SIMATH - a Computer Algebra System for Number Theoretic Applications

Horst G. Zimmer

Fachbereich 9 Mathematik
Universität des Saarlandes
D-66041 Saarbrücken, Germany
zimmer@math.uni-sb.de
http://emmy.math.uni-sb.de

(Survey Paper)

1 Introduction

The aim of this paper is to give a survey of the wide range of number theoretic applications of the computer algebra system SIMATH [42].[1] This system, focusing on algebraic number theory, enables the user to attack a broad spectrum of number theoretic problems. Special attention is paid to the arithmetic of elliptic curves and its applications in cryptography.

SIMATH is developed by the research group of the author at the Universität des Saarlandes in Saarbrücken. It is written in the programming language C and will be soon extended to the programming language C++. A list system serves as a foundation for all SIMATH types such as integers, rationals, polynomials, algebraic numbers, algebraic functions, matrices and vectors. In addition to the libraries which contain all SIMATH functions, the system is equipped with a calculator called simcalc. In simcalc almost all SIMATH functions are available and can be handled in an interactive mode.

SIMATH is running on 32 bit Unix systems. An interface enables the user to apply other computer algebra systems such as MAPLE, KANT, LiDIA or PARI while working with SIMATH. This is accomplished by using a simple script language to extract numerical data from text files. A comparison of the performance of SIMATH with that of the other systems mentioned is not possible, since most of the algorithms under consideration in this survey are missing in the other systems.

Symbolic computation is one of the main ingredients of the system. The technical details are contained in the SIMATH manual (the manual can be obtained via ftp from ftp.math.uni-sb.de, the system itself from http://emmy.math.uni-sb.de). We confine ourselves here to giving a mathematical table of contents. The most remarkable success of applying the computer algebra system SIMATH to number theory is the solution in integers of the famous diophantine equation of Mordell

$$y^2 = x^3 + k$$

for integers $k \neq 0$ in the range

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

Until recently, it was only possible to solve this equation for k in the order of magnitude of 100 and in some cases up to 1,000. This achievement distinguishes SIMATH from other computer algebra systems. The contributions to the system are made by the various members of the research group of the author at Saarbrücken.

2 Number theoretic applications

The main applications of SIMATH concern

2.1 Algebraic, in particular abelian, number fields

We have developed or are going to develop algorithms for computing

2.1.1 an integral basis and the decomposition law of primes in arbitrary number fields,

2.1.2 unit groups in abelian, especially cyclotomic, number fields,

2.1.3 class numbers of abelian number fields,

2.1.4 Stickelberger ideals in cyclotomic number fields.

[1] SIMATH was supported in part by the DFG within the research program "Algorithmic Number Theory and Algebra". However, the referees of the DFG eventually suggested that we discontinue the development of SIMATH and instead incorporate some of our algorithms in other systems. We hope that this survey, together with [48], illustrates why we prefer to ignore this suggestion.

2.2 Congruence function fields of one variable

The algorithms developed and implemented in SIMATH are designed for computing resp. considering

2.2.1 an integral basis and the decomposition law of places in general congruence function fields,

2.2.2 the regulator and the unit group in hyperelliptic congruence function fields,

2.2.3 the divisor class group and the ideal class group in hyperelliptic congruence function fields,

2.2.4 invariants which are important for cryptographic applications,

2.2.5 cryptographic applications, especially key exchange protocols.

2.3 Elliptic curves over algebraic number fields

We have developed and implemented in SIMATH fundamental algorithms for computing resp. constructing

2.3.1 the torsion group,

2.3.2 the rank and a basis of the Mordell-Weil group,

2.3.3 elliptic curves of high rank over certain number fields,

2.3.4 all integral or, more generally, all S-integral points in the Mordell-Weil group,

2.3.5 the 2-rank of cubic number fields by virtue of Selmer groups.

2.4 Elliptic curves over finite fields

Our aim is to construct

2.4.1 elliptic curves of large order over large finite fields of characteristic $p \neq 2$ or $p = 2$,

2.4.2 elliptic curves over large finite fields which are of cryptographic relevance,

and to develop efficient procedures for

2.4.3 counting points on elliptic curves.

2.5 Modular curves

The task consists in constructing small models for certain modular curves and to apply these models, e.g. to the problem of

2.5.1 counting points on elliptic curves over finite fields (cf. 2.4.3).

3 Number fields

3.1 Integral basis

A fundamental problem in algebraic number theory is the determination of an integral basis. R. Böffgen [1] developed and implemented the Ford-Zassenhaus algorithm ORDMAX-IV for computing the maximal order in a polynomial algebra. It is based on local methods involving the concept of the p-radical. The algorithm provides at the same time also a tool for determining the decomposition of rational primes p in an algebraic number field K (see [2]).

Let now K be an abelian number field. Two fundamental problems consist in computing the unit group and the class number of K.

3.2 Unit group

Let us consider the special case of the n-th cyclotomic field

$$K_n = \mathbb{Q}(\zeta_n),$$

where ζ_n denotes a primitive n-th root of unity. One defines the group of *circular units* in K_n by

$$C^{(n)} := \langle \{\pm\zeta_n^a, 1-\zeta_n^a \mid a \in \mathbb{Z}\} \rangle \cap \mathbb{Z}[\zeta_n]^*.$$

Theoretically, a basis of $C^{(n)}$ was given by Gold-Kim [14] and Kučera [17]. M. Conrad [3] constructed an explicit basis of $C^{(n)}$ in the special case, where n is the product of at most three primes:

$$n = p^\lambda q^\mu r^\nu \quad (p,q,r \in \mathbb{P},\ \lambda,\mu,\nu \in \{0,1\}).$$

This construction facilitates the explicit computation of a basis of $C^{(n)}$. Such a basis, consists of $\frac{1}{2}\varphi(n) - 1$ elements, where φ denotes Euler's totient function.

Example (see [3]). $n = 2^2 \cdot 3 \cdot 5$, such that $\frac{1}{2}\varphi(n) - 1 = 7$. A basis of $C^{(n)}$ consists of the 7 elements

$$1-\zeta_4^{-1}\zeta_5^2,\ 1-\zeta_4^{-1}\zeta_5,\ 1-\zeta_4\zeta_3^{-1}\zeta_5^2,\ 1-\zeta_4\zeta_3^{-1},$$
$$1-\zeta_3\zeta_5^{-1},\ 1-\zeta_3\zeta_5^{-2},\ (1-\zeta_5^2)(1-\zeta_5)^{-1}.$$

At present M. Conrad is working on a general module theory which can be applied to the calculation of unit groups and Stickelberger ideals. Regarding the unit group, what one does is to compute a basis of a suitable subgroup of $C^{(n)}$ and to estimate the index of that subgroup in the full unit group of K_n.

3.3 Class number

Let $K_n^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq K_n = \mathbb{Q}(\zeta_n)$ be the maximal real subfield of the n-th cyclotomic field K_n, and denote by h_n^+ resp. h_n the class number of K_n^+ resp. K_n, and by

$$h_n^- = \frac{h_n}{h_n^+}$$

the relative class number of K_n.

In the special case of an odd prime power

$$n = l^\lambda \quad (l \in \mathbb{P},\ l \neq 2,\ \lambda \in \mathbb{N}),$$

W. Schwarz [35] used the Demjanenko matrix to characterize the

$$\text{2-divisibility of } h_n^+ \text{ and } h_n^-.$$

J. Sands and W. Schwarz [25] were then able to generalize the concept of Demjanenko matrix to obtain a characterization of the 2-divisibility of h^+ and h^- for an imaginary abelian number field K of odd prime power conductor $n = l^\lambda$. This characterization also leads to a new upper bound for h^-. The p-divisibility of the class number h of K is investigated in [39]

It is interesting to observe that the Demjanenko matrix originally arose in connection with torsion groups of elliptic curves (see [7]).

W. Schwarz [38] furthermore derived a relation between the Stickelberger ideal and the signature of circular units.

All these theoretical findings have a computational impact on the following tasks.

3.3.1 The computation of the relative class number h^- for imaginary abelian number fields K of odd prime power conductor $n = l^\lambda$ and the computation of $h^- \pmod p$ for primes $p \neq l$.

3.3.2 The programming of a necessary condition for the divisibility relation $p|h^+$ of the plus class number h^+ by a prime $p \neq 2$ in the case of an imaginary abelian number field K of odd prime power conductor $n = l^\lambda$ or, more generally, in the case of an imaginary abelian number field K in which p does not ramify. This latter case is a generalization of work of Jacubec [16].

3.3.3 The programming of the decision whether or not the divisibility relation

$$2|h^+$$

is satisfied for imaginary abelian fields K of odd degree $[K : \mathbb{Q}]$.

3.3.4 The attempt to *compute* the plus class number h^+ of certain abelian number fields K. This is also important in view of the non-existence of integral solutions of Catalan's equation

$$x^p - y^q = 1.$$

W. Schwarz [36] simplified a criterion of Mignotte [21] by showing that Catalan's equation has no non-trivial integral solution if

$$q \nmid h^-(K_p) \text{ and } p^{q-1} \not\equiv 1 \mod q^2.$$

The simplification consists in the replacement of the condition $q \nmid h(K_p)$ by $q \nmid h^-(K_p)$ for the p-th cyclotomic field $K_p = \mathbb{Q}(\zeta_p)$. In this way, the non-solvability of Catalan's equation could be shown for a much larger range than before, namely for $\min(p, q) \approx 10,500$ rather than $\min(p, q) \approx 600$.

As an example of an interesting SIMATH-assisted computation, we mention here some numerical experiments made by W. Schwarz [37], [39]. Recall that an odd prime p is called *regular* if p does not divide the Bernoulli numbers B_ν for $\nu = 2, 4, \ldots, p-3$. Schwarz [37], [39] defines a real abelian field K to be *p-regular*, if its conductor is not divisible by p and if all its characters $\chi \neq 1$ are p-regular in a certain sense (see [37], [39]). An odd prime p is then regular if and only if the field $K_p^+ = \mathbb{Q}(\zeta_p)^+$ is p-regular.

Now let us fix an odd prime p and a positive integer n and consider the subfields of $K_l^+ = \mathbb{Q}(\zeta_l)^+$ of degree n over $\mathbb{Q}$, as l ranges over all primes l satisfying the congruence relation

$$l \equiv 1 \pmod{2n}.$$

If $p \nmid n$, one expects a proportion of

$$1 - \prod_{\substack{d|n \\ d \neq 1}} (1 - p^{-f_d})^{\varphi(d)/f_d}$$

p-irregular fields, where f_d denotes the order of $p \pmod d$. W. Schwarz [37], [39] obtained the following numerical results (showing the expected proportion in the last column):

Table 1

p	n	l	irregular	exp.
3	2	$l < 5000$	999/2549 = 0.392	0.333
3	2	$5000 < l < 100000$	920/2234 = 0.412	0.333
3	5	$l < 100000$	33/2387 = 0.0138	0.0123
5	2	$l < 50000$	573/2549 = 0.225	0.200
5	2	$50000 < l < 100000$	528/2234 = 0.236	0.200
5	3	$l < 100000$	209/4784 = 0.0437	0.040
7	2	$l < 100000$	773/4783 = 0.162	0.143
7	3	$l < 50000$	780/2556 = 0.305	0.265
7	3	$50000 < l < 100000$	655/2228 = 0.294	0.265
7	5	$l < 100000$	2/2387=0.0008	0.0004
11	2	$l < 100000$	435/4783=0.0909	0.0909
11	10	$l < 100000$	727/1181 = 0.616	0.576
31	30	$l < 100000$	360/585=0.615	0.614
101	100	$l < 100000$	78/121=0.645	0.627
199	198	$l < 100000$	45/72 = 0.625	0.629

4 Function fields

Algebraic function fields, especially those with finite field of constants, i.e. *congruence function fields*, can be treated in complete analogy to algebraic number fields. It is therefore of interest to compute an integral basis, the unit group, the class groups and class numbers of such fields. Applications to cryptography arise here too.

4.1 Integral basis

The Ford-Zassenhaus algorithm ORDMAX-IV can also be used for computing an integral basis of an arbitrary congruence function field K/k of one variable over a finite field of constants k, i.e. an integral basis of the integral closure in K of the polynomial ring $k[x]$ in one variable x over the field k. The algorithm provides at the same time also a way of determining the decompositions in K of the places of the rational subfield $k(x)$ of K. The corresponding algorithms have been implemented in SIMATH by J. Schmitt [30].

4.2 Unit group and regulator

Here we restrict to the case of a real quadratic congruence function field K/k of odd characteristic. Hence, K is generated over its rational subfield $k(x)$ by adjunction of the square-root of a square-free polynomial $D \in k[x]$ of even degree having a square in k^* as its leading coefficient:

$$K = k(x)(\sqrt{D}).$$

Then the place at infinity $\mathfrak{p}_\infty$ splits in K:

$$\mathfrak{p}_\infty = \mathfrak{p}_1\mathfrak{p}_2,$$

and the unit group $U = \mathcal{O}^*$, where $\mathcal{O} := k[x, \sqrt{D}]$ is the integral closure of $k[x]$ in K, has the structure (see, e.g. [46])

$$U = k^* \times \langle \epsilon \rangle$$

with a fundamental unit ϵ. The *regulator* R is the normalized additive $\mathfrak{p}_i$-adic value of the fundamental unit ϵ:

$$R = |v_{\mathfrak{p}_1}(\epsilon)| = |v_{\mathfrak{p}_2}(\epsilon)|.$$

Since the infinite place splits in K, this field K is embedded in the field of Laurent series in $\frac{1}{x}$ over k, viz.

$$K \subseteq K_{\mathfrak{p}_i} = k((\frac{1}{x})) \quad (i = 1, 2).$$

Therefore, we can bring in the continued fraction expansion of the functions in K. A very efficient algorithm is D. Shanks' baby step - giant step method for computing the regulator and a fundamental unit $\epsilon \in U$. This algorithm was developed and implemented in SIMATH by A. Stein [44].

4.3 Class numbers and class groups

Let $K = k(x)(\sqrt{D})$ be a real quadratic congruence function field with ring of integers $\mathcal{O} = k[x, \sqrt{D}]$ as before. Then the ideal class number h' with respect to the principal order $\mathcal{O}$ and the divisor class number h of K/k, i.e. the order of the group of divisor classes of degree zero of K/k, are related by the equation

$$h = R \cdot h'$$

involving the regulator R. An algorithm of Artin implemented in SIMATH by B. Weis (see [46]) yields both class numbers h and h'. Moreover, it is possible by the method of Artin to compute the ideal class group as well as the divisor class group of K/k (see [46]). By bringing in Shanks' infrastructure ideas [43], the algorithm becomes much more efficient as was shown by A. Stein ([44], [45]). A subexponential algorithm for computing regulators, class numbers and class groups, and for solving the discrete logarithm problem - analogous to the number field case - was developed by A. Stein and coauthors ([23]). It is probabilistic and works in function fields K/k of sufficiently large genus.

4.4 Cryptographic applications

In computing the regulator and a fundamental unit of a real quadratic congruence function field $K = k(x)(\sqrt{D})$ by Shanks' baby step - giant step method, one uses the concept of a reduced ideal and applies repeated ideal multiplication and ideal reduction. In this way one utilizes the set $\mathcal{R}$ of reduced principal $\mathcal{O}$-ideals of K as the basic structure. As in the number field case (see [27]), this set can be used in designing a secret key distribution protocol. Compared to the number field case, this key exchange protocol is easier to handle in the function field case. We sketch the protocol, refer to [28], [45] for more details, and give an example.

In a precomputation, two persons A and B generate an odd prime power q and a square-free polynomial $D \in \mathbb{F}_q[x]$ of even degree $\deg D = n$ with leading coefficient a square in $\mathbb{F}_q^*$ so that

$$K = k(x)(\sqrt{D}) \text{ with } k = \mathbb{F}_q$$

is a real quadratic congruence function field. Then, by applying a few baby steps, A and B generate and publicize a reduced ideal $\mathfrak{c} \in \mathcal{R}$ of small "distance" $\delta(\mathfrak{c})$ to the identity ideal $\mathcal{O}$. Then,

A:

(i) secretly generates a positive integer $a < q^{\frac{n}{4}}$

(ii) computes the reduced $\mathcal{O}$-ideal $\mathfrak{a} = \lfloor \mathfrak{c}^a \rfloor \in \mathcal{R}$ "nearest" to $a \cdot \delta(\mathfrak{c})$ and its distance $\delta(\mathfrak{a})$

(iii) publicly transmits $\mathfrak{a}$ to B

B:

(i) secretly generates a positive integer $b < q^{\frac{n}{4}}$

(ii) computes the reduced $\mathcal{O}$-ideal $\mathfrak{b} = \lfloor \mathfrak{c}^b \rfloor \in \mathcal{R}$ "nearest" to $b \cdot \delta(\mathfrak{c})$ and its distance $\delta(\mathfrak{b})$

(iii) publicly transmits $\mathfrak{b}$ to A

Finally,

A computes the reduced $\mathcal{O}$-ideal $\mathfrak{k} = \lfloor \mathfrak{b}^{\delta(\mathfrak{a})} \rfloor \in \mathcal{R}$ nearest to $\delta(\mathfrak{a})\delta(\mathfrak{b})$,

B computes the reduced $\mathcal{O}$-ideal $\mathfrak{k} = \lfloor \mathfrak{a}^{\delta(\mathfrak{b})} \rfloor \in \mathcal{R}$ nearest to $\delta(\mathfrak{b})\delta(\mathfrak{a})$.

This accomplishes the key exchange.

The cardinality of the set $\mathcal{R}$ of reduced principal $\mathcal{O}$-ideals

$$m = \#\mathcal{R}$$

turns out to be the quasi-period of the continued fraction expansion of $\sqrt{D}$. It is chosen to the order of magnitude

$$m \approx q^{\frac{n}{2}}$$

(or smaller).

In the table below, $q = p$ is taken to be a prime and the size of the exponents is fixed according to

$$a,\ b \approx 10^{100}.$$

We exhibit the running times for the key calculations on an SGI challenge workstation as the degree

$$n = \deg\ D$$

and the prime p vary.

Table 2

n	p	$\#\mathcal{R} \approx$	Time
60	1000003	10^{180}	1 m 5 s
60	999999929	10^{270}	1 m 47 s
60	1000000000000000003	10^{540}	15 m 3 s
70	999999929	10^{315}	2 m 25 s
80	1000003	10^{240}	1 m 56 s
80	999999929	10^{360}	3 m 10 s
90	1000003	10^{270}	2 m 26 s
90	999999929	10^{405}	3 m 58 s
100	991	10^{150}	1 m 26 s
100	1000003	10^{300}	2 m 57 s
100	999999929	10^{450}	4 m 53 s
100	999999999999989	10^{750}	42 m 10 s
100	99999999999999999889	10^{1150}	54 m 32 s

5 Elliptic curves over number fields

Let

$$E: \quad y^3 = x^3 + ax + b \quad (a, b \in K)$$

be an elliptic curve in short Weierstrass form defined over an algebraic number field K with ring of integers $\mathcal{O}_K$. Then E has discriminant

$$\Delta = 4a^3 + 27b^2 \neq \mathcal{O}$$

and modular invariant

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

By the Mordell-Weil Theorem, the group $E(K)$ of rational points on E over K, i.e. the Mordell-Weil group of E over K, is finitely generated:

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

where $E_{tors}(K)$ is the *torsion group*, i.e. the (finite) group of points of finite order in $E(K)$, and r is the *rank* of E over K.

The SIMATH system contains basic algorithms for computing the torsion group, the rank and a basis of $E(K)$. Moreover, in SIMATH implemented are algorithms for determining all integral and S-integral points in $E(K)$ if $K = \mathbb{Q}$ is the field of rational numbers. A comprehensive report on these algorithms is given in [48].

5.1 Torsion groups

By a recent theorem of Merel, the order of the torsion group $E_{tors}(K)$ is bounded by a constant depending only on the degree $[K : \mathbb{Q}]$ of the number field K. Moreover, for $K = \mathbb{Q}$, all possible torsion groups $E_{tors}(\mathbb{Q})$ are known by a theorem of Mazur, and for quadratic fields K, the groups $E_{tors}(K)$ are equally known by results of Kamienny, Kenku and Momose.

On restricting the class of elliptic curves E over a number field K by assuming integrality of their modular invariant:

$$j \in \mathcal{O}_K,$$

we used SIMATH to determine all possible torsion groups $E_{tors}(K)$ for curves E over quadratic, cubic and totally real as well as totally complex biquadratic fields K (see [22], [47]). Some results on $E_{tors}(K)$ were obtained also over general quartic fields. Furthermore, aside from torsion groups of small order, all curves E and number fields K of degree $[K : \mathbb{Q}] \leq 4$ such that the group $E_{tors}(K)$ has one of the given structures could be determined.

A special result in this direction is the following

Theorem 5.1 *Let E be an elliptic curve defined over a totally real biquadratic field K, and assume that E has modular invariant $j = \mathcal{O}_K$. Then,*

$$E_{tors}(K) \cong \left\{ \begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & \text{for } 1 \leq m \leq 8,\ m = 14 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mu\mathbb{Z} & \text{for } 1 \leq \mu \leq 3 \end{array} \right\}.$$

We exhibit one example.

Table 3

K	$\mathbb{Q}(\alpha)$ with $\alpha = -2 + 3\sqrt{2} + 2\sqrt{5} - \sqrt{10}$
integral bases	$\omega_1 = 1$ $\omega_2 = \frac{1}{2}\alpha$ $\omega_3 = \frac{1}{8}\alpha^2$ $\omega_4 = \frac{1}{16}\alpha^3$
discriminant	$D_K = 1600 = 2^6 \cdot 5^2$ (totally real)
j	$23365142116 - 43379067008\omega_2$ $+24400725192\omega_3 + 5422383376\omega_4$ $= 3031204456 - 1355595844\sqrt{5}$
$E:\ a$	$-\frac{5553441}{8} + 490833\sqrt{2} + \frac{2483541}{8}\sqrt{5}$ $-219510\sqrt{10}$
b	$445214151 - \frac{1259253945}{4}\sqrt{2}$ $-\frac{796422267}{4}\sqrt{5} + \frac{563156199}{4}\sqrt{10}$
P	$(\frac{963}{4} - 171\sqrt{2} - \frac{429}{4}\sqrt{5} + 75\sqrt{10}, -\frac{81}{2}$ $+\frac{27}{2}\sqrt{2} + \frac{27}{2}\sqrt{5} - \frac{27}{2}\sqrt{10})$ is a point of order 8

The method of proof relies on

- reduction theory
- parametrizations
- norm equations

the latter being solved by the techniques of

- Groebner bases
- Elimination theory
- Fibonacci- and Lucas sequences.

By means of reduction theory, we restrict the possible torsion groups to a finite family. This reduction process requires the assumption that $j \in \mathcal{O}_K$. Then we find parametrizations of elliptic curves with small torsion groups. Finally, we transform the integrality condition on j into a set of norm equations for a parameter α which at the same time yields the elliptic curve E and the number field K such that E over K has torsion group $E_{tors}(K)$ of one of the predetermined structures.

5.2 Rank and basis

Once the torsion group $E_{tors}(K)$ of an elliptic curve E over a number field K is known, the (much more difficult) task remains of determining the rank r and a basis of the free part of the Mordell-Weil group $E(K)$. This goal can be reached in various ways, e.g. via

- Manin's "conditional" algorithm,
- 2-descent via 2-isogeny or general 2-descent,
- 3-descent.

The first method, taking the conjectures of

- Birch and Swinnerton-Dyer
- Shimura-Taniyama
- Hasse-Weil

for granted, was worked out and implemented over $K = \mathbb{Q}$ by J. Gebel (see [12]). The algorithm works for curves E over $\mathbb{Q}$ of rank $r \leq 7$, where the case of rank 7 already takes some extra effort. We mention that in the cases of rank $r \leq 1$ parts of the Birch and Swinnerton-Dyer conjecture are a theorem by work of Coates-Wiles, Rubin, Kolyvagin, Gross-Zagier and Diamond, and furthermore, the conjecture of Shimura-Taniyama was shown to be true for semi-stable elliptic curves by Taylor and Wiles, and the conjecture of Hasse-Weil holds for modular curves by work of Deuring. In any case, Manin's algorithm can be made largely independent of those conjectures by employing 2-descent resp. 3-descent provided that the 2- resp. 3-Tate-Shafarevich group of E over $\mathbb{Q}$ is trivial.

The basic idea behind Manin's algorithm is to embed $E(\mathbb{Q})$ in the r-dimensional real space $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$:

$$E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R},$$

where the kernel is the group $E_{tors}(\mathbb{Q})$, and to apply the method of successive minima from geometry of numbers to the space $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$. This space is Euclidean with respect to the norm induced by the Néron-Tate height $\hat{h}$ on $E(\mathbb{Q})$.

Manin's algorithm has not been worked out for number fields K other than $\mathbb{Q}$. However, first steps are taken already to make a similar procedure available over quadratic fields K, e.g. by performing height computations.

The first algorithm for computing the rank r and r independent points of elliptic curves over quadratic fields K is based on 2-descent and was developed by P. Serf ([40], [5]). It arises from an algorithm sketched by Birch and Swinnerton-Dyer and implemented by Cremona [4] over the rational number field $\mathbb{Q}$. The sophisticated generalization by P. Serf functions over the real quadratic fields

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

of class number one. It will soon be available as part of the SIMATH system.

5.3 High ranks over number fields

A folklore conjecture asserts that the rank of elliptic curves over $\mathbb{Q}$ is unbounded:

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

However, to date only examples of curves E over $\mathbb{Q}$ of relatively small ranks are known. Nagao and Kouya [24] constructed curves E over $\mathbb{Q}$ of rank $r \geq 21$ and Fermigier [6] extended the construction to $r \geq 22$. It is therefore of some interest to study the rank of elliptic curves E over number fields K other than $\mathbb{Q}$.

U. Schneiders [33] investigated the behaviour of the rank of curves E over $\mathbb{Q}$ upon transition to a quadratic extension K of $\mathbb{Q}$. She applied 2-descent via 2-isogeny to establish conditions under which the rank grows at least by one upon transition from $\mathbb{Q}$ to K.

On applying these conditions, M. Sens [29] was able to show, e.g., that an elliptic curve E of rank 9 over $\mathbb{Q}$ attains rank ≥ 28 over an explicitly given multiquadratic field K_{19} of degree $2^{19} = [K_{19} : \mathbb{Q}]$:

$$\mathrm{rk}_{K_{19}} E \geq 28.$$

However, one should be able to do better than that, since, as mentioned above, Fermigier found already curves E over $\mathbb{Q}$ of rank

$$\mathrm{rk}_{\mathbb{Q}} E \geq 22.$$

H. Graf [13] constructed elliptic curves E of high rank over quadratic fields K of class number one. The method used in this construction consists in 2-descent via 2-isogeny. He obtained curves of rank

$$r = \mathrm{rk}_K E \geq 7.$$

The method of 2-decent via 2-isogeny (see [41]) works for curves E with a non-trivial 2-torsion point over $\mathbb{Q}$ or, more generally, over a number field K. It was described by Tate and applied by Penny and Pomerance, Kretschmer, Fermigier and others.

The 2-torsion point is usually assumed to be $P_0 = (0, 0)$ and thus the curve E over K is defined by an equation of the form

$$E: \quad y^2 = x(x^2 + cx + d) \quad (c, d \in K).$$

The 2-isogenous curve is then

$$E': \quad y^2 = x(x^2 + c'x + d') \quad (c', d' \in K)$$

with coefficients

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

One defines the usual group homomorphism

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

and the corresponding homomorphism for the 2-isogenous curve E':

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

and uses the rank formula for $r = \mathrm{rk}_K E$:

$$2^{r+2} = \#\alpha E(K) \cdot \#\alpha' E'(K).$$

The images $\alpha E(K)$, $\alpha' E'(K)$ are calculated by solving certain quartic diophantine equations (see, e.g. [40]).

5.4 Integral points

An interesting question concerns the size of coordinates of integer points on an elliptic curve

$$E: \quad y^2 = x^3 + ax + b$$

over $\mathbb{Q}$ with integer coefficients $a, b \in \mathbb{Z}$. Lang [18] enunciated the following

Conjecture 5.4.1 *The first coordinate of an integer point $P = (x, y) \in E(\mathbb{Q})$ satisfies*

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

with a fixed positive real number h not depending on a, b.

On choosing $a = 0$ and $b = k \in \mathbb{Z} \setminus \{0\}$, one arrives at Mordell's elliptic curves

$$E_k: \quad y^2 = x^3 + k.$$

A conjecture of M. Hall [15] states the following.

Conjecture 5.4.2 *Any integral point $P = (x, y) \in E_k(\mathbb{Q})$ has first coordinate of absolute value*

$$|x| < C|k|^2$$

with a positive real constant C not depending on k.

In [8] we developed and implemented in SIMATH a general procedure for computing all integral points on elliptic curves E over the rationals $\mathbb{Q}$. The procedure relies on a method of Lang and Zagier and requires the knowledge of the rank and a basis of the Mordell-Weil group $E(\mathbb{Q})$. Since, by [12], the group $E(\mathbb{Q})$ can be regarded as known, the method of Lang and Zagier is applicable. The crucial tools are the Néron-Tate height $\hat{h}$ on $E(\mathbb{Q})$ and elliptic logarithms. For computing all integral points in $E(\mathbb{Q})$, the classical complex elliptic logarithms suffice, but if one wants to compute also all S-integral points in $E(\mathbb{Q})$ for a finite set $S = \{\infty, p_1, \ldots, p_s\}$ of places of $\mathbb{Q}$, p-adic elliptic logarithms come into play. The problem with the p-adic elliptic logarithms is that, as opposed to the classical complex elliptic logarithms, no explicit lower bound for linear forms in p-adic logarithms is known in general.

We give here an example of a curve of rank 3.[2]

We list S-integral points for $S_i = \{\infty, p_1, \ldots, p_i\}$ $(0 \le i \le 8)$, where $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, $p_7 = 17$, $p_8 = 19$, on the elliptic curve

$$E: \; y^2 + y = x^3 - 7x + 6$$

of rank 3 with generating points $P_1 = (1, 0)$, $P_2 = (2, 0)$, $P_3 = (0, 2)$. The representation of points in the table reads

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

where $\xi, \eta, \zeta \in \mathbb{Z}$, $\zeta > 0$, $\gcd(\xi, \zeta) = 1 = \gcd(\eta, \zeta)$ with factorization F of ζ.

[2]The author wishes to thank J. Gebel for providing him with these data.

Table 4

S-integral points on $E: \; y^2 + y = x^3 - 7x + 6$

S_i	Nr.	ξ	η	ζ	F
S_0	-1	-3	0	1	
	1	-3	0	1	
	2	-2	3	1	
	3	-1	3	1	
	4	0	2	1	
	5	1	0	1	
	6	2	0	1	
	7	3	3	1	
	8	4	6	1	
	9	8	21	1	
	10	11	35	1	
	11	14	51	1	
	12	21	95	1	
	13	37	224	1	
	14	52	374	1	
	15	93	896	1	
	16	342	6324	1	
	17	406	8180	1	
	18	816	23309	1	
S_1	19	-7	25	2	2
	19	-7	25	2	2
	20	1	13	2	2
	21	9	7	2	2
	22	25	111	2	2
	23	9	69	4	2^2
	24	17	-25	4	2^2
	25	33	17		2^2
	26	-151	1333	8	2^3
	27	625	14839	8	2^3
	28	-47	9191	16	2^4
	29	1793	68991	16	2^4
	30	-2759	60819	32	2^5
	31	207331217	2985362173625	64	2^6
S_2	32	-26	28	3	3
	33	4	35	3	3
	34	7	17	3	3
	35	25	64	3	3
	36	31	116	3	3
	37	58	559	9	3^2
	38	172	350	9	3^2
	39	6142	480700	9	3^2
	40	4537	305425	6	$2 \cdot 3$
	41	-1343	36575	24	$2^3 \cdot 3$
	42	-8159	233461	54	$2 \cdot 3^3$
	43	6169	109871	81	3^4
S_3	44	-69	204	5	5
	45	-66	252	5	5
	46	24	18	5	5
	47	26	-24	5	5
	48	49	-32	5	5
	49	391	7564	5	5
	50	1219	-5797	52	5^2
	51	-33304	562994	125	5^3
	52	13961	1648791	10	$2 \cdot 5$
	53	338776	197180774	15	$3 \cdot 5$
	54	19849	1058743	90	$2 \cdot 3^2 \cdot 5$

S_4	55	-68	1079	7	7
	56	-13	804	7	7
	57	43	132	7	7
	58	106	209	7	7
	59	114	377	7	7
	60	221	2624	7	7
	61	-1525	321308	49	7^2
	62	848961	782099809	56	$2^3 \cdot 7$
	63	1541761	1822623039	392	$2^3 \cdot 7^2$
	64	-11948	-73513	63	$3^2 \cdot 7$
S_5	65	-304	3094	11	11
	66	-164	4179	11	11
	67	113	301	11	11
	68	247	244	11	11
	69	8449	610719	44	$2^2 \cdot 11$
	70	2875	71299	33	$3 \cdot 11$
	71	5200101	11796727776	385	$5 \cdot 7 \cdot 11$
S_6	72	-497	1503	13	13
	73	-139	6336	13	13
	74	66	3056	13	13
	75	329	-1045	13	13
	76	575	9164	13	13
	77	3273	154071	26	$2 \cdot 13$
	78	34953	-1832193	182	$2 \cdot 7 \cdot 13$
	79	12864601	329797213955	6084	$2^2 \cdot 3^2 \cdot 13^2$
S_7	80	-475	15471	17	17
	81	308	-2375	17	17
	82	696	6549	17	17
	83	1436	45214	17	17
	84	9569	91633	68	$2^2 \cdot 17$
	85	433	232928	51	$3 \cdot 17$
	86	521763	397727100	833	$7^2 \cdot 17$
	87	-10391688	18763995251	2023	$7 \cdot 17^2$
	88	-1093232	692674750	663	$3 \cdot 13 \cdot 17$
S_8	89	-451	21344	19	19
	90	913	11477	19	19
	91	21543	3155489	19	19
	92	-3143	155991	38	$2 \cdot 19$
	93	-8501	11871028	171	$3^2 \cdot 19$
	94	19244	436722	95	$5 \cdot 19$
	95	46498	-3933216	209	$11 \cdot 19$

Other tables will be published in the SIGSAM Bulletin.

S. Schmitt [31] used the algorithm of [8] and her procedure [32] for computing the Mordell-Weil group $E(\mathbb{Q})$ to calculate all integer points on the elliptic curves

$$\tilde{E}_k: \quad y^2 = x^3 + 54k^2x + 540k^3 \quad (0 \neq k \in \mathbb{Z},\ 3 \nmid k)$$

and

$$\tilde{E}'_k: \quad y^2 = x^3 + 6(\frac{k}{3})^2x + 20(\frac{k}{3})^3 \quad (0 \neq k \in \mathbb{Z},\ 3|k)$$

in the range

$$k < 100.$$

She found that Lang's conjecture 5.4.1 holds with

$$h = 0.38258353338323422422$$

in the case of $3 \nmid k$, and with

$$h = 0.71590910795617837384$$

in the other case, where $3|k$.

The most successful application of the algorithm [8] and its modification [9] was made on Mordell's elliptic curves E_k. By the SIMATH system, we succeeded in computing all integral points on Mordell's curves E_k in the range (see [10], [11])

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

It turns out that Hall's conjecture holds in this range with the constant

$$C = 5^2.$$

Moreover, we were able to compute all S-integral points on E_k for $S = \{\infty, 2, 3, 5\}$ in the range (see [9], [10])

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

Initially, there were some open rank-one-cases in which we could not find a generating point, and we guessed that there were no integer points on the corresponding Mordell curves. This guess was recently shown to be a fact by K. Wildanger (unpublished).

5.5 Cubic fields and Selmer groups

The right hand polynomial $f(x)$ of the equation

$$E: \quad y^2 = x^3 + ax + b = f(x) \quad (a, b \in \mathbb{Z})$$

defines a non-Galois cubic number field

$$K = \mathbb{Q}(\theta)$$

generated by a root θ of $f(x)$, provided that $f(x) \in \mathbb{Z}[x]$ is irreducible and has discriminant

$$0 \neq D_f = -\Delta = -(4a^3 + 27b^2) \notin \mathbb{Q}^{*2}.$$

By relating the 2-rank of the class group of K to the 2-Selmer group of the elliptic curve E over $\mathbb{Q}$, U. Schneiders [34] was able to construct cubic fields K of 2-class rank ≥ 7. The method of construction generalizes to a great extent an earlier procedure, G. Frey and others had applied to certain Mordell curves. On the other hand, a somewhat different method involving the Jacobians of suitable hyperelliptic curves enabled E. Schaefer [26] to construct cubic fields of 2-rank ≥ 13. U. Schneiders procedure is implemented in SIMATH and can be made available.

6 Elliptic curves over finite fields

G. Lay [20] employed class field theory to construct elliptic curves E of large group order over large finite fields $\mathbf{F}_p$, where p is an odd prime, or $\mathbf{F}_{2^n}$ ($n \leq 1,000$). This construction solves the following tasks:

6.1 Given a positive integer $m > 3$, find a prime p and an elliptic curve E over $\mathbf{F}_p$ of order

$$\#E(\mathbf{F}_p) = m.$$

6.2 Given two positive integers n and c_0, find an elliptic curve E over $\mathbf{F}_{2^n}$ of order

$$\#E(\mathbf{F}_{2^n}) = c \cdot q,$$

where q is a large prime and c is a positive integer $\leq c_0$.

6.3 Given an integer $n > 1$, decide whether or not there is a prime $p > 3$ and an elliptic curve E over $\mathbb{F}_p$ such that

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

6.4 Given a prime $p > 3$ and a positive integer m in the Hasse interval $|p + 1 - m| \leq 2\sqrt{p}$, build an elliptic curve E over $\mathbb{F}_p$ with group order

$$\#E(\mathbb{F}_p) = m$$

and endomorphism ring of small class number.

We comment briefly on 6.3. In general, elliptic curves E over $\mathbb{F}_p$ have cyclic groups $E(\mathbb{F}_p)$. Hasse proved the following

Theorem 6.1 *The structure of the group $E(\mathbb{F}_p)$ of rational points of an elliptic curves E over $\mathbb{F}_p$ is*

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

for positive integers n, m such that $n|m$ and

$$n \mid \gcd(\#E(\mathbb{F}_p), p - 1).$$

Moreover, if we want to achieve $n = m$, then the endomorphism ring $\mathrm{End}(E)$ is an order in K where

$$K = \begin{cases} \mathbb{Q}(\sqrt{-1}) & \text{and} \quad p = n^2 + 1 \\ \text{or} & \\ \mathbb{Q}(\sqrt{-3}) & \text{and} \quad p = n^2 \pm n + 1. \end{cases}$$

Examples (see [19]). We wish to find the smallest integer

$$n \geq 10^{50}$$

such that there is a curve E over $\mathbb{F}_p$ with group

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

We find $n = 10^{50} + 4$ and $p = n^2 + n + 1$. Hence $p \equiv 1 \pmod 3$, and $p = \omega\overline{\omega}$ splits in K. The elliptic curve is

$$E_b : \quad y^2 = x^3 + b$$

with an integer b satisfying the congruence

$$(4b)^{\frac{p-1}{6}} \equiv \left(\frac{4b}{\omega}\right)_6 \pmod p$$

with the sextic residue symbol on the right. The curve E_b is, of course, a CM-curve with invariant $j = 0$.

If we want a CM-curve of type

$${}_aE : \quad y^2 = x^3 + ax,$$

we take $n = 10^{50} + 206$ and $p = n^2 + 1$. Here we have $p \equiv 1 \pmod 4$, and $p = \omega\overline{\omega}$ splits in K. We ensure that the integer a satisfies the congruence

$$(-a)^{\frac{p-1}{4}} \equiv \left(\frac{-a}{\omega}\right)_4 \pmod p$$

with the quartic residue symbol on the right. The curve ${}_aE$ is a CM-curve with invariant $j = 12^3$.

Tables 5 - 7

Type b^- : $p = n^2 - n + 1$

n	b
127822	7558712786
401566	97599279706
1261597	1342884907217
3963435	6625165381497
12451503	61795763555622
39117555	949708068313938
122891451	1750163157126086
386074917	75435874918307051

Type b^+ : $p = n^2 + n + 1$

n	b
12421482	126497545733191
39023243	671003825169805
122595152	8804798066751686
385144068	116776394578684323
1209965882	1294784153356827079
3801220256	3463338849072647762
11941886670	49367926766201606059
37516546691	1383210512453568752380
117861717497	5645314496679314056430
370273537290	11475088408080322688880294

Type a : $p = n^2 + 1$

n	a
3664960	1149851825852
11513830	60257224372045
36171794	1223140504722291
113637066	6492875736404902
357001420	115992465672407033
1121553136	242490182600179197
3523463404	7003561508250280060
11069287696	96350275535540968690
34775195870	989946416399172056564
109249509186	992667512304620575561
343217484646	4928298706659440786394

Obviously, the general construction can be used to find elliptic curves E over $\mathbb{F}_p$ that are applicable in cryptosystems based on discrete logarithms. However, we refrain from going into any details here.

7 Modular curves

The problem under consideration is the construction of small models for the modular curves $X_0(N)$, when N runs through the primes up to 179. This problem is of relevance with respect to the task of counting points on elliptic curves over finite fields. Weierstrass points on the curves $X_0(N)$ are also constructed. This is work in progress, and the corresponding algorithms will be implemented in SIMATH. We confine ourselves here to making the announcement that a paper by M. Pfeifer on this topic will appear later on in this year.

References

[1] Böffgen, R., Der Algorithmus von Ford/Zassenhaus zur Berechnung von Ganzheitsbasen in Polynomalgebren. Ann. Univ. Saraviensis, Ser. Math. **1** No. 3 (1987), 60-129.

[2] R. Böffgen, M. Reichert, Computing the Decomposition of Primes p and p-adic Absolute Values in Semi-Simple Algebras over $\mathbb{Q}$. J. Symb. Comp. **4** (1987), 3-10.

[3] M. Conrad, Gruppenringe und ihre Anwendung auf die Gruppe der zyklotomischen Einheiten. Diploma Thesis, Saarbrücken 1992.

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

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

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

[7] H.G. Folz, H.G. Zimmer, What is the rank of the Dem'janenko matrix? J. Symb. Comp. **4** (1987), 53-67.

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

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

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

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

[12] J. Gebel, H.G. Zimmer, Computing the Mordell-Weil Group of an Elliptic Curve over $\mathbb{Q}$. CRM Proc. and Lect. Notes **4** (1994), 61-83. Amer. Math. Soc., Providence, RI, 1994.

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

[14] R. Gold, J. Kim, Bases for cyclotomic units. Compos. Math. **71** (1989), 13-28.

[15] M. Hall, The Diophantine equation $x^3 - y^2 = k$. In "Computers in Number Theory", ed. by A.O.L. Atkin and B.J. Birch, Acad. Press, London 1971.

[16] S. Jacubec, On Divisibility of Class Numbers of Real Abelian Fields of Prime Conductor. Abh. Math. Sem. Univ. Hamburg **63** (1993), 67-86.

[17] R. Kučera, On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic field. J. Numb. Th. **40** (1992), 284-316.

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

[19] G.J. Lay, Konstruktion elliptischer Kurven mit gegebener Gruppenordnung. Diploma Thesis, Saarbrücken 1994.

[20] G. Lay and H.G. Zimmer, Constructing elliptic curves with given group order over large finite fields. In: "Algorithmic Number Theory" ed. by L.M. Adleman and M.-D. Huang. Lect. Notes in Comp. Sci. **877** (1994), 250-263. Springer-Verlag, Heidelberg, Berlin.

[21] M. Mignotte, A criterion on Catalan's equation. J. Numb. Th. **52** (1995), 280-283.

[22] 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", edited by J.-M. De Koninck and C. Levesque. W. de Gruyter, Berlin, New York 1989, 671-698.

[23] V. Müller, Chr. Thiel, A. Stein, Computing discrete logarithms in real quadratic congruence function fields of large genus. Submitted to Math. Comp.

[24] 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.

[25] J. Sands, W. Schwarz, A Dem'janenko Matrix for Abelian Fields of Prime Power Conductor. J. Number Th. **52** (1995), 85-97.

[26] E.F. Schaefer, Class Groups and Selmer Groups, J. Numb. Th. **56** (1996), 79-114.

[27] R. Scheidler, J.A. Buchmann, H.C. Williams, A key exchange protocol using real quadratic fields. J. Cryptology **7** (1994), 171-199.

[28] R. Scheidler, A. Stein, Key-Exchange in Real Quadratic Congruence Function Fields. Designs, Codes and Cryptography **7** (1996), 153-174.

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

[30] J. Schmitt, An embedding algorithm for algebraic congruence function fields. Proc. Intern. Sympos. Symbolic Alg. Comp. 1991, ed. by St. Watt, ACM Press, New York 1991, 187-188.

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

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

[33] U. Schneiders, H.G. Zimmer, The rank of elliptic curves upon quadratic extension. In: "Computational Number Theory", ed. by A. Pethö, M. Pohst, H.C. Williams and H.G. Zimmer. W. de Gruyter, Berlin 1991, 239-260.

[34] U. Schneiders, Estimating the 2-rank of cubic fields by the Selmer group of elliptic curves. J. Numb. Th. **62** (1997), 375-396.

[35] W. Schwarz, Dem'janenko matrix and 2-divisibility of class numbers. Arch. Math. **60** (1993), 154-156.

[36] W. Schwarz, A note on Catalan's equation. Acta Arith. **72** (1995), 277-279.

[37] W. Schwarz, Über die Klassenzahl abelscher Zahlkörper. PhD Thesis, Saarbrücken 1995.

[38] W. Schwarz, H.G. Zimmer, Stickelberger ideal and signature of circular units. Math. Z. **223** (1996), 1-11.

[39] W. Schwarz, On p-divisibility of the class number of a real abelian field. To appear.

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

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

[42] SIMATH manual, Saarbrücken 1996.

[43] D. Shanks, The Infrastructure of a Real Quadratic Field and its Applications. Proc. 1972 Number Theory Conference, Boulder, Colorado (1972), 217-224.

[44] A. Stein, Baby step - Giant step - Verfahren in reell-quadratischen Kongruenzfunktionenkörpern mit Charakteristik ungleich 2. Diploma Thesis, Saarbrücken 1992.

[45] A. Stein, Algorithmen in reell-quadratischen Kongruenzfunktionenkörpern. PhD Thesis, Saarbrücken 1996.

[46] B. Weis, H.G. Zimmer, Artins Theorie der quadratischen Kongruenzfunktionenkörper und ihre Anwendung auf die Berechnung der Einheiten- und Klassengruppen. Mitt. Math. Ges. Hamburg **12**, Heft 2 (1991), 261-286.

[47] H.G. Zimmer, Torsion Groups of Elliptic Curves over Cubic and Certain Biquadratic Number Fields. Contemp. Math. **174** (1994), 203-220.

[48] H.G. Zimmer, Basic algorithms for elliptic curves. To appear in: Proceedings of the Number Theory Conference held in 1996 at Eger, Hungary.