac{d}{d_1} \text{ has a} \\ & & \quad \text{rational point over all completions } K_{\mathfrak{p}} \text{ of } K\}, \\ S^{(\Phi)}(E/K) & \cong & \{d_1' \in K_2(d');\ y^2 = d_1'x^4 + c'x^2 + \frac{d'}{d_1'} \text{ has a} \\ & & \quad \text{rational point over all completions } K_{\mathfrak{p}} \text{ of } K\}. \end{array}$$

The Tate-Shafarevich groups are (up to suitable identifications)

$$\begin{array}{lcl} \text{III}(E'/K)[\Phi'] & \cong & S^{(\Phi')}(E'/K)/(E(K)/\Phi'E'(K)) \\ \text{III}(E/K)[\Phi] & \cong & S^{(\Phi)}(E/K)/(E'(K)/\Phi E(K)) \end{array}$$

with

$$\begin{array}{lcl} E(K)/\Phi'E'(K) & \cong & \alpha E(K), \\ E'(K)/\Phi E(K) & \cong & \alpha' E'(K). \end{array}$$

We remark that, under the assumption that $\text{III}(E/K)$ and $\text{III}(E'/K)$ are finite, the order of their 2-torsion $\sharp\text{III}(E/K)[2]$ and $\sharp\text{III}(E'/K)[2]$ must be an even power of 2.

For the Tate-Shafarevich groups, we have the exact sequences

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{III}(E/K)[\Phi] & \longrightarrow & \text{III}(E/K)[2] & \xrightarrow{\Phi} & \text{III}(E'/K)[\Phi'], \\ 0 & \longrightarrow & \text{III}(E'/K)[\Phi'] & \longrightarrow & \text{III}(E'/K)[2] & \xrightarrow{\Phi'} & \text{III}(E/K)[\Phi]. \end{array}$$

The first sequence implies the inequalities

$$\sharp\text{III}(E/K)[\Phi] \leq \sharp\text{III}(E/K)[2] \leq \sharp\text{III}(E/K)[\Phi] \cdot \sharp\text{III}(E'/K)[\Phi'].$$

Hence, if

$$\sharp\text{III}(E/K)[\Phi] = 1, \tag{i}$$

we infer from the first sequence

$$1 \leq \sharp\text{III}(E/K)[2] \leq \sharp\text{III}(E'/K)[\Phi'] \tag{ii}$$

and from the second sequence

$$\sharp\text{III}(E'/K)[2] = \sharp\text{III}(E'/K)[\Phi']. \tag{iii}$$

The determination of the rank r is now accomplished by calculating all square-free divisors d_1 of d and d_1' of d' and then solving the quartics, occurring in $\alpha E(K)$ and $\alpha' E'(K)$ at first everywhere locally and then also globally over K (see [6], [46], [47], [52]). P. Serf ([6], [52]) has applied this method to elliptic curves E of ranks $\geq 4, 5, 6, 7$ over quadratic fields K of class number one found by H. Graf [19]. She determined (or estimated) the rank r and produced r independent points in the Mordell-Weil group $E(K)$. We mention that some curves E with large Tate-Shafarevich groups $\text{III}(E/K)[2]$ over real quadratic fields K are also constructed in [6], [52].

We list here some examples. The curves E are given in normal form (1.3) over some quadratic fields $K = \mathbb{Q}(\sqrt{D})$ of class number one.

In the tables 5 and 6 below a lower bound ρ calculated by H. Graf [19] for the rank r of E over $K = \mathbb{Q}(\sqrt{D})$ is exhibited and at least ρ linearly independent points in $E(K)$ are listed. Furthermore, since condition (i) is satisfied for the curves E over the fields $K = \mathbb{Q}(\sqrt{D})$ in those tables, the orders of the 2-Tate-Shafarevich groups could be either estimated from (ii) or calculated from (iii).

Table 5

$E:\ Y^2 = X(X^2+cX+d)$ over $K=\mathbb{Q}(\sqrt{D})$

$D=5,\ d=(38874,15048),\ N_{K/\mathbb{Q}}(d)=2^2\cdot 3^2\cdot 11^2\cdot 19^2\cdot 29\cdot 41$

	lower bound	possible	linearly independent	$\sharp\text{Ш}(\dots/K)[2]$	
c	for r	ranks r	points in $E(K)$	E'	E
(135,765)	4	4	$\sharp1\ x=(114,-12)$ $y=(750,2238)$ $\sharp2\ x=(-228,-570)$ $y=(-4560,-6384)$ $\sharp3\ x=(30,-78)$ $y=(-1278,-690)$ $\sharp4\ x=(200,200)$ $y=(5880,10900)$	1	1

$D=5,\ d=(84018,125400),\ N_{K/\mathbb{Q}}(d)=2^2\cdot 3^2\cdot 11^2\cdot 19^2\cdot 29\cdot 41$

	lower bound	possible	linearly independent	$\sharp\text{Ш}(\dots/K)[2]$	
c	for r	ranks r	points in $E(K)$	E'	E
(663,664)	6	7	$\sharp1\ x=(750,600)$ $y=(-31020,17160)$ $\sharp2\ x=(-432,-552)$ $y=(-4500,-8676)$ $\sharp3\ x=(346,384)$ $y=(13188,20892)$ $\sharp4\ x=(15720,-9870)$ $y=(-2344506,145832)$ $\sharp5\ x=(-408,-672)$ $y=(-2748,-4848)$ $\sharp6\ x=\frac{1}{25}(-9570,-11088)$ $y=\frac{1}{125}(-647328,-1248852)$ $\sharp7\ x=(-376,-302)$ $y=(-4822,-9448)$	1	1

Table 6

$Y^2 = X(X^2+cX+d)$ over $K=\mathbb{Q}(\sqrt{D})$

$D=6,\ d=(-183540,-72105),\ N_{K/\mathbb{Q}}(d)=2\cdot 3^2\cdot 5^2\cdot 19^2\cdot 23^2\cdot 29$

	lower bound	possible	linearly independent	$\sharp\text{Ш}(\dots/K)[2]$	
c	for r	ranks r	points in $E(K)$	E'	E
(700,207)	5	5 7 9	$\sharp1\ x=\frac{1}{4}(711,234)$ $y=\frac{1}{8}(25173,10857)$ $\sharp2\ x=\frac{1}{8}(2755,1140)$ $y=\frac{1}{32}(409260,169575)$ $\sharp3\ x=\frac{1}{9}(-875,130)$ $y=\frac{1}{27}(-88685,-20700)$ $\sharp4\ x=(-69,-46)$ $y=(-5175,-1955)$ $\sharp5\ x=\frac{1}{49}(-1368,-1197)$ $y=\frac{1}{343}(-1103292,-437703)$	16 4 1	$1\vee 4\vee 16$ $1\vee 4$ 1

$$D = 6,\ d = (-1786893, -595631),\ N_{K/\mathbb{Q}}(d) = 3 \cdot 19^2 \cdot 23^2 \cdot 29^2 \cdot 47^2$$

	lower bound	possible	linearly independent	$\sharp$III$(\ldots/K)[2]$	
c	for r	ranks r	points in $E(K)$	E'	E
(2588,773)	5	6	$\sharp 1\ x = (-1972, -1276$	4	$1 \vee 4$
		8	$y = (34394, -4582)$	1	1
			$\sharp 2\ x = (118436, 48375)$		
			$y = (58203986, 23759932)$		
			$\sharp 3\ x = \frac{1}{4}(2497, 480)$		
			$y = \frac{1}{8}(166083, 61686)$		
			$\sharp 4\ x = (-1114, -854)$		
			$y = (-58796, -38601)$		
			$\sharp 5\ x = (817, 171)$		
			$y = (37620, 12692)$		
			$\sharp 6\ x = (25209, 10149)$		
			$y = (-5841786, -2386356)$		

By a standard procedure, based on special 2-descent, one can determine r independent points in $E(K)$ and in certain cases also a basis of $E(K)$. This was done by S. Schmitt [46] for the basic field $K = \mathbb{Q}$ and the parametrized family of elliptic curves of the special form

$$E''_k: \quad Y^2 = (X + k)(X^2 + k^2) \quad (k \in \mathbb{Z} \text{ square-free})$$

The curves E''_k over $\mathbb{Q}$ had been previously considered for prime parameters $k = p \in \mathbb{P}$ by Stroeker and Top [62]. It is easy to see that E''_k is birationally isomorphic to the curve

$$E_k: \quad Y^2 = X(X - 2kX + 2k^2)$$

over $\mathbb{Q}$. All these curves have the 2-division point $P_0 = (0, 0)$ as the only non-trivial torsion point and hence, their torsion group is (see [46], [47])

$$E_{k,tors}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.$$

S. Schmitt ([46], [47]) explicitely computed the Selmer groups $S^{(\Phi)}(E_k/\mathbb{Q})$ and $S^{(\Phi')}(E'_k/\mathbb{Q})$ of E_k and the 2-isogenous curve E'_k of E_k. Moreover, for square-free integers k in the interval

$$|k| < 100,$$

she determined the rank and a basis of the Mordell-Weil group $E_k(\mathbb{Q})$. Applying the procedure of Gebel, Pethö and the author (see [13], [14]), she also found all integer points [2] in $E_k(\mathbb{Q})$ within the above interval (see [46]).

These results can be used to estimate the constant h in conjecture 2.4 of S. Lang. It is suggested that one may take $h = \frac{5}{3} + \epsilon$.

If $3 \not| k$, the birational transformation

$$X = u^2\tilde{X} + \kappa,\ Y = u^3\tilde{Y} \text{ with } u := \frac{1}{3},\ \kappa = \frac{2}{3}k$$

yields the model

$$\tilde{E}_k: \quad \tilde{Y}^2 = \tilde{X}^3 + 54k^2\tilde{X} + 540k^3$$

[2] The referee of [47] has caused the author to remove this interesting part from her paper. That is why we wish to include it here and publish the corresponding tables.

and if $3|k$, the birational transformation

$$X = u^2\tilde{X} + \kappa,\ Y = u^3\tilde{Y} \text{ with } u = 1,\ \kappa = \frac{2}{3}k$$

leads to the model

$$\tilde{E}_k: \quad \tilde{Y}^2 = \tilde{X}^3 + 6(\frac{k}{3})^2\tilde{X} + 20(\frac{k}{3})^3$$

of the original curve E_k.

In this way, in the case of $3 \not| k$, the set of integral points on E_k over $\mathbb{Q}$ is transformed into the set of integral points on $\tilde{E}_k$ over $\mathbb{Q}$, whereas in the case of $3|k$, there can be some additional integral points on $\tilde{E}_k$ not arising from integral points on E_k. By means of the algorithm of Gebel et al. [13], [14] S. Schmitt has determined the set of all integral points on $\tilde{E}_k$ in both cases.

In Lang's conjecture for the curve $\tilde{E}_k$, we choose the factor 1 in front of the maximum and have in the case of $3 \not| k$:

$$\max\{|54k^2|^3, |540k^3|^2\} = 540^2k^6,$$

and on choosing

$$h = 0.38258353338323422422,$$

we obtain

$$|x| < (540^2k^6)^h,$$

whereas in the case of $3|k$:

$$\max\{|6(\frac{k}{3})^2|^3, |20(\frac{k}{3})^3|^2\} = 20^2(\frac{k}{3})^6,$$

and on choosing

$$h = 0.71590910795617837384,$$

we obtain

$$|x| < (20^2(\frac{k}{3})^6)^h.$$

In tables 7 and 8 below, corresponding to the cases $3 \not| k$ and $3|k$, we list all integral points on $\tilde{E}_k$ over $\mathbb{Q}$ in their representations in terms of a torsion point and the basis points.

Table 7: $3 \nmid k$

k	$\mathrm{rk}(\tilde{E}_k(\mathbb{Q}))$	integral points with their representation
-97	0	$(582,0) = (582,0)$
-95	0	$(570,0) = (570,0)$
-94	1	$(564,0) = (564,0) + 0 \ast (56518482817/100160064, 636544162316609/1002401920512)$
-91	1	$(546,0) = (546,0) + 0 \ast (47635, 10397555)$ $(47635, 10397555) = \mathcal{O} + (47635, 10397555)$
-89	0	$(534,0) = (534,0)$
-86	0	$(516,0) = (516,0)$
-85	1	$(510,0) = (510,0) + (53686/9, 12497516/27)$
-83	1	$(498,0) = (498,0) + 0 \ast (355596987/290521, 6968424770775/156590819)$
-82	0	$(492,0) = (492,0)$
-79	0	$(474,0) = (474,0)$
-77	1	$(462,0) = (462,0) + 0 \ast (1897/4, 27685/8)$ $(78870, 22150260) = (462,0) - (1897/4, 27685/8)$
-74	1	$(444,0) = (444,0) + 0 \ast (1700409/49, 2217595185/343)$
-73	0	$(438,0) = (438,0)$
-71	0	$(426,0) = (426,0)$
-70	0	$(420,0) = (420,0)$
-67	1	$(402,0) = (402,0) + 0 \ast (144499800520865496767692540 20/230306067187787573172 6961, 17417745611605213067189617597705266685 61370/3495087628170223048756412645776211209)$
-65	0	$(390,0) = (390,0)$
-62	1	$(372,0) = (372,0) + 0 \ast (16919769/6400, 70383858147/512000)$
-61	1	$(366,0) = (366,0) + 0 \ast (2001715/9, 2832071705/27)$
-59	1	$(354,0) = (354,0) + 0 \ast (15483, 1927287)$ $(15483, 1927287) = \mathcal{O} + 1 \ast (15483, 1927287)$
-58	1	$(348,0) = (348,0) + 0 \ast (55743347049/109098025, 12526929846746343/1139528871125)$
-55	0	$(330,0) = (330,0)$
-53	1	$(318,0) = (318,0) + 0 \ast (7468707/49, 20411247375/343)$
-47	2	$(282,0) = (282,0) + 0 \ast (570, 14040) + 0 \ast (4332, 285930)$ $(570, 14040) = \mathcal{O} + (570, 14040) + 0 \ast (4332, 285930)$ $(4332, 285930) = \mathcal{O} + 0 \ast (570, 14040) + (4332, 285930)$
-46	1	$(276,0) = (276,0) + 0 \ast (732851187553/166978084, 629033451858521263/2157690801448)$
-43	1	$(258,0) = (258,0) + 0 \ast (198656774670466243/740904827667489, 355874762984527560180839 95/20167108597318670557263)$
-41	2	$(246,0) = (246,0) + 0 \ast (1353/4, 45387/8) + 0 \ast (2665/4, 142885/8)$ $(3198, 181548) = (246,0) - (1353/4, 45387/8) + 0 \ast (2665/4, 142885/8)$ $(218046, 101817540) = (246,0) - 2 \ast (1353/4, 45387/8) + (2665/4, 142885/8)$ $(894, 27540) = (246,0) + 0 \ast (1353/4, 45387/8) - (2665/4, 142885/8)$
-38	0	$(228,0) = (228,0)$
-37	1	$(222,0) = (222,0) + 0 \ast (1220997595/1394761, 43837024928795/1647212741)$
-35	1	$(210,0) = (210,0) + 0 \ast (651, 17199)$ $(651, 17199) = \mathcal{O} + (651, 17199)$ $(660, 17550) = (210,0) - (651, 17199)$

k	$\mathrm{rk}(\tilde{E}_k(\mathbb{Q}))$	integral points with their representation
-34	0	$(204,0)=(204,0)$
-31	2	$(186,0)=(186,0)+0*(348,6642)+0*(1963/9,63937/27)$ $(348,6642)=\mathcal{O}+(348,6642)+0*(1963/9,63937/27)$ $(1147,39401)=(186,0)-(348,6642)+0*(1963/9,63937/27)$
-29	1	$(174,0)=(174,0)+0*(8787/49,295191/343)$ $(25752,4132674)=(174,0)-(8787/49,295191/343)$
-26	1	$(156,0)=(156,0)+0*(273,4563)$ $(273,4563)=\mathcal{O}+(273,4563)$ $(1092,36504)=(156,0)-(273,4563)$
-23	0	$(138,0)=(138,0)$
-22	0	$(132,0)=(132,0)$
-19	1	$(114,0)=(114,0)+0*(10627/49,1123291/343)$
-17	0	$(102,0)=(102,0)$
-14	1	$(84,0)=(84,0)+0*(777/4,22491/8)$ $(372,7344)=(84,0)-(777/4,22491/8)$
-13	1	$(78,0)=(78,0)+0*(1027/9,31265/27)$
-11	1	$(66,0)=(66,0)+0*(507,11529)$ $(507,11529)=\mathcal{O}+(507,11529)$
-10	1	$(60,0)=(60,0)+0*(100,1000)$ $(100,1000)=\mathcal{O}+(100,1000)$ $(465,10125)=(60,0)-(100,1000)$
-7	0	$(42,0)=(42,0)$
-5	1	$(30,0)=(30,0)+0*(75,675)$ $(75,675)=\mathcal{O}+(75,675)$ $(120,1350)=(30,0)-(75,675)$ $(1830,78300)=(30,0)+2*(75,675)$
-2	0	$(12,0)=(12,0)$
-1	0	$(6,0)=(6,0)$
1	1	$(-6,0)=(-6,0)+0*(3,27)$ $(3,27)=\mathcal{O}+(3,27)$ $(12,54)=(-6,0)-(3,27)$ $(66,540)=(-6,0)+2*(3,27)$ $(43,287)=\mathcal{O}-3*(3,27)$
2	0	$(-12,0)=(-12,0)$
5	0	$(-30,0)=(-30,0)$
7	1	$(-42,0)=(-42,0)+0*(30,540)$ $(30,540)=\mathcal{O}+(30,540)$
10	1	$(-60,0)=(-60,0)+0*(-15,675)$ $(-15,675)=\mathcal{O}+(-15,675)$ $(300,5400)=(-60,0)-(-15,675)$
11	0	$(-66,0)=(-66,0)$
13	0	$(-78,0)=(-78,0)$
14	1	$(-84,0)=(-84,0)+0*(-287/4,4753/8)$ $(2508,125712)=(-84,0)-(-287/4,4753/8)$
17	1	$(-102,0)=(-102,0)+0*(-53,1295)$ $(-53,1295)=\mathcal{O}+(-53,1295)$
19	0	$(-114,0)=(-114,0)$

k	$\mathrm{rk}(\tilde{E}_k(\mathbb{Q}))$	integral points with their representation
22	0	$(-132,0) = (-132,0)$
23	1	$(-138,0) = (-138,0) + 0 * (567433/4356, 1016523755/287496)$
26	1	$(-156,0) = (-156,0) + 0 * (1417, 53911)$ $(1417, 53911) = \mathcal{O} + (1417, 53911)$
29	0	$(-174,0) = (-174,0)$
31	1	$(-186,0) = (-186,0) + 0 * (35185/64, 7433335/512)$
34	0	$(-204,0) = (-204,0)$
35	0	$(-210,0) = (-210,0)$
37	0	$(-222,0) = (-222,0)$
38	0	$(-228,0) = (-228,0)$
41	1	$(-246,0) = (-246,0) + 0 * (82, 6724)$ $(82, 6724) = \mathcal{O} + (82, 6724)$
43	0	$(-258,0) = (-258,0)$
46	1	$(-276,0) = (-276,0) + 0 * (12, 7344)$ $(12, 7344) = \mathcal{O} + (12, 7344)$
47	1	$(-282,0) = (-282,0) + 0 * (-488617312694303/1733056399936,$ $3352636710520241 89265/2281492496034146816)$
53	0	$(-318,0) = (-318,0)$
55	1	$(-330,0) = (-330,0) + 0 * (75, 10125)$ $(75, 10125) = \mathcal{O} + (75, 10125)$ $(880, 30250) = (-330,0) - (75, 10125)$
58	1	$(-348,0) = (-348,0) + 0 * (-8439/25, 295191/125)$ $(51852, 11807640) = (-348,0) - (-8439/25, 295191/125)$
59	0	$(-354,0) = (-354,0)$
61	0	$(-366,0) = (-366,0)$
62	1	$(-372,0) = (-372,0) + 0 * (13461019400401/30178638400,$ $92310315227997559399/5242633062848000)$
65	1	$(-390,0) = (-390,0) + 0 * (-260, 8450)$ $(-260, 8450) = \mathcal{O} + (-260, 8450)$ $(4875, 342225) = (-390,0) - (-260, 8450)$
67	0	$(-402,0) = (-402,0)$
70	0	$(-420,0) = (-420,0)$
71	1	$(-426,0) = (-426,0) + 0 * (-5352400391/19096900, 813232264308227/83453453000)$
73	1	$(-438,0) = (-438,0) + 0 * (23907/49, 7409205/343)$
74	1	$(-444,0) = (-444,0) + 0 * (5809, 444925)$ $(5809, 444925) = \mathcal{O} + (5809, 444925)$
77	0	$(-462,0) = (-462,0)$
79	1	$(-474,0) = (-474,0) + 0 * (-186, 14040)$ $(-186, 14040) = \mathcal{O} + (-186, 14040)$
82	0	$(-492,0) = (-492,0)$
83	0	$(-498,0) = (-498,0)$

k	$\mathrm{rk}(\tilde{E}_k(\mathbb{Q}))$	integral points with their representation
85	2	$(-510,0) = (-510,0) + 0*(-204,15606) + 0*(1785/4,195075/8)$ $(-204,15606) = \mathcal{O} + (-204,15606) + 0*(1785/4,195075/8)$ $(3315,195075) = (-510,0) - (-204,15606) + 0*(1785/4,195075/8)$ $(3309186,6019796016) = (-510,0) - 2*(-204,15606) + (1785/4,195075/8)$ $(3540,214650) = \mathcal{O} + (-204,15606) - (1785/4,195075/8)$ $(-221,15317) = (-510,0) - (-204,15606) + (1785/4,195075/8)$ $(714,31212) = (-510,0) + 0*(-204,15606) - (1785/4,195075/8)$ $(-60,17550) = \mathcal{O} - (-204,15606) - (1785/4,195075/8)$ $(2091,101439) = (-510,0) + (-204,15606) + (1785/4,195075/8)$
86	0	$(-516,0) = (-516,0)$
89	1	$(-534,0) = (-534,0) + 0*(-40253237/127449,665725746673/45499293)$
91	0	$(-546,0) = (-546,0)$
94	1	$(-564,0) = (-564,0) + 0*(30263817/30976,234317843739/5451776)$
95	1	$(-570,0) = (-570,0) + 0*(3075,176175)$ $(3075,176175) = \mathcal{O} + (3075,176175)$
97	1	$(-582,0) = (-582,0) + 0*(623467/121,497854945/1331)$

Table 8: $3|k$

k	$\mathrm{rk}(\tilde{E}_k(\mathbb{Q}))$	integral points with their representation
-93	1	$(62,0) = (62,0) + 0 * (6597335332521/75619500100,$ $15717246614188482181/20794606332499000)$
-87	0	$(58,0) = (58,0)$
-78	1	$(52,0) = (52,0) + 0 * (527644/625, 384253272/15625)$
-69	1	$(46,0) = (46,0) + 0 * (713/4, 19573/8)$ $(118,1332) = (46,0) - (713/4, 19573/8)$
-66	0	$(44,0) = (44,0)$
-57	0	$(38,0) = (38,0)$
-51	1	$(34,0) = (34,0) + 0 * (187, 2601)$ $(187,2601) = \mathcal{O} + (187,2601)$ $(68,578) = (34,0) - (187,2601)$
-42	1	$(28,0) = (28,0) + 0 * (27713/64, 4626335/512)$
-39	0	$(26,0) = (26,0)$
-33	0	$(22,0) = (22,0)$
-30	1	$(20,0) = (20,0) + 0 * (425, 8775)$ $(425,8775) = \mathcal{O} + (425,8775)$
-21	1	$(14,0) = (14,0) + 0 * (273/16, 3577/64)$ $(302,5256) = (14,0) - (273/16, 3577/64)$
-15	0	$(10,0) = (10,0)$
-6	0	$(4,0) = (4,0)$
-3	1	$(2,0) = (2,0) + 0 * (3,5)$ $(3,5) = \mathcal{O} + (3,5)$ $(20,90) = (2,0) - (3,5)$
3	0	$(-2,0) = (-2,0)$
6	0	$(-4,0) = (-4,0)$
15	1	$(-10,0) = (-10,0) + 0 * (35,225)$ $(35,225) = \mathcal{O} + (35,225)$ $(0,50) = (-10,0) - (35,225)$
21	2	$(-14,0) = (-14,0) + 0 * (35,245) + 0 * (-7/4, 637/8)$ $(35,245) = \mathcal{O} + (35,245) + 0 * (-7/4, 637/8)$ $(4,90) = (-14,0) - (35,245) + 0 * (-7/4, 637/8)$ $(58,468) = (-14,0) + 0 * (35,245) - (-7/4, 637/8)$ $(-13,29) = \mathcal{O} - (35,245) - (-7/4, 637/8)$ $(868,25578) = (-14,0) + (35,245) + (-7/4, 637/8)$
30	1	$(-20,0) = (-20,0) + 0 * (25,225)$ $(25,225) = \mathcal{O} + (25,225)$ $(20,200) = (-20,0) - (25,225)$ $(7180,608400) = (-20,0) - 2 * (25,225)$
33	1	$(-22,0) = (-22,0) + 0 * (-117/49, 54095/343)$
42	1	$(-28,0) = (-28,0) + 0 * (1953/16, 90895/64)$

k	$\mathrm{rk}(\tilde{E}_k(\mathbb{Q}))$	integral points with their representation
51	2	$(-34,0) = (-34,0) + 0 * (17/4, 2601/8) + 0 * (153/4, 3757/8)$ $(102, 1156) = (-34,0) - (17/4, 2601/8) + 0 * (153/4, 3757/8)$ $(38, 468) = (-34,0) + 0 * (17/4, 2601/8) - (153/4, 3757/8)$ $(510, 11560) = (-34,0) + (17/4, 2601/8) + (153/4, 3757/8)$ $(14066174, 52755042600) = (-34,0) + 0 * (17/4, 2601/8) - 2 * (153/4, 3757/8)$
57	1	$(-38,0) = (-38,0) + 0 * (1643, 66625)$ $(1643, 66625) = \mathcal{O} + (1643, 66625)$
66	0	$(-44,0) = (-44,0)$
69	0	$(-46,0) = (-46,0)$
78	1	$(-52,0) = (-52,0) + 0 * (7124/25, 620568/125)$
87	1	$(-58,0) = (-58,0) + 0 * (50112/361, 13481230/6859)$
93	0	$(-62,0) = (-62,0)$

4.2.3 General 2-descent.

Here we take $E' = E$ and replace Φ by multiplication by 2 (instead of any positive integer $m \geq 2$) to obtain the *Kummer sequence*

$$0 \longrightarrow E(K)/2E(K) \xrightarrow{\partial} H^1(G, E(\overline{K})[2]) \longrightarrow H^1(G, E(\overline{K}))[2] \longrightarrow 0$$

and derive from it the exact sequence

$$0 \longrightarrow E(K)/2E(K) \longrightarrow S^{(2)}(E/K) \longrightarrow \mathrm{III}(E/K)[2] \longrightarrow 0$$

for the 2-parts $S^{(2)}(E/K)$ and $\mathrm{III}(E/K)[2]$ of the Selmer group and the Tate-Shafarevich group, respectively.

The elementary abelian 2-group $H^1(G, E(\overline{K}))[2]$ is isomorphic to the group $\mathcal{G}$ of equivalence classes of 2-coverings of E:

$$\mathcal{G} \cong H^1(G, E(\overline{K}))[2].$$

The subgroup G of $\mathcal{G}$ consisting of all equivalence classes of 2-coverings which have a rational point everywhere locally over K is isomorphic to the 2-Selmergroup

$$G \cong S^{(2)}(E/K),$$

and the subgroup G' of G of all equivalence classes of 2-coverings with a global rational point over K is isomorphic to $E(K)/2E(K)$:

$$G' \cong E(K)/2E(K).$$

The groups of G and G' are finite and have 2-power orders:

$$\sharp G = 2^k,\ \sharp G' = 2^{k'} \quad \text{with } k' \leq k.$$

Hence the order of the 2-Tate-Shafarevich group is:

$$\sharp \mathrm{III}(E/K)[2] = 2^{k-k'}.$$

In particular, the group $\mathrm{III}(E/K)[2]$ is trivial if and only if $k' = k$.

Now the 2-coverings of E which admit a rational point everywhere locally over K are represented by quartic equations of the form

$$Y^2 = \alpha X^4 + \beta X^3 + \gamma X^2 + \delta X + \epsilon =: g(X) \quad (\alpha, \beta, \gamma, \delta, \epsilon \in K).$$

Their invariants

$$I = 12\alpha\epsilon - 3\beta\delta + \gamma^2 \text{ and } J = 72\alpha\gamma\epsilon - 27\alpha\delta^2 - 27\beta^2\epsilon + 9\beta\gamma\delta - 2\gamma^3$$

are related to the Tate coefficients of E in (1.1) by the equations

$$I = \lambda^4 c_4 \text{ and } J = \lambda^6 2c_6 \quad \text{for some } \lambda \in K^*.$$

The algorithm of Birch and Swinnerton-Dyer ([2], see also [5]) for computing the rank of E over $K = \mathbb{Q}$ now consists in a stepwise search procedure

(i) for a region for α,

(ii) for a region for β, while α is fixed,

(iii) for a region for γ, while (α, β) is fixed,

(iv) for a region for δ and ϵ such that $I(\alpha, \beta, \gamma, \delta, \epsilon) = I$ and $J(\alpha, \beta, \gamma, \delta, \epsilon) = J$, while (α, β, γ) is fixed.

Of course, the quartics g arising in this way must be tested for triviality, equivalence, and local and global solvability.

This algorithm can also be used for finding independant points in $E(K)$. In fact, any global rational point (x, y) on a quartic over K can be taken to transform the quartic to an equivalent quartic

$$Y^2 = \alpha' X^4 + \beta' X^3 + \gamma' X^2 + \delta' X + \epsilon' \quad (\alpha', \beta', \gamma', \delta', \epsilon' \in K)$$

for which $\alpha' \in K^{*2}$. This is achieved by sending x to ∞. Then (see [6], [52])

$$P = \left(\frac{3\beta'^2 - 8\alpha'\gamma')}{4\alpha'}, \frac{27(\beta'^3 + 8\alpha'\delta' - 4\alpha'\beta'\gamma')}{8\alpha'^{3/2}} \right)$$

is a rational point on the elliptic curve

$$E' : \quad Y^2 = X^3 - 27IX - 27J$$

which is isomorphic over K to the given curve E.

Once all quartics belonging to a given pair (I, J) of invariants satisfying $I = \lambda^4 c_4$, $J = \lambda^6 2c_6$ have been found, the task remains of determining all pairs (I, J) which are *relevant* for the curve E. This is accomplished by a complicated reduction procedure sketched by Birch and Swinnerton-Dyer [2] for $K = \mathbb{Q}$ and generalized by P. Serf [52] for arbitrary number fields K. It turns out that, for quadratic fields K of class number one, the reduction leads to one, two, three or four pairs of invariants (I, J) to be taken into account for the task of determining the rank.

This algorithm was designed for $K = \mathbb{Q}$ by Birch and Swinnerton-Dyer [2] and implemented by Cremona [5]. It was further developed and implemented for some real quadratic fields K of class number one by P. Serf ([52], see also [6]). In fact the procedure works over the fields

$$K = \mathbb{Q}(\sqrt{D}) \quad \text{for } D = 5, 8, 12, 13$$

of class number one. It should be pointed out that the algorithm over real quadratic fields is rather involved and takes a lot of computing time, since the search regions for the first three coefficients α, β, γ are in general very large. That is why, in applying the algorithm, one must choose suitable examples requiring a manageable computing time.

We list here some examples. The elements of $K = \mathbb{Q}(\sqrt{D})$ are represented in the form

$$(x, y) = x + y\sqrt{D} \quad (D \in \mathbb{N} \text{ square-free}).$$

All curves are defined over K but not over $\mathbb{Q}$. Their 2-torsion groups are each trivial so that special 2-descent via 2-isogeny cannot be applied. The elliptic curves are represented in the form

$$E = [a_1, a_2, a_3, a_4, a_6] \quad \text{with } a_i \in K$$

and the quartics in the form

$$g = [\alpha, \beta, \gamma, \delta, \epsilon] \quad \text{over } K.$$

Example 1. $K = \mathbb{Q}(\sqrt{5})$,

$$E = [(-2,0),(2,-1),(-1,1),(1,-1),(0,0)]$$

$\underline{r = \mathrm{rk}(E/K) = 2:}$

One pair: $I = (64,16)$, $J = (-736,-464)$

$$\begin{array}{rcl}
g_1 & = & ((1,0),(0,0),(0,2),(-4,-4),(5,1)) \\
 & & \longrightarrow P_1 = ((-1,0),(-1,-1)) \\
g_2 & = & ((1,0),(0,0),(-84,50),(484,-300),(-791,493)) \\
 & & \longrightarrow P_2 = ((13,-8),(74,-46)) \\
g_3 & = & ((1,0),(0,0),(0,-10),(-12,-12),(-3,-7)) \\
 & & P_3 = ((-1,2),(-2,0)) \\
 & & \mathit{Relation:}\ 3P_3 = 5P_1 + P_2
\end{array}$$

Example 2. $K = \mathbb{Q}(\sqrt{5})$

$$E = [(-2,0),(0,1),(2,0),(-1,2),(-2,0)]$$

$\underline{\text{r = rk(E/K)=3:}}$

Two pairs: $I = (11,-3)$, $(J = 8,-7)$

$$\begin{array}{rcl}
g_1 & = & [(1,0),(0,-1),(1,1),(-1,-1),(1,0)] \\
 & & \longrightarrow P_1 = (\frac{1}{4}(-3,-3), \frac{1}{8}(-19,-8)) \\
\multicolumn{3}{l}{I = (176,-48),\ J = (512,-448)} \\
g_2 & = & [(1,0),(0,0),(4,-2),(8,-8),(13,-3)] \\
 & & \longrightarrow P_2 = ((-1,0),(-1,-1)) \\
g_3 & = & [(1,0),(0,0),(-248,154),(-2504,1544),(-7087,4385)] \\
 & & \longrightarrow P_3 = ((41,-26),(-273,167)) \\
g_4 & = & [(1,0),(0,0),(-218,136),(2064,-1280),(-5487,3396)] \\
 & & \longrightarrow P_4 = ((36,-23),(293,-183)) \\
g_5 & = & [(1,0),(0,0),(-56,-110),(-536,-872),(-1255,-2039)] \\
 & & \longrightarrow P_5 = ((9,18),(-59,-91)) \\
g_6 & = & [(1,0),(0,0),(-2,-8),(0,-16),(9,-12)] \\
 & & \longrightarrow P_6 = ((0,1),(-1,-1)) \\
g_7 & = & [(1,0),(0,0),(-92,-26),(24,-536),(-747,-459)] \\
 & & P_7 = ((15,4),(17,-63)) \\
 & & \mathit{Relations:}\ \ P_4 = P_1 + 5P_2 + P_3, \\
 & & \qquad\qquad\quad P_5 = -P_1 + 2P_2 + P_3 \\
 & & \qquad\qquad\quad P_6 = P_2 + P_3, \\
 & & \qquad\qquad\quad P_7 = -P_1 + P_2 + 2P_3.
\end{array}$$

Example 3. $K = \mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2})$

$$E = [(0,0),(1,2),(0,0),(0,1),(-1,-1)]$$

$\underline{R = \mathrm{rk}(E/K) = 0:}$

Three pairs: $I = (9, 1),\ J = (13, -8)$
$I = (36, 4),\ J = (104, -64)$
$I = (144, 16),\ J = (832, -512)$
$\longrightarrow$ no points

Example 4. $K = \mathbb{Q}(\sqrt{12}) = \mathbb{Q}(\sqrt{3})$

$$E = [(0, 0), (-2, -1), (0, 0), (-3, 0), (-2, 3)]$$

$\underline{r = \mathrm{rk}(E/K) = 2:}$

Three pairs: $I = (16, -9),\ J = (655, -378)$
$\longrightarrow$ no points
$I = (16, 4),\ J = (160, -24)$

$$\begin{aligned} g_1 &= [(5, 3), (-2, 0), (-2, 2), (-4, 2), (-5, 3)] \\ &\quad \longrightarrow P_1 = (1, -1), (0, 1)) \\ g_2 &= [(1, 1), (2, 2), (4, 2), (4, 0), (1, 0)] \\ &\quad \longrightarrow P_2 = ((2, -1), (2, -2)) \\ g_3 &= [(1, 1), (-2, 2), (-8, 2), (-6, 2), (-2, 1)] \\ &\quad \longrightarrow P_3 = ((30, -9), (-130, 102)) \end{aligned}$$

$I = (640, 368),\ J = (24640, 14208)$
$\longrightarrow$ no points
Relation: $P_3 = P_1 + P_2$

Example 5. $K = \mathbb{Q}(\sqrt{13})$

$$E = [(0, 0), (2, -1), (0, 0), (-1, -1), (-3, 1)]$$

$\underline{r = \mathrm{rk}(E/K) = 1:}$

Two pairs: $I = (10, 0),\ J = (44, -7)$
$\longrightarrow$ no points
$I = (160, 0),\ J = (2816, -448)$
$\longrightarrow P_1 = ((3, 0), (-6, 1))$

4.2.4 General 3-descent.

In cases where general 2-descent is not applicable since the 2-Tate-Shafarevich group is non-trivial, 3-descent is employed for determining the rank and independent generators. The method described by J. Quer [43] is used by Gebel [13] (see also [15], [16], [17]). It works when the 3-Tate-Shafarevich group is trivial.

4.3 Integral and S-Integral points.

We consider elliptic curves E defined over a number field K. Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$ be a finite set of places of K including the infinite ones $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$. It is of interest, e. g. in view of Theorem 2.3 and the conjecture 2.3 of Lang and Demjanenko, to determine all S-integral points on elliptic curves E over K. This fundamental task can be solved by a method of Lang [30] and Zagier [65]. The method is based on the assumption that the Mordell-Weil group $E(K)$ is known. Of course, the coefficients a_i of the general Weierstrass equation (1.1) for E must be integers in K:

$$a_i \in \mathcal{O}_{\mathcal{K}} \quad (i = 1, 2, 3, 4, 6).$$

Since, for $K = \mathbb{Q}$ the rank r and a basis of $E(K)$ can be computed by the algorithm explained in subsection 4.2, the method of Lang and Zagier is applicable in this case. We shall explain the procedure in the general case. Let $P_1, \ldots, P_r \in E(K)$ be a basis of $E(K)$. Then any rational point $P \in E(K)$ has a unique representation of the form

$$P = n_1 P_1 + \cdots + n_r P_r + P_{r+1} \quad (n_i \in \mathbb{Z}) \tag{4.3.1}$$

with a torsion point $P_{r+1} \in E_{tors}(K)$. The problem we encounter here consists in finding a bound N_1 for the coefficients n_i:

$$|n_i| \leq N_1 \quad (i = 1, \ldots, r)$$

such that all S-integral points in $E(K)$ have coefficients n_i within that range.

Such a bound is obtained by estimating the x-coordinate of an S-integral point $P = (x, y) \in E(K)$ from above and below and then comparing the upper and lower bound.

The *lower* bound arises from the method of successive minima in geometry of numbers via height estimates. Starting from the long Weierstrass equation (1.1) for E, we use Tate's coefficients $b_2, b_4, b_6, b_8 \in \mathcal{O}_K$ to define for $\mathfrak{p} \in \mathcal{M}_K$ the quantities:

$$\mu_{\mathfrak{p}} := \min\{v_{\mathfrak{p}}(b_2), \frac{1}{2}v_{\mathfrak{p}}(b_4), \frac{1}{3}v_{\mathfrak{p}}(b_6), \frac{1}{4}v_{\mathfrak{p}}(b_8)\}$$

and

$$\alpha_{\mathfrak{p}} := \left\{ \begin{array}{cl} -\log\ 2 & \text{if } \mathfrak{p} = \mathfrak{q} \text{ is an infinite place} \\ 0 & \text{if } \mathfrak{p} \text{ is a finite place} \end{array} \right\}.$$

Then we put (see [66])

$$\mu := -\sum_{\mathfrak{p} \in \mathcal{M}_K} n_{\mathfrak{p}} \mu_{\mathfrak{p}} \geq 0$$

and

$$\alpha := -\sum_{\mathfrak{p} \in \mathcal{M}_K} n_{\mathfrak{p}} \alpha_{\mathfrak{p}} \geq 0,$$

where $n_{\mathfrak{p}}$ are the local degrees introduced in section 4.2.1. If we restrict to the infinite places $\mathfrak{q} \in \mathcal{M}_K$, we have

$$\mu_{\mathfrak{q}} = -\max\{\log|b_2|_{\mathfrak{q}}, \frac{1}{2}\ \log|b_4|_{\mathfrak{q}}, \frac{1}{3}\ \log|b_6|_{\mathfrak{q}}, \frac{1}{4}\ \log|b_8|_{\mathfrak{q}}\}.$$

Summing over the infinite places only yields the quantity

$$\mu_\infty := -\sum_{\mathfrak{q}|\infty} n_{\mathfrak{q}} \mu_{\mathfrak{q}} \geq 0.$$

One readily establishes for the heights of $P \in E(K)$ the estimates (see [66])

$$-\frac{1}{2}(\mu + \mu_\infty) - \frac{4}{3}\alpha \leq \hat{h}(P) - h(P) \leq \frac{1}{2}(\mu_\infty + \alpha).$$

Hence, in particular

$$h(P) \geq \hat{h}(P) - \frac{1}{2}(\mu_\infty + \alpha) \quad \text{ for } P \in E(K).$$

Let $\lambda_1 \in \mathbb{R}$, $\lambda_1 > 0$, be the smallest eigenvalue of the regulator matrix

$$(\hat{h}(P_i, P_j))_{i,j=1,\ldots,r}.$$

Then

$$\hat{h}(P) \geq \lambda_1 N^2$$

for

$$N := \max_{i=1,\dots,r} \{|n_i|\} \tag{4.3.2}$$

in the basis representation (4.3.1) of P. Therefore,

$$h(P) \geq \lambda_1 N^2 - \frac{1}{2}(\mu_\infty + \alpha) \quad \text{for } P \in E(K).$$

For any point $P = (x, y) \in E(K)$, we choose a place $\mathfrak{r} \in S$ such that

$$|x|_{\mathfrak{r}} = \max_{i=1,\dots,s; j=1,\dots,t} \{|x|_{\mathfrak{p}_i}, |x|_{\mathfrak{q}_j}\}.$$

Then we conclude (cf. [16]) that, for any S-integral point $P \in E(K)$,

$$h(P) \leq \frac{s+t}{2} \log |x|_{\mathfrak{r}}$$

and hence

$$\lambda_1 N^2 - \frac{1}{2}(\mu_\infty + \alpha) \leq \frac{s+t}{2} \log |x|_{\mathfrak{r}}.$$

Exponentiating leads to the desired lower estimate

$$C_2 \cdot e^{C_1 N^2} \leq |x|_{\mathfrak{r}}^{\frac{1}{2}}, \tag{4.3.3}$$

where

$$C_1 := \frac{\lambda_1}{s+t}, \quad C_2 := \exp\left\{-\frac{1}{2}\frac{\mu_\infty + \alpha}{s+t}\right\}.$$

The *upper* bound for $|x|_{\mathfrak{r}}^{\frac{1}{2}}$ is derived by virtue of elliptic logarithms. Here we assume E to be given in short Weierstrass form (1.2) over K with coefficients $a, b \in \mathcal{O}_{\mathcal{K}}$. The curve E is parametrized by the Weierstrass function $\wp(u)$ with respect to a lattice $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ in $\mathbb{C}$ and its derivative $\wp'(u)$. In fact, we have

$$P = (x, y) = (\wp(u), \frac{1}{2}\wp'(u)) \in E(K),$$

and the argument $u \in \mathbb{C}$ modulo Ω (suitably normalized, see [14], [65]) is called the (classical) *elliptic logarithm* of P. Suppose that S consists only of the infinite places of K:

$$S = \{\mathfrak{q}_1, \dots, \mathfrak{q}_t\}$$

so that the S-integral points are simply the ordinary integral points of E over K. Then it suffices to consider the classical elliptic logarithms of the integral points in $E(K)$.

Denote by $n = [K : \mathbb{Q}]$ the degree of $K/\mathbb{Q}$, by $g = \sharp E_{tors}(K)$ the order of the torsion group of E/K and by C the constant (see [7])

$$C := 2,9 \cdot 10^{6(r+1)} \cdot 4^{2r^2}\ (r+1)^{2r^2+9r+12,3}.$$

We define the *height* of the curve E in terms of the coefficients $a, b \in \mathcal{O}_{\mathcal{K}}$ and the invariant j of E by

$$h(E) := h(a, b, j) := \log \prod_{\mathfrak{p} \in \mathcal{M}_K} \max\{1, |a|_{\mathfrak{p}}, |b|_{\mathfrak{p}}, |j|_{\mathfrak{p}}\}$$

and set

$$h = \max\{1, h(E)\}.$$

Let $u_i \in \mathbb{C}$ denote the elliptic logarithm of the basis point P_i $(i = 1, \ldots, r)$ and denote by τ the quotient of the periods ω_1, ω_2:

$$\tau = \frac{\omega_2}{\omega_1} \in \mathbb{C}.$$

In fact one chooses the lattice $\Omega = \mathbb{Z} + \mathbb{Z}\tau$ and normalizes the u_i to $0 < |u_i| \leq \frac{1}{2}$. Then, we select real numbers $V_i \in \mathbb{R}$ such that (see [7])

$$\log(V_i) \geq \max\left\{\hat{h}(P_i), h, \frac{3\pi|u_i|^2}{|\omega_1|^2 \ \mathrm{Im}(\tau n)}\right\} \qquad (i = 1, \ldots, r)$$

and $\rho \in \mathbb{R}$ such that

$$e \leq \rho \leq \min\left\{\frac{e(n \ \log \ V_i)^{\frac{1}{2}}}{\frac{\sqrt{3\pi}|u_i|}{|\omega_1|\sqrt{\mathrm{Im}(\tau)}}}\right\} \qquad\qquad (1 \leq i \leq r).$$

By increasing N if need by we can ensure that

$$n \ \log\left(\frac{n+1}{2}gN\right) \geq \log \ V_i \quad (i = 1, \ldots, r).$$

Then a theorem of S. David [7] yields the desired upper estimate with respect to $\mathfrak{r} \in S$:

$$(4.3.4) \qquad \begin{array}{rcl} |x|_{\mathfrak{r}}^{\frac{1}{2}} & < & c_1 \ \exp\{\frac{C}{(\log \ g)^{2r+1}} n^{2(r+1)}(\log(\frac{r+1}{2}gN) + \log(n\rho)) \\ & \cdot & (\log\log(\frac{r+1}{2}gN) + \log(n\rho))^{r+1} \prod_{i=1}^{r} \log \ V_i\}. \end{array}$$

Here the factor c_1 in front of the exponential equals $\frac{g\sqrt{8}}{|\omega_1|}$ if K is a totally real field.

After some computations one derives from the inequalities (4.3.3) and (4.3.4) an inequality of the shape (cf. [14])

$$N^2 < C_1' + C_2' \ \log^{r+2} N^2.$$

Since, for a sufficiently large N, the left hand expression exceeds the right hand expression, the number N must be bounded above. Indeed, to see this, we put

$$N_0 := 2^{r+2}\sqrt{C_1' C_2'} \log^{\frac{r+2}{2}}(C_2'(r+2)^{r+2}),$$

enlarge N_0 if necessary to ensure that

$$N_0 > \max\left\{e^e, (6(r+1))^2, \sqrt{\frac{\log(2gc_1)}{\lambda_1}}\right\}$$

and define

$$N_1 := \max\left\{N_0, \frac{2V}{r+1}\right\}$$

with

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

Then, this N_1 is the desired upper bound for the maximum N in (4.3.2) of the absolute values of the coefficients n_i in the basis representation (4.3.1) of an integral point $P \in E(K)$.

In the general case of an arbitrary finite set of places

$$S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$$

of K including the infinite places $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$, one must argue with $\mathfrak{p}$-adic elliptic logarithms in addition to the classical elliptic logarithm. One obtains an upper bound for N in a similar manner (cf. [16], [59]). However, in the general case no explicit constant C for $\mathfrak{p}$-adic elliptic logarithms is known unless $r \leq 2$. Such a constant should be of a similar type as the above constant C for the complex elliptic logarithm. The constant C for $r \leq 2$ for the $\mathfrak{p}$-adic elliptic logarithm was given by Rémond and Urfels [44]. For $r > 2$ we hope to use new estimates for the size of integer points obtained by Hajdu and Herendi [20].

The bound N_1 for N is by far too large for practical calculations of integral or S-integral points. However, de Weger reduction (see [63]) via numerical diophantine approximation leads to a bound N_1' of order of magnitude ~ 10, and with this bound, the integral or S-integral points can be computed.

To date this algorithm was applied only to elliptic curves E over the rational number field $K = \mathbb{Q}$ (see [14], [15], [16], [17], [59] and [62]). However, we hope to extend it to quadratic fields K as ground fields and implement it in SIMATH, as this was done already in the case of $K = \mathbb{Q}$.

Table 9

X-coordinates of integral points on the rank 7 curve

$$E: \ Y^2 + 1641Y = X^3 - 168X^2 + 161X - 8$$

-53, -52, -46, -43, -41, -24, -17, 5, 9, 26, 44, 50, 65, 69, 76, 88, 99, 100, 101, 102, 103, 120, 122, 123, 125, 142, 145, 159, 185, 187, 192, 244, 258, 292, 323, 328, 407, 477, 494, 576, 655, 990, 1104, 1137, 1334, 1455, 1563, 2080, 2326, 3103, 3298, 4724, 6162, 6588, 14907, 17389, 30243, 40324, 44069, 48170, 57634, 85145, 108498, 116755, 166618, 224949, 235985, 650243, 1045726, 5552299, 6524989, 23188554, 83552324

A particular interesting application of the algorithm is to Mordell's elliptic curves

$$E_k: \quad Y^2 = X^3 + k \quad (k \in \mathbb{Z}).$$

J. Gebel et al. ([13], [15], [17]), with the exception of about 20 curves, computed all integral points in $E_k(\mathbb{Q})$ for

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

Moreover, for $S = \{2, 3, 5, \infty\}$ all S-integral points on Mordell's curves (see [15]) in the range

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

could also be computed. It turns out that the strong version of Hall's conjecture 2.5 holds in the range $|k| \leq 100,000$ with the constant

$$C = 5.$$

The rank of Mordell's curves grows with the number of digits in k and is less than or equal to 5 in the range $|k| \leq 100,000$. In this larger range, there were about 1,200 cases in which no generator could be found and hence, we believed that there were no integral points on these curves. In the meantime, this was proved by K. Wildanger [64]. We hope to settle the case of the 20 exceptional curves in the near future.

In table 10.1, we list all S-integral points on the elliptic curve

$$E: \quad Y^2 = X^3 - 43847$$

over the rationals for sets of places

$$S_n = \{p_1, \dots, p_n, \infty\} \quad (0 \le n \le 8)$$

and primes

$$\begin{aligned} p_1 &= 2, \\ p_2 &= 3, \\ p_3 &= 5, \\ p_4 &= 7, \\ p_5 &= 11, \\ p_6 &= 13, \\ p_7 &= 17, \\ p_8 &= 19. \end{aligned}$$

The Mordell-Weil group has

$$\begin{array}{ll} \text{torsion group} & E_{tors}(\mathbb{Q}) = \{\mathcal{O}\}, \\ \text{rank} & r = \mathrm{rk}_{\mathbb{Q}} E = 5 \end{array}$$

and basis points with Néron-Tate heights

$$\begin{array}{ll} P_1 = (38,\, 105), & \hat{h}(P_1) = 3.1417818777, \\ P_2 = (56,\, 363), & \hat{h}(P_2) = 3.3800071986, \\ P_3 = (62,\, 441), & \hat{h}(P_3) = 3.4491918254, \\ P_4 = (36,\, 53), & \hat{h}(P_4) = 3.6612335368, \\ P_5 = (87,\, 784), & \hat{h}(P_5) = 4.7085278296. \end{array}$$

In the table the points are represented by

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

where

$$\xi,\ \eta,\ \zeta \in \mathbb{Z}, \quad \zeta > 0, \quad \text{and} \quad \gcd(\xi,\, \zeta) \;=\; 1 \;=\; \gcd(\eta,\, \zeta).$$

In the column F we display the prime factorization of the denominator ζ.[3]

[3] I wish to thank J. Gebel for providing me with these data.

Table 10.1

S	ξ	η	ζ	F	linear combination
S_0	36	53	1		P_4
	38	105	1		P_1
	51	298	1		$-P_2-P_3$
	56	363	1		P_2
	62	441	1		P_3
	87	784	1		P_5
	96	917	1		$-P_1-P_3$
	263	4260	1		$-P_3+P_4$
	582	14039	1		P_1-P_2
	602	14769	1		$-P_1-P_4$
	872	25749	1		$P_1+P_2+P_3$
	912	27541	1		$-P_2-P_3+P_4+P_5$
	1226	42927	1		P_2-P_5
	2252	106869	1		P_3-P_5
	6167	484296	1		$-P_1+P_4$
	14382	1724761	1		$P_1+P_3-P_4-P_5$
	17838	2382425	1		P_2-P_3
	35538	6699455	1		$P_1+P_3+P_5$
S_1	177	1655	2	2	$P_2+P_3-P_5$
	593	14343	2	2	$-P_2-P_4$
	641	9153	4	2^2	$-P_3+P_4+P_5$
	6681	545923	4	2^2	P_1-P_3
	28369697	151106117169	4	2^2	$P_1+2P_2+2P_3-P_4-P_5$
	13329	1535111	8	2^3	$-P_1+P_2-P_4-P_5$
	5652998361	425028731908067	64	2^6	$P_1-P_2+2P_3-P_4-P_5$
S_2	742	19405	3	3	$-P_4-P_5$
	1003	31258	3	3	$-P_1-P_2$
	1618	64837	3	3	$P_2+P_3-P_4$
	2866	15463	9	3^2	$P_1+P_3-P_5$
	3892	188819	9	3^2	$P_1-P_2+P_5$
	2910664	4965785569	27	3^3	$P_1+P_2-P_4-P_5$
	4008943	8026842932	27	3^3	$2P_2+2P_3-P_5$
	15885262	63241473005	243	3^5	$-2P_1+P_2-P_3$
	4657	314569	6	$2\cdot 3$	$P_1+P_3+P_4$
	247969	123473809	18	$2\cdot 3^2$	$-P_2-P_3-P_5$
	217616881633	57123378374292143	73728	$2^{13}\cdot 3^2$	$-3P_2-P_3+P_4+P_5$

S	ξ	η	ζ	F	linear combination
S_3	1884	77473	5	5	$P_1+P_3-P_4$
	4586	309459	5	5	$-P_1-P_2-P_3+P_5$
	5576	415551	5	5	$P_1+P_4+P_5$
	8516	785439	5	5	$-P_2+P_4$
	11514	1235213	5	5	$P_2+P_3+P_4$
	60194	14768253	5	5	$P_1-P_2-P_3+P_5$
	434246	286156581	5	5	$-2P_2-P_3$
	51839204	373239403233	5	5	$2P_1-P_2+P_4$
	24524	2011107	25	5^2	$-P_3-P_5$
	68579	17658642	25	5^2	$P_2+2P_3-P_4-P_5$
	1612899	2048378482	25	5^2	$-P_1-P_3-P_4+P_5$
	611121	477739081	10	$2\cdot5$	$P_1+P_2+P_5$
	15929	1111533	20	$2^2\cdot5$	$P_1-P_2+P_3$
	112361	35198859	40	$2^3\cdot5$	$-P_1+P_4+P_5$
	9004	480133	15	$3\cdot5$	$-P_1+P_3-P_4$
	4735351	10304531776	15	$3\cdot5$	$-2P_1-P_2-P_3-P_4$
	85486	16143859	45	$3^2\cdot5$	$P_1+P_2+2P_3$
S_4	3284	173949	7	7	$-P_1-P_5$
	5394	389591	7	7	$P_1+P_2+P_4$
	10004	998019	7	7	P_1-P_5
	75203	20622918	7	7	$P_2+P_4+P_5$
	87807273	159221895083	1568	$2^5\cdot7^2$	$-2P_5$
	21226	2408867	21	$3\cdot7$	$-P_1+P_2+P_4$
	1014568	775831463	147	$3\cdot7^2$	$-2P_3$
	44171	2361906	35	$5\cdot7$	$-P_2-P_4+P_5$
	428184	280041623	35	$5\cdot7$	$-2P_1$
	104246676	992329814701	1225	$5\cdot7^2$	$P_1-P_2+2P_4+P_5$
S_5	295916	160972623	11	11	$-P_1+P_2-P_3+P_4$
	532448	388522065	11	11	$-P_2-2P_3$
	31662	5626981	11	11	$-P_1+P_3-P_4-P_5$
	818832	641408291	121	11^2	$-2P_2$
	21569	2250111	22	$2\cdot11$	$-P_1-P_2-P_3+P_4$
	17073	72073	22	$2\cdot11$	$-P_1-P_2+P_5$
	912521	871511973	22	$2\cdot11$	$P_3-P_4+P_5$
	291448	157160843	22	$2\cdot11$	$-P_2-P_3-P_4+P_5$
	730743478	19753650521227	22	$2\cdot11$	$P_1-P_2+2P_4$
	688884	570704723	22	$2\cdot11$	$-P_1+P_2+P_5$
	3999186	6707955691	22	$2\cdot11$	$-P_2-P_3+P_4+2P_5$
	24731646	113916861181	605	$5\cdot11$	$-P_1-P_2-2P_4$
	3589433	6757328115	154	$2\cdot7\cdot11$	$-P_1-2P_3+P_5$
	4901851	10811918474	165	$3\cdot5\cdot11$	$P_1-2P_2-P_3+P_4+P_5$

S	ξ	η	ζ	F	linear combination
S_6	6447	237320	13	13	$-P_1+P_2-P_4$
	21074	3024501	13	13	$-P_3-P_4$
	22208	3277383	13	13	$-P_1+P_2+P_3$
	1135872	1210581575	13	13	$-P_1-P_2-P_4+P_5$
	30670721	169187731647	416	$2^5\cdot 13$	$2P_2+P_3+P_4-P_5$
	723736737	19025004651121	2704	$2^4\cdot 13^2$	$2P_1+P_2+P_3+P_4+P_5$
	922726	886270897	39	$3\cdot 13$	$-2P_3+P_4+P_5$
	1752956	2320187979	65	$5\cdot 13$	$P_3-2P_4-P_5$
	1111171812	32051953250351	4459	$7^3\cdot 13$	$-P_1+P_2+2P_3-2P_4-P_5$
	1576786	1228644091	195	$3\cdot 5\cdot 13$	$2P_2-P_5$
	1101613422274	1156228920836465111	2457	$3^3\cdot 7\cdot 13$	$P_1-P_2-2P_3-P_4$
S_7	12278	890247	17	17	$-P_2+P_4+P_5$
	42294	8636921	17	17	P_4-P_5
	415379	267709386	17	17	P_1+2P_3
	737073	350701865	136	$2^3\cdot 17$	$P_1+2P_2+P_3$
	542160137	12623836852581	136	$2^3\cdot 17$	$P_1+P_2+P_3+2P_4$
	2669009	1121000679	272	$2^4\cdot 17$	$-2P_1+P_2$
	147088	49098745	51	$3\cdot 17$	$-P_1-P_2-2P_3+P_4+P_5$
	55506019	413532270386	153	$3^2\cdot 17$	$-P_2+P_3-2P_4$
	682464	548931313	85	$5\cdot 17$	$-P_2+P_3-P_4-P_5$
	5920214	14339534139	187	$11\cdot 17$	$-P_1-P_2-P_3-P_4-P_5$
	2961331998	161073602112097	2873	$13^2\cdot 17$	$-P_1-P_2-2P_3+2P_5$
	603907049	9303235598859	3808	$2^5\cdot 7\cdot 17$	P_2-2P_4
	47503344326	8959109425064301	29155	$5\cdot 7^3\cdot 17$	$2P_1-P_2-P_4+P_5$
S_8	13268	522375	19	19	$-P_1-P_2-P_3-P_4$
	18251	2004138	19	19	$P_1+P_2+P_3-P_4-P_5$
	2571713	4058053983	152	$2^3\cdot 19$	$P_1-P_4+P_5$
	1370503099	50735747678734	1083	$3\cdot 19^2$	$2P_1+P_4-P_5$
	11871451	40889648258	171	$3^2\cdot 19$	$P_2+P_3-2P_5$
	6885642	17966861119	209	$11\cdot 19$	$2P_4+P_5$
	125182873	1400608281923	228	$2^2\cdot 3\cdot 19$	$-2P_1+P_2+P_3-P_4-P_5$
	275187041	4333187977839	1900	$2^2\cdot 5^2\cdot 19$	$-P_1+P_2+P_3-2P_4$
	28172592214937	149534090523948547395	532	$2^2\cdot 7\cdot 19$	$-3P_2$

The Tate-Shafarevich groups for Mordell's curves

$$E_k: \quad Y^2 = X^3 + k, \quad |k| \leq 100,000.$$

were also computed by J. Gebel.

Table 10.2

#Ш	number of curves	group structure
1	$166,412$	$(1) \times (1)$
4	$19,909$	$(2) \times (2)$
9	$10,773$	$(3) \times (3)$
16	$1,726$	$(4) \times (4)$
16	81	$(2) \times (2) \times (2) \times (2)$
25	478	$(5) \times (5)$
36	499	$(6) \times (6)$
49	85	$(7) \times (7)$
64	25	$(8) \times (8)$
81	9	$(9) \times (9)$
100	3	$(10) \times (10)$
total	$200,000$	

Curves with large Tate-Sharareivč group arise for the following k's.

Table 10.3

#Ш	k						
100	−96414	−85417	−59118				
81	−96505	−96253	−92459	−88754	−79242	−71870	−70934
	−67658	−56157					
64	−98654	−98485	−93346	−92606	−92338	−87874	−86677
	−85410	−82960	−78361	−75309	−73986	−71809	−71737
	−65985	−65885	−64149	−56885	−56409	−56302	−48562
	−43998	−43765	−40930	55101			
49	−98521	−97133	−95973	−94894	−94370	−93885	−93840
	−92886	−92121	−90798	−90464	−90357	−87809	−85793
	−83238	−83210	−82553	−81357	−80685	−80629	−79710
	−78478	−77766	−77486	−77136	−75085	−74238	−71942
	−69557	−68981	−68370	−68022	−67893	−66489	−66202
	−65670	−62394	−61386	−60242	−60145	−59342	−57506
	−55366	−55338	−54510	−53294	−52809	−52657	−52305
	−52097	−51422	−50018	−49120	−47993	−47265	−46238
	−43830	−43746	−43718	−43358	−41805	−39929	−37941
	−37733	−36914	−35808	−28213	−25126	−23397	−21353
	−20338	−19302	−19113	−18077	−16101	50551	54970
	59595	69703	83626	84181	85586	88085	89170
	93335						

5. Constructions.

Recently some elliptic curves E of high rank r over the field of rational numbers $\mathbb{Q}$ have been constructed. Nagao and Kouya [40] found curves of rank $r \geq 21$ by applying a method of Mestre. He first constructs a curve of high rank over the rational function field $\mathbb{Q}(T)$ and then obtains $E/\mathbb{Q}$ by specializing the variable T to suitable values $t \in \mathbb{Q}$. Over $\mathbb{Q}(T)$, Nagao [39] obtained a curve of rank ≥ 13. Recently Fermigier [9] pushed ahead slightly by coming up with a curve E of rank

$r \geq 22$ over $\mathbb{Q}$. Basically, he used the same method of Mestre. All these curves have trivial torsion group. Curves with non-trivial torsion group, e. g.

$$E_{tors}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z},$$

tend to have lower ranks. For instance, U. Schneiders (see [48]) found curves of rank $r = 11$. Here the rank can be exactly computed by 2-descent via 2-isogeny. Curves of rank $r = 10$ had been obtained previously by Kretschmer [29]. By refining the method of Mestre and bringing in some ideas of Kretschmer, Fermigier [9] succeeded in finding curves with torsion group $E_{tors}(\mathbb{Q}) \geq \mathbb{Z}/2\mathbb{Z}$ and exact rank $r = 14$. Moreover, Fermigier constructed an infinite number of elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z}$ and rank $r \geq 8$. This infinite set is obtained by spezializing a curve over $\mathbb{Q}(T)$ of rank $r \geq 8$. In view of these endeavors, it is therefore of interest to study the rank of curves over number fields other than $\mathbb{Q}$.

5.1 Rank of elliptic curves over multiquadratic fields.

The rank of an elliptic curve E over a multiquadratic number field K is known to tend to infinity with the degree of K over $\mathbb{Q}$, i. e. with $2^n = [K : \mathbb{Q}]$ (see [4], [11], [27]). However, it takes some effort to actually construct elliptic curves E and multiquadratic fields K such that E over K has large rank. This can be done in the following manner. We start from the curve E in normal form (1.3) with coefficients $c, d \in \mathbb{Z}$ and consider E as a curve over the multiquadratic field $K_n = \mathbb{Q}(\sqrt{D_1}, \ldots, \sqrt{D_n})$ generated by square-free integers $D_i \in \mathbb{Z}$ such that K_n over $\mathbb{Q}$ has degree

$$2^n = [K_n : \mathbb{Q}].$$

Let

$$\mathcal{D}_n := \{D \in \mathbb{Z} \mid D = \prod_{i=1}^{n} D_i^{e_i},\ e_i \in \{0, 1\}\}.$$

Then the rank of E over K_n is given in terms of the ranks of the D_i-twists E_{D_i} over $\mathbb{Q}$ by the formula (see, e. g. [27], [51])

$$\mathrm{rk}_{K_n}(E) = \sum_{D \in \mathcal{D}_n} \mathrm{rk}_{\mathbb{Q}}(E_D).$$

The problem is to make sure that each D-twist E_D has rank at least one over $\mathbb{Q}$. This is accomplished by 2-descent via 2-isogeny in the following way (cf., e. g. [48]):
Suppose that we have a decomposition $d = d_1 d_2$ for $d_1, d_2 \in \mathbb{Z}$ such that

$$d_1 + c + d_2 = Dz^2 \text{ for } z, D \in \mathbb{Z},\ D \neq 1,\ D \text{ square-free}$$

and

$$\begin{aligned} & c^2 - 4d \in \mathbb{Q}^{*2}, \\ & d_1 \not\equiv d_2 \mod \mathbb{Q}^{*2}, \\ & d_1, d_2 \not\equiv D \mod \mathbb{Q}^{*2}. \end{aligned}$$

Then

$$\mathrm{rk}_{\mathbb{Q}}(E_D) \geq 1.$$

A corresponding result is true also over an arbitrary number field K in place of $\mathbb{Q}$. This construction rendered e. g. an example of an elliptic curve E over $\mathbb{Q}$ of rank $r \geq 28$ over K_n constructed by M. Sens [51]. However, in view of the fact that Fermigier obtained curves E of rank $r \geq 22$ already over $\mathbb{Q}$, the above construction obviously requires a considerable refinement. This can probably be achieved by the method explained by Frey and Jarden [11].

Example

$$E: \; Y^2 = X^3 + cX^2 + dX$$

Table 11

$$\begin{aligned} c &= 616349365 \\ d &= 1041756931095803 \\ &= 13 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 59 \end{aligned}$$

$\mathrm{rk}_{\mathbb{Q}} E \geq 9$	
D_1 = -10362359	$\mathrm{rk}(E_{D_1}(\mathbb{Q})) \geq 1$
D_2 = -8236631	$\mathrm{rk}(E_{D_2}(\mathbb{Q})) \geq 1$
D_3 = -7554911	$\mathrm{rk}(E_{D_3}(\mathbb{Q})) \geq 1$
D_4 = -4948679	$\mathrm{rk}(E_{D_4}(\mathbb{Q})) \geq 1$
D_5 = -2052431	$\mathrm{rk}(E_{D_5}(\mathbb{Q})) \geq 1$
D_6 = -898631	$\mathrm{rk}(E_{D_6}(\mathbb{Q})) \geq 1$
D_7 = -56159	$\mathrm{rk}(E_{D_7}(\mathbb{Q})) \geq 1$
D_8 = -5759	$\mathrm{rk}(E_{D_8}(\mathbb{Q})) \geq 1$
D_9 = 68209	$\mathrm{rk}(E_{D_9}(\mathbb{Q})) \geq 1$
D_{10} = 274201	$\mathrm{rk}(E_{D_{10}}(\mathbb{Q})) \geq 1$
D_{11} = 788329	$\mathrm{rk}(E_{D_{11}}(\mathbb{Q})) \geq 1$
D_{12} = 2051329	$\mathrm{rk}(E_{D_{12}}(\mathbb{Q})) \geq 1$
D_{13} = 3997729	$\mathrm{rk}(E_{D_{13}}(\mathbb{Q})) \geq 1$
D_{14} = 4204561	$\mathrm{rk}(E_{D_{14}}(\mathbb{Q})) \geq 1$
D_{15} = 7233889	$\mathrm{rk}(E_{D_{15}}(\mathbb{Q})) \geq 1$
D_{16} = 7862929	$\mathrm{rk}(E_{D_{16}}(\mathbb{Q})) \geq 1$
D_{17} = 10000249	$\mathrm{rk}(E_{D_{17}}(\mathbb{Q})) \geq 1$
D_{18} = 10442809	$\mathrm{rk}(E_{D_{18}}(\mathbb{Q})) \geq 1$
D_{19} = 10618969	$\mathrm{rk}(E_{D_{19}}(\mathbb{Q})) \geq 1$
$\mathrm{rk}_{K_{19}} E \geq 28$	

5.2 High ranks over quadratic fields.

Tate's method [57] for computing the rank r of an elliptic curves E by 2-descent via 2-isogeny works also for curves E defined by (1.3) over a number field $K \neq \mathbb{Q}$. We apply it here to the case when $K = \mathbb{Q}(\sqrt{D})$ is a quadratic field of class number one (see [19]). As described in section 4.2.2, the task consists in determining the image $\alpha E(K)$ of E under the homomorphism

$$\alpha : \; E(K) \longrightarrow K/K^{*2}$$

for the curve in normal form (1.3) with coefficients $c, d \in \mathcal{O}_K$. ¿From formula (*) in section 4.2.2, we obtain for the rank $r = \mathrm{rk}_K E$ the relation

$$r = \log \sharp\alpha E(K) + \log \sharp\alpha' E'(K) - 2.$$

Since

$$\{K^{*2}, d'K^{*2}\} \subseteq \alpha' E'(K)\},$$

we have

$$\sharp\alpha' E'(K) \geq \begin{Bmatrix} 1 \\ 2 \end{Bmatrix} \text{ according as } d' = c^2 - 4d \begin{Bmatrix} \in \\ \notin \end{Bmatrix} K^{*2}.$$

It follows that

$$r \geq \log \sharp\alpha E(K) - \begin{Bmatrix} 2 \\ 1 \end{Bmatrix} \text{ according as } d' \begin{Bmatrix} \in \\ \notin \end{Bmatrix} K^{*2}.$$

To compute $\alpha E(K)$, we proceed as follows.

We choose a set of integers in K

$$\mathcal{B}^* = \{d_1^*, \dots, d_t^*\} \subseteq \mathcal{O}_K$$

such that

(i) d_i^*, d_j^* are non-associates for $i \neq j$,

(ii) for every integral divisor $d^* \mid d$, there is an index i such that $d^* \cong d_i^*$ are associates.

Let $\zeta \in K$ be a generator of the group of roots of unity in K (hence $\zeta = -1$ if K is complex quadratic) and denote by ϵ a fundamental unit of K (if K is real quadratic). Then we replace $\alpha E(K)$ by the group

$$T \cdot K^{*2} \subseteq \alpha E(K)$$

for the computable set

$$\begin{aligned} T = \{1, d\} \quad \cup \quad & \{d^* \in \mathcal{O}_K \mid d^* = \zeta^{e_0}\epsilon^{e_1} d_i^*,\ d_i^* \in \mathcal{B}^*, \\ & 1 \leq i \leq t;\ e_0, e_1 \in \{0, 1\}, d = d^* d'^* \\ & \text{such that } d^* + c + d'^* \text{ is a square in } \mathcal{O}_K\}. \end{aligned}$$

Then we obtain for the rank $r = \mathrm{rk}_K E$ the lower bound

$$r \geq \log \sharp(T \cdot K^{*2}) - \left\{ \begin{matrix} 2 \\ 1 \end{matrix} \right\} \text{ according as } d' \left\{ \begin{matrix} \in \\ \notin \end{matrix} \right\} K^{*2}.$$

The algorithm for constructing curves E over K of large rank consists in three steps:

(1) Choose an integer $d \in \mathcal{O}_K$ with many prime divisors.

(2) Find an integer $c \in \mathcal{O}_K$ such that $\sharp T$ is as large as possible.

(3) Estimate the rank r below by the above formula.

In step (1), the integers $d \in \mathcal{O}_K$ are chosen in such a way that the coefficients in their basis representation in $K = \mathbb{Q}(\sqrt{D})$ are small and their prime divisors consists mainly of split primes. It turns out in step (2), that the best results are obtained by choosing $c \in \mathcal{O}_K$ such that the absolute values of the coefficients in the basis representation of c in K are of about the same size as the square roots of the absolute values of the coefficients of $d \in \mathcal{O}_K$ in the basis representation of d in K. In practice, one chooses the c's in $\mathcal{O}_K$ as numbers in a fixed residue class

$$c = c_0 + \gamma m$$

for an integer $c_0 \in \mathcal{O}_K$, $c_0 = d^* + c + \frac{d}{d^*}$, and a suitably chosen modulus $m \in \mathcal{O}_K$ with γ's varying in a finite subset $\Gamma \subseteq \mathcal{O}_K$. As a complete residue system modulo m for $m = m' + m''\omega \in \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$, one may take

$$\mathcal{R} = \{r' + r''\omega \in \mathcal{O}_K \mid 0 \leq r' < \left| \frac{N(m)}{m_1} \right|,\ 0 \leq r'' < m_1\},$$

where $N = N_{K/\mathbb{Q}}$ denotes the norm with respect to $K/\mathbb{Q}$ and

$$m_1 := \left\{ \begin{array}{cl} |m'| & \text{if } m'' = 0 \\ |m''| & \text{if } m' = 0 \\ \gcd(m', m'') & \text{if } m' \neq 0,\ m'' \neq 0 \end{array} \right\}.$$

Then one stores all solutions of the congruence

$$x^2 \equiv c_0 \mod m$$

in order to be able to detect squares in the residue class $c_0 \pmod{m}$. Since inert prime factors of the modulus m appear as squares in the norm and hence enlarge the size of the coefficient r' and hence the size of $\mathcal{R}$, they should be avoided when one chooses m. For the same reason, inert prime factors should be avoided in the choice of coefficients $d \in \mathcal{O}_K$.

Unfortunately, this procedure is not yet very efficient and thus requires a substantial refinement. So far, only curves E over K with rank ≥ 7 could be constructed. We give an example.

Example

$$K = \mathbb{Q}(\vartheta),\ \vartheta = \sqrt{-3}$$

$$E: \quad Y^2 = X^3 + cX^2 + dX$$

$$\begin{aligned} d &= 267995\vartheta + 321595 \\ &= \vartheta(-\vartheta+2)(-2\vartheta+1)(2\vartheta+1)(-\vartheta+4)(\vartheta+4), \end{aligned}$$

$$\vartheta^2 = -3,\ (-\vartheta+2)(\vartheta+2) = 7,\ (-2\vartheta+1)(2\vartheta+1) = 13$$
$$(-\vartheta+4)(\vartheta+4) = 19,\ (-3\vartheta+2)(3\vartheta+2) = 31,$$
$$(-2\vartheta+5)(2\vartheta+5) = 37$$

Table 12

values for c	$\mathrm{rk}_K E \geq$
$261\vartheta + 389$	7
$365\vartheta + 26$	7
$385\vartheta + 782$	7
$375\vartheta + 152$	7
$\frac{117}{2}\vartheta + \frac{1381}{2}$	7
$\frac{273}{2}\vartheta + \frac{433}{2}$	7
$\frac{365}{2}\vartheta + \frac{253}{2}$	7
$\frac{105}{2}\vartheta + \frac{1321}{2}$	7
$\frac{857}{2}\vartheta + \frac{1609}{2}$	7
$\frac{185}{2}\vartheta + \frac{1033}{2}$	7
$\frac{267}{2}\vartheta + \frac{1641}{2}$	7
$721\vartheta + 173$	
$-285\vartheta + 338$	6
$\frac{655}{2}\vartheta + \frac{13}{2}$	6
$\frac{19}{2}\vartheta + \frac{1081}{2}$	6

5.3 2-rank of cubic number fields.

Let $K = \mathbb{Q}(\theta)$ be a non-Galois cubic number field generated by a root θ of an irreducible polynomial over $\mathbb{Z}$

$$f(X) = X^3 + aX + b \quad (a, b \in \mathbb{Z})$$

and consider the associated elliptic curve of Weierstrass form (1.1)

$$E: \quad Y^2 = f(X).$$

Suppose that the normalized p-values of a, b are

$$v_p(a) < 2 \text{ or } v_p(b) < 3 \text{ for all rational primes } p \neq 2, 3,\ p \in \mathbb{P},$$

so that E over $\mathbb{Q}$ has good reduction at all primes $p \neq 2, 3$.

U. Schneiders [49], [50] related the 2-rank of the class group of K to the order of the 2-Selmer group of E over $\mathbb{Q}$ and used this relation to construct non-Galois cubic number fields K of high 2-ranks. Her method is a generalization of an approach taken by Frey et al. ([8], [10]) in the special case of Mordell's elliptic curves

$$E_{\pm k^2}: \quad Y^2 = f(X) = X^3 \pm k^2.$$

One starts off with a modified exact sequence, similar to the one used in section 4.2.2, but built with respect to a finite set V of places of a number field L.

At first we take an arbitrary elliptic curve E given in short Weierstrass form (1.1) over a number field L (more precisely, over its ring of integers $\mathcal{O}_L$) and choose a positive integer $n \geq 2$. Then we have the following commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & E(L)/nE(L) \arrow[r, "\partial"] \arrow[d, equal] & S_V^{(n)}(G, E/L) \arrow[r, "\kappa"] \arrow[d] & Ш_V(E/L)[n] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(L)/nE(L) \arrow[r, "\partial"] \arrow[d, "\alpha_{\mathfrak{p}}"] & H^1(G, E(\overline{L})[n]) \arrow[r, "\kappa"] \arrow[d, "\beta_{\mathfrak{p}}"] & H^1(G, E(\overline{L}))[n] \arrow[r] \arrow[d, "\gamma_{\mathfrak{p}}"] & 0 \\
0 \arrow[r] & E(L_{\mathfrak{p}})/nE(L_{\mathfrak{p}}) \arrow[r, "\partial_{\mathfrak{p}}"] & H^1(G_{\mathfrak{p}}, E(\overline{L}_{\mathfrak{p}})[n]) \arrow[r, "\kappa_{\mathfrak{p}}"] & H^1(G_{\mathfrak{p}}, E(\overline{L}_{\mathfrak{p}}))[n] \arrow[r] & 0
\end{tikzcd}$$

where $G = \mathrm{Gal}(\overline{L}/L)$ resp. $G_{\mathfrak{p}} = \mathrm{Gal}(\overline{L}_{\mathfrak{p}}/L_{\mathfrak{p}})$ is the absolute Galois group of L resp. $L_{\mathfrak{p}}$, the field $L_{\mathfrak{p}}$ denoting the completion of L at a place $\mathfrak{p}$ of L and $\overline{L}$ resp. $\overline{L}_{\mathfrak{p}}$ the corresponding algebraic closure. Here the n-Selmer group is

$$S_V^{(n)}(G, E/L) = \bigcap_{\mathfrak{p} \notin V} \ker(\gamma_{\mathfrak{p}} \circ \kappa)$$

and the n-Tate-Shafarevich group

$$Ш_V(G, E/L)[n] = \bigcap_{\mathfrak{p} \notin V} \ker(\gamma_{\mathfrak{p}}).$$

This diagram is applied in the special case of

$$L = \mathbb{Q} \text{ and } n = 2.$$

Referring to an explicit decomposition law in the cubic field K and its normal closure N and employing the theorem of Tate-Bašmakov, U. Schneiders [49], [50] derives the following upper and lower bound for the 2-rank r_2 of the class group of K. She first defines certain sets of primes of $\mathbb{Q}$ depending on the decomposition law in N, viz.

$$T := \{\infty, 2\} \cup \{p \in \mathbb{P} \mid p | \Delta_0\}$$

and

$$\begin{array}{rcl} V & := & T \setminus \{p \in \mathbb{P} \setminus \{2,3\} \mid 2 = v_p(b) \leq v_p(a) \text{ or } (3 \leq v_p(a) \text{ and } v_p(b) = 4)\} \\ & & \cup \{3 \mid 3 \in T \text{ and } E \text{ has good reduction at } 3\} \end{array}$$

Furthermore,

$$\begin{array}{rcl} \tilde{V} & := & \{p \in V \cap \mathbb{P} \mid p = \left\{ \begin{array}{c} \mathfrak{P}_1 \, \mathfrak{P}_2 \, \mathfrak{P}_3 \\ \mathfrak{P}_1^2 \, \mathfrak{P}_2^2 \, \mathfrak{P}_3^2 \end{array} \right\} \text{ in } N\}, \\ V_2 & := & \{p \in V \cap \mathbb{P} \mid \left\{ \begin{array}{rcl} p & = & 2 = \left\{ \begin{array}{c} \mathfrak{P}_1 \mathfrak{P}_2 \\ \mathfrak{P}^3 \end{array} \right\} \text{ or} \\ p & = & \mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3 \mathfrak{P}_4 \mathfrak{P}_5 \mathfrak{P}_6 \end{array} \right\} \text{ in } N\}, \\ & & \cup \{\infty \mid m > 0\}, \end{array}$$

where $k := \mathbb{Q}(\sqrt{m}) \leq N$ is the unique quadratic subfield of N, and

$$V_1 := \tilde{V} \cup V_2.$$

Now she introduces the following subgroups of the Selmer group $S^{(2)}_{\tilde{V}}(G, E/\mathbb{Q})$:

$$S_i := \{\xi \in S^{(2)}_{\tilde{V}}(G, E/\mathbb{Q}) \mid \beta_p(\xi) = 0 \text{ for } p \in V_i\} \quad (i = 1, 2).$$

Then, U. Schneiders ([49], [50]) proves

Theorem 5.1. *The 2-rank r_2 of the class group of the non-Galois cubic number field $K = \mathbb{Q}(\theta)$ satisfies the inequalities*

$$\sharp S_1 \leq 2^{r_2} \leq \sharp S_2.$$

The lower bound $\sharp S_1$ can be computed by general 2-descent according to Birch and Swinnerton-Dyer [2] and Cremona and Serf (see [5], [6]). The procedure is described in detail in [52]. It appears to be a problem to calculate $\sharp S_2$, since the 2-coverings used in the calculation of $\sharp S_2$ are represented by quartics only if they admit a rational point everywhere locally, whereas for the Selmer group S_2, this condition is satisfied only up to the finite set of places V_2. However, a lower bound for 2^{r_2} can be found in this way. We list here two examples, one when K contains a real quadratic subfield $k = \mathbb{Q}(\sqrt{m})$ and one when K contains a complex quadratic subfield $k = \mathbb{Q}(\sqrt{m})$. The 2-rank of K is then $r_2 \geq 7$. We mention that E. Schaefer [45] was able to construct cubic number fields with $r_2 \geq 13$ by means of similar cohomological method involving abelian varieties.

Table 13

$$Y^2 = X^3 + aX + b$$

a	$=$	-1364272			
b	$=$	1381701520			
Δ	$=$	-41388735394003774208			
m	$=$	$-161674747632827243 \quad < \quad 0$			
$\Delta(K)$	$=$	Δ			
places		in $\mathbb{Q}$	in k	in K	in N
		2	$\wp$	$\mathfrak{p}^3$	$\mathfrak{P}^3$
		161674747632827243	$\wp^2$	$\mathfrak{p}\mathfrak{q}^2$	$\mathfrak{P}_1{}^2\mathfrak{P}_2{}^2\mathfrak{P}_3{}^2$
T	$=$	$\{\infty, 2, 161674747632827243\}$			
V	$=$	T			
$\widetilde{V}$	$=$	$\{161674747632827243\}$			
V_1	$=$	$\{2, 161674747632827243\}$			
V_2	$=$	$\{2\}$			
$\#S_1$	$=$	128			
$\#S_2$	$\geq$	128			
$\mathrm{rk}(E)$	$\geq$	8			
r_2	$\geq$	7			

Table 14

a	$=$	-713479312			
b	$=$	7334399549200			
Δ	$=$	372110264148187065517312			
m	$=$	1453555719328855724677 $\quad > \quad 0$			
$\Delta(K)$	$=$	Δ			
places		in $\mathbb{Q}$	in k	in K	in N
		2	$\wp$	$\mathfrak{p}^3$	$\mathfrak{P}^3$
		1453555719328855724677	$\wp^2$	$\mathfrak{p}\mathfrak{q}^2$	$\mathfrak{P}_1{}^2\mathfrak{P}_2{}^2\mathfrak{P}_3{}^2$
T	$=$	$\{\infty, 2, 1453555719328855724677\}$			
V	$=$	T			
$\widetilde{V}$	$=$	$\{1453555719328855724677\}$			
V_1	$=$	$\{\infty, 2, 1453555719328855724677\}$			
V_2	$=$	$\{\infty, 2\}$			
$\#S_1$	$=$	128			
$\#S_2$	$\geq$	128			
$\mathrm{rk}(E)$	$\geq$	9			
r_2	$\geq$	7			

5.4 Elliptic curves of large order over large finite fields.

The construction of elliptic curves E with large order over large finite fields $K = \mathbb{F}_q$, where $q = 2^n$ or $q = p \in \mathbb{P}$ is a prime, is an important goal in computational number theory. There are applications to

(i) the construction of large primes (of order of magnitude up to 10^{1000}),

(ii) primality proving resp. testing by virtue of the algorithm of Goldwasser-Kilian-Atkin,

(iii) the determination of cryptographically relevant curves via discrete logarithms.

An algorithm developed by G. Lay ([32], [33]) solves the following tasks:

5.4.1 Given an integer $m > 3$, find a prime p and an elliptic curve E over $\mathbb{F}_p$ of order $\sharp E(\mathbb{F}_p) = m$.

5.4.2 Given two integers n and c_0, find an elliptic curve E over $\mathbb{F}_{2^n}$ of order $\sharp E(\mathbb{F}_{2^n}) = c \cdot q$ with a prime q and a positive integer $c \leq c_0$.

5.4.3 Given an integer $n > 1$, decide whether there is a prime $p > 3$ and an elliptic curve E over $\mathbb{F}_q$ with group of rational points of isomorphism type

$$E(\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

5.4.4 Given a prime $p > 3$ and an integer m satisfying the Hasse inequality $|p + 1 - m| < 2\sqrt{p}$, construct an elliptic curve E over $\mathbb{F}_p$ of order $\sharp E(\mathbb{F}_p) = m$ and with endomorphism ring of small class number.

The construction is carried through via class field theory. The order $m = \sharp E(\mathbb{F}_q)$ satisfies the Hasse inequality (see Theorem 2.4)

$$|m - (q + 1)| \leq 2\sqrt{q}.$$

Therefore, one starts from an imaginary quadratic field

$$K = \mathbb{Q}(\sqrt{D}) \text{ with } D = (m - (q+1))^2 - 4q$$

and considers an order

$$\mathcal{O} \subseteq \mathcal{O}_K \subseteq K$$

in the maximal order $\mathcal{O}_K$ of K of discriminant δ and conductor

$$\mathfrak{f} = [\mathcal{O}_K : \mathcal{O}].$$

We have the following result (see [33]).

Theorem 5.2. *Let $p \in \mathbb{P}$ be a prime of $\mathbb{Q}$ which splits in K and denote by $\mathfrak{P}$ over p a prime of the ring class field $L_{\mathcal{O}}$ associated with the order $\mathcal{O}$. Suppose that p is chosen in such a way that the prime $\mathfrak{P}$ of degree f does not divide the conductor $\mathfrak{f}$:*

$$\mathfrak{P} \not| \mathfrak{f}.$$

Let $\mathcal{E}$ be an elliptic curve defined over $L_{\mathcal{O}}$ and having complex multiplication by $\mathcal{O}$ and good ordinary reduction modulo $\mathfrak{P}$. Designate by E the reduced curve $\mathcal{E} \pmod{\mathfrak{P}}$. Then there exists an element $\pi \in \mathcal{O} \setminus p\mathcal{O}$ satisfying the norm equations

$$\begin{array}{rcl} q & = & N_{K/\mathbb{Q}}(\pi), \\ m & = & N_{K/\mathbb{Q}}(1-\pi), \end{array}$$

and the endomorphism ring of E is

$$\mathrm{End}(E) = \mathrm{End}(\mathcal{E}) = \mathcal{O}.$$

Conversely, every elliptic curve E over $\mathbb{F}_q$ with endomorphism ring $\mathcal{O}$ arises in this way.

To build the curve $\mathcal{E}$ and its field of definition $L_{\mathcal{O}}$, one considers the one-to-one correspondence

$$[\mathfrak{a}] \longleftrightarrow [Q]$$

between classes $[\mathfrak{a}]$ of ideals $\mathfrak{a}$ of $\mathcal{O}$ and classes $[Q]$ of positive definite quadratic forms

$$Q(X,Y) = AX^2 + BXY + CY^2 \quad (A, B, C \in \mathbb{Z})$$

of discriminant

$$\delta = B^2 - 4AC.$$

Then the ideal is the $\mathbb{Z}$-module

$$\mathfrak{a} = [1, \tau_Q]$$

for the unique root (in the complex upper half plane)

$$\tau_Q = \frac{-B + \sqrt{\delta}}{2A}$$

of the equation

$$Q(\tau, 1) = 0.$$

The ring class field $L_{\mathcal{O}}$ of the complex quadratic field $K = \mathbb{Q}(\sqrt{\delta})$ is generated over K by the value $j(\tau_Q)$ of the modular invariant j at τ_Q:

$$L_{\mathcal{O}} = K(j(\tau_Q)).$$

The elliptic curve is given by the lattice

$$L = [1, \tau_Q] \subseteq \mathbb{C}$$

via

$$\mathcal{E}(\mathbb{C}) \cong \mathbb{C}/L.$$

The minimal polynomial of $j(\tau_Q)$ is

$$W_\delta[j](X) = \prod_{[Q]} (X - j(\tau_Q)) \in \mathbb{Z}[X]$$

of degree $h_\mathcal{O}$, the class number of $\mathcal{O}$. This *class equation* of $\mathcal{O}$ has very large coefficients. Therefore, following Yui-Zagier, it is replaced by the minimal polynomial $W_\delta[u](X)$ of a suitable *class invariant* $u \in \mathcal{O}_K$ such that $W_\delta[u]$ has small coefficients. There is a function ψ_u which transforms a zero of $W_\delta[u](X)$ into a zero of $W_\delta[j](X)$ (see [32], [33]). Hence we have

$$L_\mathcal{O} \cong K[X]/(W_\delta[u](X))$$

for the ring class field $L_\mathcal{O}$ of $\mathcal{O}$.

Example. $K = \mathbb{Q}(\sqrt{-47})$, $\mathcal{O} = \mathcal{O}_K$, $\delta = -47$,

$$L_\mathcal{O} = K(\rho),$$

$\rho \in \mathbb{C}$ a root of the modified class equation

$$W_\delta[u](X) = X^5 + 2X^4 + 2X^3 + X^2 - 1$$

for the class invariant

$$u = (-1)^{\frac{\delta - 1}{8}} \zeta_{48} f_2$$

with Weber's function f_2 and a primitive 48-th root of unity ζ_{48}. The original class equation is

$$\begin{aligned} W_\delta[j](X) \quad = \quad & X^5 + 2257834125X^4 + 9987963828125X^3 + 5115161850595703125X^2 \\ & -14982472850828613281250X + 16042929600623870849609375. \end{aligned}$$

We remark that in this construction, the curve $\mathcal{E}$ and the ring class field $L_\mathcal{O}$ need not be determined. Furthermore, we shall restrict to the maximal order $\mathcal{O} = \mathcal{O}_K$ of the complex quadratic field K.

In characteristic $p \neq 2$, the algorithm is described in [32], [33]. In characteristic 2, the algorithm for constructing elliptic curves E over $\mathbb{F}_{2^n}$ of given order consists in the following basic steps.

The algorithm

(1) Choose a finite field $\mathbb{F}_{2^n}$ and a complex quadratic field $K = \mathbb{Q}(\sqrt{D})$.

(2) Solve the norm equation

$$2^n = N_{K/\mathbb{Q}}(\pi)$$

for a number $\pi \in \mathcal{O}_K \setminus 2\mathcal{O}_K$.

(3) Compute the group order $m = \sharp E(\mathbb{F}_{2^n})$ via

$$m = N_{K/\mathbb{Q}}(\pi \pm 1).$$

(4) Compute resp. approximate the class equation $W_D(X)$ of degree h_K = class number of K.

(5) Factorize W_D modulo 2. The polynomial W_D splits modulo 2 into irreducible factors of degree d, where d is the smallest positive integer such that the norm equation

$$2^d = N_{K/\mathbb{Q}}(\pi')$$

admits a solution $\pi' \in \mathcal{O}_K \setminus 2\mathcal{O}_K$.

(6) Determine the j-invariant of E by calculating a root ρ of W_D. This root generates the finite field

$$\mathbb{F}_{2^d} = \mathbb{F}_2(\rho).$$

$\mathbb{F}_{2^d}$ is the smallest field of definition for E. The j-invariant of E is a rational function of ρ:

$$j = \psi_D(\rho).$$

(7) Find a defining equation for E over $\mathbb{F}_{2^d}$ from the j-invariant.

An Example

We set $h_K = n = 700$, find $D = -1529959$ and compute

$$\begin{aligned} m = \sharp E(F_{2^n}) &= 52601359015483735072409898828801286655503398028231738594982 8\\ &\ 0903068732154297080822113666536277588451226984016959881025 96\\ &\ 4465532518036037974393064468707657248661287243598611378322 78\\ &\ 918600453332403861957792543282 2\\ &= 2 * q_{211} \end{aligned}$$

with a 211-digit prime cofactor q_{211} of m. The generating polynomial for F_{2^n} is

$$\begin{aligned} f = \ &1111010010100101100101111000101110111001011010010100101111 0\\ &0010011101010111110001111000110011100101101101100000000110 10\\ &1010101010110011110101110000000110101101010011000010011011 1\\ &0000100010100001111100001110111001111000010110010010001000 1\\ &0110100000000001000101000101011101000100111011100000111011 11\\ &1001101100101011110110011011101110110101010110111000000111 0\\ &1001100011001000001110110000000101100111001011101011001001 01\\ &1011011010001000000010101000100100011001111011111101101111 1\\ &1101011111100100100101001100110010000001000010110110111011 01\\ &1111000101010110001001110110001101010100000110011001100111 0\\ &1011001011010001111101101011111000111011100001110100110110 1\\ &01001101011000010100001011000010011000110101111101001 \end{aligned}$$

The elliptic curve is

$$E: \quad y^2 + xy = x^3 + a_2x^2 + a_6$$

with

$$\begin{aligned}
a_2 &= 10\\
a_6 &= 11110101100010011000111110001111111000100000110001101011100\\
& 00010011000111110001001000000110010101011011111001100110111\\
& 00011111101011011101100100101100101111111000001011011100101\\
& 00011100011001001000111101010011111010011010011001010100100\\
& 10001110111011110101111011111001110010010001111101101001010\\
& 00100000110001110111110011001100100100000000011010110000111011\\
& 11111010010101001101111001110110100110000011000101000011001\\
& 11000110010110011101010100010010111100011010000010100111101\\
& 10011111001101001000010000110011110110110001010111100111000\\
& 01100010000001001011010000001001011001000110010010100100111111\\
& 01001001011010010010000001110111101010100000011011101000000\\
& 0110010000101011001001101110001110000001110000001
\end{aligned}$$

The group $E(F_{2^n})$ is cyclic, generated by the point $P = (x_P, y_p)$ with coordinates

$$\begin{aligned}
x_P &= 11010110000001000101101011001111100101011010100001111100010\\
& 10000011111001100101011001001101001101111111100000000101110011\\
& 00101010101000111010100110111101100100000110100100001100101\\
& 11010111010000111000100000100001110111100011011111111011001\\
& 10000010101111011001100001110011000010110101001010000110001\\
& 10011111001001010011111100111010100101011000111010011010011\\
& 11000111000011000011000100100110110100100110100100111001010\\
& 10100101001001110001000000100111111110011101100111001011100 0\\
& 01000110001001001111100100010011111111111011011000101110001\\
& 10000100110000100000100000000000100110101010000001001100010 00\\
& 10001011010101011101010001011000011010001011011011101001110\\
& 11000110000000110101000011110001110101101010 1110101
\end{aligned}$$

and

$$\begin{aligned}
y_P &= 10011100000110110010000000111111100011000001110001111101110010\\
& 00000011000010000101010101011001100010000101001110100100001\\
& 01101100100100111100111101010001110000011001100100011000111\\
& 11010011111010111000001101111110000000111110010101101001110 01\\
& 00101000000001010101111010110001000011110110010011111100101 1\\
& 00110100000011010001000000110000101101011101000000110100010110\\
& 00000111101111001010000111101011111010001001101110001101101\\
& 10100000011010010000101011010111000110101001101110101001000\\
& 11111111111100011001111000100101101100011111001001001111111\\
& 01010100100111000011010010001010111010001011111010110010111\\
& 00100011010101001000101011001111010001010111001100000111100\\
& 100011101111011000100000111010101101110000100011 1001
\end{aligned}$$

References

[1] Chr. Abel-Hollinger, H.G. Zimmer, Torsion groups of elliptic curves with integral j-invariant over multiquadratic fields. In: “Number Theoretic and Algebraic Methods in Computer Science”, ed. by A.v.d. Poorten, I. Shparlinski and Horst G. Zimmer. Proc. of the Conference in Moscow 1993, World Scientific, Singapore 1995, 69-87.

[2] B.J. Birch, H.P.F. Swinnerton-Dyer, Notes on elliptic curves I. J. reine angew. Math. **212** (1963), 7-25.

[3] J.W.S. Cassels, An introduction to the geometry of numbers. Grundl. d. math. Wiss. **99**, Springer-Verlag, Berlin 1959.

[4] J.S. Chahal, A Note on the Rank of Quadratic Twists of an Elliptic Curve. Math. Nachr. **161** (1993), 55-58.

[5] J.E. Cremona, Algorithms for Modular Elliptic Curves. Cambridge Univ. Press, Cambridge 1992.

[6] J.E. Cremona, P. Serf, Computing the rank of elliptic curves over real quadratic number fields of class number 1. To appear.

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

[8] H. Eisenbeis, G. Frey, B. Ommerborn, Computation of the 2-rank of pure cubic fields. Math. Comp. **32** (1978), 559-569.

[9] S. Fermigier, Construction of High-Rank Elliptic Curves over $\mathbb{Q}$ and $\mathbb{Q}(t)$. In: "Algorithmic Number Theory". ANTS-II Proc., ed. by H. Cohen, Lect. Notes in Comp. Sci. **1122**, Springer-Verlag, Berlin 1996, 115-120.

[10] G. Frey, Die Klassengruppen quadratischer und kubischer Zahlkörper und die Selmergruppen gewisser elliptischer Kurven. Manuscr. math. **16** (1975), 333-362

[11] G. Frey, M. Jarden, Approximation theory and the rank of abelian varieties over large algebraic fields. Proc. London Math. Soc. (3) **28** (1974), 112-128.

[12] G.-W. Fung, H. Ströher, H.C. Williams, H.G. Zimmer, Torsion groups of elliptic curves with integral j-invariant over pure cubic fields. J. Number Theory **36** (1990), 12-45.

[13] 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.

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

[15] J. Gebel, A. Pethö, H.G. Zimmer, Computing integral points on Mordell's elliptic curves. To appear in Proc. Journ. Arith. Barcelona 1995, Collect. Mat.

[16] J. Gebel, A. Pethö, H.G. Zimmer, Computing S-integral points on elliptic curves. In: "Algorithmic Number Theory", ed. by H. Cohen. ANTS-2 Proceedings, Bordeaux 1996. Lect. Notes in Comp. Sci. **1122** (1996), 157-171, Springer-Verlag.

[17] J. Gebel, A. Pethö, H.G. Zimmer, On Mordell's Equation. To appear in Compos. Math.

[18] J. Gebel; H.G. Zimmer, Computing the Mordell-Weil Group of an Elliptic Curve over $\mathbb{Q}$. In: "Elliptic Curves and Related Topics", ed. by H. Kisilevsky and M. Ram Murty. CRM Proc. and Lect. Notes, vol. **4**, 61-83. Amer. Math. Soc., Providence, R.I. 1994.

[19] H. Graf, Konstruktion elliptischer Kurven hohen Ranges über quadratischen Zahlkörpern der Klassenzahl eins. Diploma Thesis, Saarbrücken 1995.

[20] L. Hajdu, T. Herendi, Explicit bounds for the solutions of elliptic equations. Manuscript, Debrecen 1996.

[21] 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.

[22] H. Hasse, Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F.K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl. I, **42** (1933), 253-262.

[23] S. Kamienny, Torsion points on elliptic curves. Bull. Amer. Math. Soc. (New Ser.) **23** (1990), 371-373.

[24] S. Kamienny, Torsion points on elliptic curves and q-coefficients of modular forms. Invent. math. **109** (1992), 221-229.

[25] S. Kamienny, Torsion points on elliptic curves over fields of higher degree. Duke Math. J., I.M.R.N. no. **6** (1992), 129-133.

[26] M.A. Kenku, F. Momose, Torsion points on elliptic curves defined over quadratic fields. Nagoya Math. J. **109** (1988), 125-149.

[27] M. Kida, On the Rank of an Elliptic Curve in Elementary 2-Extensions. Proc. Japan Acad. **69**, Ser. A., No. 10 (1993), 422-425.

[28] T. Kishi, On torsion groups of elliptic curves with integral j-invariant over imaginary cyclic biquadratic fields. Preprint, Tokyo Metropolitan University 1995.

[29] T.J. Kretschmer, Construction of elliptic curves with large rank. Math. Comp. **174** (1986), 627-635.

[30] S. Lang, Elliptic Curves: Diophantine Analysis. Grundl. d. math. Wiss. **231**, Springer-Verlag, Heidelberg 1978.

[31] S. Lang, Conjectured Diophantine Estimates on Elliptic Curves. Progr. in Math. **35**, 155-171. Birkhäuser, Basel 1983.

[32] G.-J. Lay, Konstruktion elliptischer Kurven mit vorgegebener Ordnung über endlichen Primkörpern. Diploma Thesis, Saarbrücken 1994.

[33] G.-J. Lay, H.G. Zimmer, Constructing elliptic curves with given group order over large finite fields. In: "Algorithmic Number Theory", Eds. L.M. Adleman, M.-D. Huang. Proc. ANTS-I, Ithaca, NY, USA, 1994. Lect. Notes in Comp. Sci. **877** (1994), 250-263, Springer-Verlag.

[34] Yu.I. Manin, Cyclotomic fields and modular curves. Russian Math. Surveys **26** (1971), 7-78.

[35] B. Mazur, Rational points on modular curves. In: "Mod. Functions of One Var. V". Lect. Notes in Math. **601** (1977), 107-148, Springer-Verlag, Berlin.

[36] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. math. **124** (1996), 437-449.

[37] H.H. Müller, H. Ströher, H.G. Zimmer, Torsion groups of elliptic curves with integral j-invariant over quadratic fields. J. reine angew. Math. **397** (1989), 100-161.

[38] H.H. Müller, H. Ströher, H.G. Zimmer, Complete determination of all torsion groups of elliptic curves with integral absolute invariant over quadratic and pure cubic fields. In: "Number theory", ed. by J.-M. de Koninck and C. Levesque, 671-698, W. de Gruyter Verlag, Berlin 1989.

[39] K. Nagao, An Example of an Elliptic Curve over $\mathbb{Q}(T)$ with rank ≥ 13. Proc. Japan Acad. **70**, Ser. A, No. **5** (1994), 152-153.

[40] K. Nagao, T. Kouya, An Example of an Elliptic Curve over $\mathbb{Q}$ with Rank ≥ 21. Proc. Japan Acad. **70**, Ser. A, No. 4 (1994), 104-105.

[41] A. Nitaj, La conjecture abc. Preprint, Saarbrücken 1996.

[42] A. Pethö, Th. Weis, H.G. Zimmer, Torsion group of elliptic curves with integral j-invariant over general cubic number fields. To appear in Intern. J. Alg. and Comp.

[43] J. Quer, Sobra el 3-rang del cossos quadraàtics i la corba ell-iptica $Y^2 = X^3 + M$. PhD Thesis, Barcelona 1987.

[44] G. Rémond, F. Urfels, Approximation diophantienne de logarithmes elliptiques p-adiques. J. Number Theory **57** (1996), 133-169.

[45] E.F. Schaefer, Class Groups and Selmer Groups. J. Number Theory **56** (1996), 79-114.

[46] S. Schmitt, Berechnung der Mordell-Weil Gruppe parametrisierter elliptischer Kurven. Diploma Thesis, Saarbrücken 1995.

[47] S. Schmitt, Computing the Selmer group of certain parametrized elliptic curves. Acta Arith. **78** (1997), 241-254.

[48] U. Schneiders; H.G. Zimmer, The rank of elliptic curves upon quadratic extension. In: "Computational Number theorey". Proc. Colloq. at Kossuth Lajos Univ., Debrecen 1989, 239-260, W. de Gruyter, Berlin 1991.

[49] U. Schneiders, Eine Abschätzung der 2-Klassenzahl von Nicht-Galoisschen kubischen Zahlkörpern durch die Selmergruppe der zugehörigen elliptischen Kurven. PhD Thesis, Saarbrücken 1995.

[50] U. Schneiders, Estimating the 2-rank of cubic fields by Selmer groups of elliptic curves. J. Number Theory **62** (1997), 375-396.

[51] M. Sens, Rangsprünge elliptischer Kurven mit nicht-trivialem 2-Teilungspunkt beim Übergang vom rationalen Zahlkörper $\mathbb{Q}$ zu multiquadratischen Erweiterungen. Diploma Thesis, Saarbrücken 1994.

[52] P. Serf, The rank of elliptic curves over real quadratic number fields of class number 1. PhD Thesis, Saarbrücken 1995.

[53] J.P. Serre, Lectures on the Mordell-Weil theorem. Vieweg Verlag, Braunschweig 1989.

[54] S. Siksek, Infinite descent on elliptic curves. Rocky Mountain J. Math. **25** (1995), 1501-1538.

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

[56] J.H. Silverman, A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves. J. reine angew. Math. **378** (1987), 60-100.

[57] J.H. Silverman, J.T. Tate, Rational points on elliptic curves. Springer-Verlag, Heidelberg 1992.

[58] SIMATH Manual, Saarbrücken 1996.

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

[60] J. Stein, Die Torsionsgruppe elliptischer Kurven mit ganzer j-Invariante über totalreellen biquadratischen Zahlkörpern. Diploma Thesis, Saarbrücken 1994.

[61] R.J. Stroeker, J. Top, On the equation $Y^2 = (X + p)(X^2 + p^2)$. Rocky Mountain J. Math. **27** (1994), 1135-1161.

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

[63] B.M.M. de Weger, Algorithms for diophantine equations. PhD Thesis, Amsterdam 1987.

[64] K. Wildanger, Computing all integral points of Mordell's equation $y^2 = x^3 + k$ by solving cubic index form equations. To appear.

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

[66] H.G. Zimmer, A limit formula for the canonical height of an elliptic curve and its application to height computations. In: "Number Theory", ed. by R. Mollin. Proc. First Conf. Canad. Numb. Th. Assoc. at Banff, 1988, 641-659, W. de Gruyter, Berlin 1990.

[67] H.G. Zimmer, Torsion groups of elliptic curves over cubic and certain biquadratic number fields. Contemp. Math. **174** (1994), 203-220.

[68] H.G. Zimmer, An elemenatry proof of the Riemann hypothesis for an elliptic curve over a finite field. Pacific J. Math. **36** (1971), 267-278.