COMPUTERS AND COMPUTATIONS IN ALGEBRAIC NUMBER THEORY

Horst G. Zimmer
Mathematisches Institut der Universität (TH) Karlsruhe
Karlsruhe, Germany

Summary. In the present survey an outline is given of certain recent as well as earlier developments in the use of electronic high-speed computers in algebraic number theory.

Introduction

The basic task of providing non-trivial numerical examples in algebraic number theory frequently requires the aid of an electronic computer. Such examples serve various purposes such as to illustrate known theorems or, in many cases, to make up or support conjectures which may finally lead to new theorems. However, it is often far from easy to devise algorithms which are capable of being converted into effective computer programs. Efforts to invent such algorithms frequently yield as by-products new theoretical findings which are also per se of interest (see e.g. [23], [81]).

This survey is aimed at sketching by means of selected topics what has been done toward these directions. The treatment of the subject matter is not strictly confined to investigations involving the computer but rather includes also some researches devoted to general computational problems.

The ten sections of this report are only loosely connected. The bibliography is, of course, by no means complete but further references may often be found in the papers quoted. Some of the papers included in the bibliography are unpublished manuscripts.

I wish to take this occasion to express my gratitude to those authors who made their manuscripts available to me.

1. Finite fields

For many number-theoretic applications it is of significance that finite fields can be constructively handled. Computing in a finite prime field GF(p) means simply carrying out the four rational operations in integers modulo p. If, by induction, the Galois field GF(q) with $q = p^m$ elements is constructively known its overfield $GF(q^n)$ can be constructed by producing an irreducible polynomial of degree n over GF(q) such that a root b yields a basis $1, b, \ldots, b^{n-1}$ over GF(q) or, more generally, by exhibiting a basis $a_1, a_2, \ldots, a_n$ of $GF(q^n)$ over GF(q) together with a multiplication table (cf. [1], [2], [14], [53], [65], [78] for the former, and [20], [24], [78] for the latter). In Section 3 we shall show in greater generality how to find b if a basis $a_1, a_2, \ldots, a_n$ is given.

Regarding the multiplicative structure of $GF(p^n)$, a primitive root, i.e. a generator of the multiplicative group of $GF(p^n)$, is to be determined [2]. This task is solved by Gauss' method [78].

2. Factorization of polynomials

Procedures for factoring polynomials over a finite prime field GF(p) are useful in many regards such as, for instance, the construction of finite extensions of GF(p) (cf. Section 1), the factorization of polynomials over the ring of all rational integers, $\underline{Z}$, (see [81]), or the decomposition of prime numbers p in finite algebraic number fields ([16], [40], [56], [69]).

To reduce, whenever it is possible, the task of factoring a monic separable polynomial f(x) of degree n over GF(p) to that of factoring a polynomial of lower degree one makes use of the fact that an irreducible factor of degree m of f(x) over GF(p) must divide the polynomial $x^{p^m} - x$ over GF(p). Accordingly, Kempfert [39] suggested to compute the greatest common divisors over GF(p)

$$(f(x),\ x^{p^i} - x) \quad \text{for } i = 1, \ldots, \left[\tfrac{n}{2}\right].$$

However, this process need not yield a proper factor of f(x) let alone the complete factorization of f(x) over GF(p). To obtain the complete factorization, an algorithm of Berlekamp [4] may be applied which essentially amounts to the calculation of the null-space of a certain matrix. This algorithm, consisting of several g.c.d.-processes, is very efficient for small primes p (or, more generally, small powers of p). The null-space approach was replaced with a different explicit construction by Mc Eliece [47]. For large primes p, however, the algorithm has to be modified in order to retain efficiency. Modified versions, which then also permit to factor polynomials over GF(q) with large p-powers $q = p^m$, are due to Berlekamp [5], [6] and Zassenhaus [81].

In general more difficult is the problem of factoring a monic separable polynomial f(x) of degree n over $\underline{Z}$. If C is the maximal absolute value attained by the coefficients of f(x), the coefficients of a factor $g(x) = x^m + b_1 x^{m-1} + \ldots + b_m$ satisfy the inequalities

$$|b_j| \leq \binom{m}{j}(C+1)^j \qquad (j = 1, \ldots, m).$$

If these bounds are not too large for $m \leq \left[\frac{n}{2}\right]$ the factorization of f(x) over $\underline{Z}$ can be accomplished by picking a prime p which is greater than the maximal bound and by factoring then f(x) over GF(p). If need be, this process is to be repeated for some more suitably chosen p (cf. [45]).

Zassenhaus [81] turned Hensel's Lemma into an effective routine for factoring polynomials f(x) over $\underline{Z}$. Instead of a large prime, any prime p not dividing the discriminant d(f) is chosen and a decomposition of f(x) into two monic factors modulo $p^1\underline{Z}[x]$ is pro-

duced. Clearly, $f(x)$ is irreducible over $\underline{Z}$ if it has no proper decomposition modulo $p\underline{Z}[x]$. Otherwise the decomposition modulo $p\underline{Z}[x]$ is lifted to a modulus which involves a higher power of p, proceeding inductively from

$$f(x) \equiv f_1(x)f_2(x) \bmod p^r\underline{Z}[x]$$

to

$$f(x) \equiv f_1'(x)f_2'(x) \bmod p^{2r}\underline{Z}[x].$$

Since this way the p-power contained in the modulus will rapidly approach the magnitude of the above-mentioned bounds it will be possible for a suitable p-power, say the s-th power of p, to decide whether or not the decomposition of $f(x)$ modulo $p^s\underline{Z}[x]$ gives rise to a decomposition of $f(x)$ over $\underline{Z}$. This process is to be repeated for all possible decompositions of $f(x)$ into two monic factors modulo $p\underline{Z}[x]$. To obtain the complete factorization of $f(x)$ over $\underline{Z}$ the procedure has to be carried on recursively for each of the two factors of $f(x)$ over $\underline{Z}$ which resulted from the first step. The weakness of this routine becomes apparent when $f(x)$ has way more factors modulo $p\underline{Z}[x]$ for the prime p chosen than it has over $\underline{Z}$ itself. As for the details of this algorithm, we refer to the papers [81] (in which different bounds for the coefficients of factors are used) and [83].

A thorough discussion of effectiveness questions regarding the factorization of polynomials and other procedures related to field theory was carried through by Fröhlich and Shepherdson ([27],[28]).

3. Field extensions

(a) Primitive elements. For finite fields k, the question of constructing finite extensions K of k was already dealt with in Section 1.

Let now k be an arbitrary constructively accessible field and K/k a finite separable extension of degree n. It is known that there exists a primitive element $b \in K$ such that $K = k(b)$. Given a basis $a_1,\ldots,a_n$ of K/k, a primitive element b for K/k can be found by a trial-and-error method, forming randomly linear combinations $\sum_{i=1}^{n} e_i a_i$ with $e_i = 0$ or 1 until a primitive element turns up. Sonn and Zassenhaus [60] who proposed this method showed that it is bound to work. In fact, the probability to catch this way a primitive element b for K/k is at worst $1 - \frac{n-1}{2^{n/2}}$, a number which approaches 1 as n tends to infinity.

(b) Tschirnhausen transformations. The p-adic method used for factoring polynomials over $\underline{Z}$ (Section 2) was also successfully employed by Zassenhaus and Liang [80] to answer the following questions Hasse [33] brought up. Let $f(x)$, $f'(x)$ be two polynomials over $\underline{Z}$ having the real roots b, b' respectively. Suppose that $f(x)$ and $f'(x)$ are irreducible of degree n over the rational number field $\underline{Q}$. How to decide whether or not b and b' generate the same field extension over $\underline{Q}$, and, if the answer is affirmative, how to find a Tschirnhausen transformation expressing b and b' in terms of one another? The solution of this problem allows at the same time to exhibit a generating element of the cyclic Galois group $G(K/k)$ of the extension $K = k(b)$ generated by b over a certain quadratic field k over $\underline{Q}$. This answers another question posed by Hasse [33]. Both questions play a part in the construction of the class field K to the quadratic number field $k = \underline{Q}(\sqrt{-47})$ (see Section 9).

(c) Real root calculus. If k is an ordered field (e.g., $k = \underline{Q}$) in which the four rational operations and, for every field element, the sign determination can be constructively performed the question arises of how to do the same in an ordered extension K of k obtained by adjoining to k the real roots (in a real closed algebraic extension of k) of a separable polynomial $f(x)$ over k. To this end the real roots of $f(x)$ are to be numbered by increasing magnitude such that every root is uniquely determined by its index. The question can then be reduced to the case of a simple extension since K/k may be broken up into a chain of simple extensions by successively adjoining to k the real roots of $f(x)$. An affirmative answer to the question, based in part on a constructive proof of Sturm's Theorem, was given by Hollkott [35] in his doctoral thesis. Subsequently Zassenhaus [82] and Kempfert [38] adapted Hollkott's methods for a computer program called "real root calculus" in which the rational operations and the sign determination are performed in certain real algebraic number fields.

4. Galois groups

The problem to be discussed here is how to construct the Galois group of the splitting field of a given equation over the rational number field $\underline{Q}$ and, conversely, how to realize certain given groups as Galois groups of equations over $\underline{Q}$.

As to the latter question, Trinks [72] verified by the aid of a computer program that $G_{168} = PSL(3,GF(2))$, the simple group of order 168, is materialized as the Galois group of the splitting field of the equation $x^7 - 7x + 3 = 0$ over $\underline{Q}$. Rowlinson and Schwerdtfeger [54] proceed along similar lines in a paper in which they discuss the problem of finding polynomials whose Galois groups satisfy certain prescribed conditions.

Regarding the first question, an attempt to determine the Galois group of a given monic separable polynomial $f(x)$ was made by Zassenhaus [77] under the supposition that it is possible to decide whether or not the polynomial $f(x)$ has a root in $\underline{Q}$ and, in case the answer is affirmative, to exhibit one. However, the method cannot be used on a computer since it is inefficient.

A more practicable approach to the problem relies on an idea of van der Waerden. Here, the cycle decomposition patterns of elements of the Galois group (as permutation group) are sampled by looking at the polynomial $f(x)$ modulo $p\underline{Z}[x]$ for several suitably chosen primes p. This way some information on the type of the Galois group of $f(x)$ as a

subgroup of the symmetric group on n letters $\underline{S}_n$ can be derived, where n is the degree of f(x). The method, if further extended by virtue of Čebotarev's Density Theorem, allows a complete determination of the Galois groups of polynomials f(x) over $\underline{Q}$ of degrees up to n = 8. D. Smeltzer, a student of Zassenhaus, is working on a corresponding computer program. The van der Waerden method was already successfully applied by Cockayne [15] to isolate some elements of the Galois groups of various polynomials over $\underline{Z}$.

5. Continued fractions

Continued fractions offer a wide field for computer-assisted computations. Quadratic irrationalities possess the simplest continued fraction expansions since for them the partial quotients become periodic. They play an important role in unit determination and class number computation for real quadratic number fields (Sections 7, 8).

It is also not too difficult to compute the simple continued fraction expansion of an irrational algebraic number that is the only real root of an equation with rational integral coefficients [48]. Zassenhaus [79] devised a method of dealing with real algebraic irrationalities which are the roots of equations over $\underline{Z}$ having more than one real root. The main difficulty to be overcome here is that of keeping apart the distinct real roots of the equation in question. Recently, D. Cantor, P. Galyean and this ([84]) author showed how one can cope with this difficulty. The Zassenhaus algorithm has been programmed by Smith [59].

A peculiar phenomenon was discovered by Brillhart and his student Morrison. In the simple continued fraction expansion of the real root of certain cubic equations as, for example, $x^3 - 8x - 10 = 0$, among mostly small partial quotients there occur also very large ones. Stark [62] showed that this phenomenon can be explained by means of the theory of modular functions. It has, roughly speaking, something to do with the fact that $x^3 - 8x - 10 = 0$ has the discriminant $-4 \cdot 163$ and that the quadratic field $\underline{Q}(\sqrt{-163})$ possesses the class number one (see Section 8), an observation that was made by D.H. Lehmer.

Extensive investigations were carried through by Bernstein regarding the question of when the Jacobi-Perron algorithm for the generalized continued fraction expansion involving a basis $a_1,\ldots,a_n$ of an algebraic number field $K/\underline{Q}$ of degree n becomes periodic. In case periodicity occurs the algorithm yields a unit of K. Elsner and Hasse [25] used a computer to detect new periodicity cases.

Continued fraction developments other than simple ones of real quadratic irrationals have been computed by E. Frank [26].

6. Modules and orders

(a) Sum and intersection of modules. Let M,N be two $\underline{Z}$-modules of rank r generated by a finite number, say m,n, respectively, of r-columns over $\underline{Q}$. A simple algorithm for determining the sum J = M + N and intersection I = M ∩ N of the two given $\underline{Z}$-modules was found independently by Cantor [12] and by Zassenhaus [74]. M and N can be represented by an r×m matrix A and an r×n matrix B over $\underline{Q}$ respectively. If we then transform the 2r×(m+n) matrix

$$\begin{pmatrix} A & B \\ A & 0 \end{pmatrix} \text{ into lower diagonal form } \begin{pmatrix} X & 0 \\ * & Y \end{pmatrix}$$

by employing elementary column operations, the sum J and intersection I are represented by the matrices X and Y respectively. This algorithm can be used for solving systems of linear Diophantine equations over $\underline{Z}$ or for determining ideals in $\underline{Z}[x]$ generated by a finite number of polynomials $f_1(x),\ldots,f_s(x)$.

(b) Embedding of an order into a maximal order. Given a finite-dimensional commutative algebra $\underline{A}$ over $\underline{Q}$ and an order $\underline{o}$ in $\underline{A}$ it is our aim to determine the maximal order $\underline{O}$ of $\underline{A}$ containing $\underline{o}$. All orders in $\underline{A}$ are to be expressed in terms of a basis $a_1,\ldots,a_r$ of $\underline{A}$ over $\underline{Q}$. That aim cannot effectively be reached by a search procedure which finds $\underline{O}$ among all (finitely many) orders between $\underline{o}$ and $d'\underline{o}$, where d' is the inverse of the discriminant d of $\underline{o}$. Zassenhaus [75], [76] suggested to construct instead by induction a chain of orders

$$\underline{o} \subset \underline{o}_1 \subset \ldots \subset \underline{o}_m \subset \underline{o}_{m+1} \subset \ldots \subset \underline{O}$$

utilizing the following fact. Suppose that $\underline{o}_m \neq \underline{O}$. Then there is a prime p whose square divides the discriminant d_m of $\underline{o}_m$. Moreover, the p-radical $\underline{R}_{p,m}$ defined by $\underline{R}_{p,m} = \{ x \in \underline{o}_m / x \bmod p\underline{o}_m \text{ is nilpotent} \}$ then gives rise to a bigger order $\underline{o}_{m+1}$ if one takes $\underline{o}_{m+1}$ to be the quotient module $\underline{R}_{p,m}/\underline{R}_{p,m}$. As soon as an intermediary order $\underline{o}_n$ is found with no prime p such that p^2/d_n the maximal order $\underline{O} = \underline{o}_n$ is reached.

This construction is of particular interest in case $\underline{A} = K$ is a finite algebraic number field over $\underline{Q}$ since it facilitates the determination of the ring of algebraic integers $\underline{O}$ in K.

(c) Fractional ideals in an order. Let $\underline{o}$ designate an order in an algebraic number field k of finite degree n over $\underline{Q}$. Gauss discovered (in a different form) that, for an order $\underline{o}$ in a quadratic number field k (n = 2), every fractional ideal of $\underline{o}$ is invertible in the semigroup of all fractional ideals of $\underline{o}$. On the other hand, Dedekind was aware of the fact that this result does not remain true if one considers orders $\underline{o}$ in algebraic number fields k of degree $n > 2$ over $\underline{Q}$. It is therefore natural to ask how the result for n = 2 can be generalized for $n > 2$.

Based on some numerical evidence provided by a computer the three authors of [21], [22] conjectured that in the general case of an order $\underline{o}$ in an algebraic number field k of degree n over $\underline{Q}$ the (n - 1)-st power and all higher powers of every fractional ideal of $\underline{o}$ are invertible in the semigroup of all fractional ideals of $\underline{o}$. This conjecture was in fact proven in [22]. In connection with it many

other interesting results on ideals in $\underline{o}$ were obtained.

7. Units in algebraic number fields

The problem to be dealt with here is, in accordance with Dirichlet's Unit Theorem, that of determining for a given algebraic number field K of degree n over $\underline{Q}$ a system of $r_1 + r_2 - 1$ fundamental units of K, where r_1 is the number of real and $2r_2$ the number of complex conjugate fields of K. Any such system consists of independent units that generate the whole unit group modulo the subgroup of the roots of unity in K.

Basically, the following procedure yields a system of fundamental units of K in a finite number of steps. Employing Minkowski's theorem on linear forms one constructs a sequence $c_1, c_2, \ldots$ of integral elements of K satisfying the conditions

$$|N(c_i)| \leq |\sqrt{d}|\,, \qquad (i = 1,2,\ldots) \qquad (1)$$

$$L(c_1) < L(c_2) < \ldots, \qquad (2)$$

where d is the discriminant of $K/\underline{Q}$ and N the norm relative to $K/\underline{Q}$, while L designates a certain linear form involving the logarithms of the absolute values of c_i and its conjugates. Because of condition (1), the sequence $c_1, c_2, \ldots$ contains only a finite number of prime factors (that is, of prime ideals dividing $c_1, c_2, \ldots$). Therefore, there are infinitely many indices i,j such that c_i/c_j is a unit of K. Condition (2) then makes it possible to construct independent units. From them fundamental units in K can be derived.

For a quadratic number field $K = \underline{Q}(\sqrt{d})$ with discriminant d, an integral element $u = \frac{x + y\sqrt{d}}{2}$ is a unit if and only if $N(u) = \pm 1$, that is, if and only if the rational integral components x, y of u satisfy the so-called Pell equation $x^2 - dy^2 = \pm 4$.

Imaginary quadratic number fields $K = \underline{Q}(\sqrt{d})$ (i.e. $d < 0$) have no units aside from roots of unity, and the latter are easily determined from Pell's equation. If $d < -4$, then ± 1 are the only roots of unity in K.

A real quadratic field $K = \underline{Q}(\sqrt{d})$ (i.e. $d > 0$) possesses a unique fundamental unit $e > 1$. The unit e can be calculated by solving Pell's equation. To this end one needs, in general, to apply the continued fraction algorithm (Section 5) to $\sqrt{d}$. For a table of fundamental units in certain K's we refer to Ince [36].

In a totally real cubic number field K two fundamental units e_1, e_2 generate the infinite part of the unit group. Billevič [7], [8] followed essentially the general method indicated above to determine two fundamental units of K, thereby at the same time improving Voronoi's Algorithm (cf. [73]). Another approach to the unit calculation in totally real cubic fields K was proposed by Godwin [30] who employed quadratic expressions rather than linear forms L.

In a cyclic cubic number field K one fundamental unit and one of its conjugates generate the unit group modulo roots of unity. Cohn and Gorn [17] computed such a fundamental unit for several cyclic cubic K's.

A table of the fundamental unit e of the cubic fields $K = \underline{Q}(\sqrt[3]{m})$ generated by the real cube root of the cube-free intergers m in the interval $50 \leq m \leq 100$ was produced by Selmer [56].

Cohn [19] showed how the information available on fundamental units of real quadratic fields can be utilized to construct systems of fundamental units in composite real quartic and octic number fields.

In an earlier paper [32] Hasse had developed an algorithm for finding systems of fundamental units in cyclic cubic and biquadratic number fields. His methods, exploiting results from the analytic theory of numbers, were generalized by Leopoldt [41], [42] to the case of an arbitrary abelian number field K.

More recently, Billevič [10] extended his above-mentioned algorithm to arbitrary algebraic number fields K of degree n over $\underline{Q}$.

8. Class numbers of algebraic number fields

The classical proof of the theorem on the finiteness of the class number h for a finite algebraic number field K of degree n over $\underline{Q}$ furnishes at the same time also one possible rational procedure for calculating h. It depends upon the existence of a positive (real) constant B, the so-called Minkowski bound, such that every ideal class of K contains an integral ideal $\underline{a}$ whose norm satisfies the inequality $N(\underline{a}) \leq B$. Explicitly, Minkowski obtained for B the general expression

$$B = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|}\,,$$

where r_2 is defined as in Section 7 and d denotes the discriminant of $K/\underline{Q}$. The task of computing h then amounts to setting up a complete system of inequivalent integral ideals $\underline{a}$ of K (cf. [9]) for which it is enough to consider only those finitely many $\underline{a}$'s with the norm condition $N(\underline{a}) \leq B$.

As a different powerful tool for computing h we mention the analytic class number formula.

It is obvious that any improvement on the bound B will make the procedure more effective. This can in particular be achieved for quadratic number fields (see [49]). Recently Newman [50] and Ordman [51] established class number tables for quadratic fields $K = \underline{Q}(\sqrt{d})$, where d ranges over certain negative prime discriminants. Also very useful are the tables Schaffstein [55] and Ince [36] published about 40 years ago.

A statistical study carried through by Leopoldt [43] shows a deviation of the computed number from the expected number of imaginary quadratic number fields $K = \underline{Q}(\sqrt{d})$ with prime discriminants $d = -p$ (where $p \equiv -1 \pmod 4$; $p < 498{,}000$) whose class number h(d) is divisible by a given number m.

For a long time it had been an open question whether Gauss' conjecture is true that there are only finitely many imaginary

quadratic fields $K = \mathbb{Q}(\sqrt{m})$ with class number one. Gauss himself already verified by means of his theory of reduced quadratic forms that the fields K with $m = -1,-2,-3,-7,-11,-19,-43,-67,-163$ possess class number one. Following up the contributions of several authors to the question if these fields are the only ones having class number unity, Heegner (see [61]) in 1952 eventually supplied the missing link for a complete affirmative answer to that question.

Class numbers of totally real cubic number fields K were computed by Godwin [31] who applied the same device he had already successfully used for unit calculations [30]. Godwin listed all those cubic fields K of an earlier table [29] which have a discriminant $d < 20{,}000$ and whose class number h is 1,2,3, or 4.

Larger class numbers turned up for some pure cubic fields $K = \mathbb{Q}(\sqrt[3]{m})$. Specifically, Cassels [13] found via the algebraic approach the class number $h = 12$ for the real field $K = \mathbb{Q}(\sqrt[3]{43})$, and Cohn [18] obtained by analytic methods class numbers between 18 and 27 for fields K generated by the real root of bigger integers m. Further tables for pure cubic fields are provided by Selmer [56].

Units and class number of an algebraic number field K areclosely related. Cohn [19] combined a class number formula of Wada, involving the index of a certain subgroup in the whole unit group, and his results on units in quartic and octic fields (Section 7) to determine the class number of these fields.

Cyclotomic fields are largely accessible to numerical calculations. Bauer [3] computed the class number of real cyclic subfields K of cyclotomic fields with the restrictions $f < 100$ on the conductor of K and $B < 50{,}000$ on the improved Minkowski-Rodgers bound for K. Leopoldt's p-adic class number formula is used in the computations and the class numbers 1,2, and 3 are obtained.

The exponent j(i) of the highest p-power dividing the class number h_{i+1} of the p^{i+1}-th cyclotomic field K_{i+1} over $\mathbb{Q}$ is, for sufficiently large i, given by Iwasawa's formula

$$j(i) = l_p i + m_p p^i + n_p ,$$

where p is a prime and $l_p \geq 0$, $m_p \geq 0$, n_p are integers depending only on p. Iwasawa and Sims [37] used a computer to determine the constants l_p, m_p, n_p for all primes $p \leq 4{,}001$. The striking result of their computations was the discovery that $m_p = 0$ for all p's within the investigated range.

9. Class groups and class fields of algebraic number fields

Once the class number of an algebraic number field K of finite degree n over $\mathbb{Q}$ is known there arises the usually far more complicated task of determining the structure of the ideal class group as well as the Hilbert class field H of K (H is the largest unramified abelian extension of K).

On the occasion of his class number calculations for imaginary quadratic number fields $K = \mathbb{Q}(\sqrt{d})$ with prime discriminant $d = -p \equiv 1 \pmod 4$ Leopoldt [43] (see Section 8) also determined all class groups of K for p within the interval $1 < p < 304{,}000$ and a selection of class groups of K for p in $304{,}000 < p \leq 551{,}407$. In the majority of all cases investigated the class groups turned out to be cyclic. The non-cyclic class groups found are of the q-types (3,3), (3,9), (3,27), (3,81), (3,243), (9,9), (9,27),(5,5), (5,25), (7,7), (7,49), (11,11).

Employing purely arithmetic methods of class field theory Hasse [33] numerically constructed the class field H of the quadratic number field $K = \mathbb{Q}(\sqrt{-47})$. This field can be characterized as the first imaginary quadratic field whose class number h is divisible by 5, namely, $h = 5$. $H/\mathbb{Q}$ is normal with the dihedral group of order $2 \cdot 5$ as Galois group, and H/K is cyclic of degree 5. The problem arises of finding an irreducible polynomial of degree 5 over $\mathbb{Z}$ such that its real root b generates H/K and, furthermore, of exhibiting a generator of the cyclic Galois group of H/K. The first task is solved via constructing a radical extension over the field of 5-th roots of unity, $K^{(5)}$, over K. A solution of the second task was achieved by the p-adic methods developed in the joint paper [80] of Zassenhaus and Liang who, as we mentioned in Section 3 (b), also settled a question regarding Tschirnhausen transformations which Hasse came across in this connection.

On establishing class number and prime decomposition tables in the real cubic fields $K = \mathbb{Q}(\sqrt[3]{m})$ for $1 < m \leq 50$, Selmer [56] also displays generators of the cyclic ideal class groups of these K's.

In his diploma thesis Matzat [46] considers number fields K of degrees 5 and 7 over $\mathbb{Q}$ generated by roots of polynomials with integral (rational) coefficients ≤ 5. A computer program was designed to determine the class number and defining relations for the class group of such fields K as well as the Galois group of some of the polynomials. It was in this connection that the polynomial of degree 7 mentioned in Section 4 turned up whose Galois group was shown to be G_{168} by Trinks.

Of great significance for class number problems is Hilbert's Theorem 94 (see [69]). It states that, for an unramified cyclic number field E of odd prime degree p over a finite algebraic number field K, there exists an ideal in K which is not principal in K but which becomes principal in E. This implies in particular that the class number of K is divisible by p.

Hilbert's Theorem 94 gives no indication as to which ideal classes of K become principal in E. Class field theory reveals that all ideal classes of K become principal in the Hilbert class field H of K. O. Taussky has in several papers (see [70], [71] and quotations given there) substantially contributed to a discussion of the deep question as to how the ideal classes of K behave in subfields of the Hilbert class field H of K. No general law governing this behavior is known yet. However, in the case of a number field K whose p-class group CG is of the

isomorphy type (p,p), where p denotes an odd prime, O. Taussky ([70],[71]), distinguishing between two types of unramified cyclic extensions E_i of K according as the subgroup CG_i of CG, pertaining to E_i, becomes principal in E_i or not, finds certain conditions under which one or the other type occurs. Also some information on how many ideal classes of K become principal in E_i is obtained.

10. Diophantine equations

Let

$$y^2 = x^3 + ax + b \qquad (a,b \in \underline{Z})$$

designate an elliptic curve over the rational number field $\underline{Q}$. By Mordell's Theorem, the group of rational points of this curve over $\underline{Q}$ is finitely generated, and, according to Siegel's Theorem, the curve has at most finitely many points with coordinates in $\underline{Z}$.

Quite a few computer-assisted computations (of which we cite here only a modest selection) have been carried out to determine all points over $\underline{Z}$ of certain elliptic curves of the above type and to find generators of the infinite part of their rational point groups over $\underline{Q}$. In these computations use is made of the information available on class numbers and units of quadratic, cubic and quartic number fields (Sections 7 and 8).

Quadratic fields are involved in Podsypanin's [52] calculations of generators for $y^2 = x^3 - D$ with $0<|D|<90$. Cassels [13] reduces the problem of determining solutions of infinite order of this equation over $\underline{Q}$ to computations in cubic fields and produces tables for $0<|D|\leq 50$, thereby correcting several errors in [52]. Hemer employed similar methods to extend existing tables of several authors, with a few exceptions, to $0<|D|\leq 100$ (see [34], [57],[58]). Further completions of those tables were accomplished by Ljunggren [44] who worked in quartic number fields and, recently, by Stephens [64] who referred again to cubic number fields.

In conclusion, we mention here the famous conjectures of Birch and Swinnerton-Dyer ([11],[66],[67]) relating the number of generators g of the rational point group of an elliptic curve over $\underline{Q}$ to a certain global L-series of the curve. The conjectures that are supported by a convincing amount of numerical evidence have entailed many further explicit calculations as well as theoretical investigations and generalizations by several authors (e.g., [63], [68]).

REFERENCES

1. J.D. Alanen and D.E. Knuth, A table of minimum functions for generating Galois of $GF(p^n)$. Sankhyā Ser. A 23 (1961), 128. MR 28 ≠≠ 4756.

2. _____, Tables of finite fields. Sankhyā Ser. A 26 (1964), 305-328. MR 32 ≠≠ 4122.

3. H. Bauer, Numerische Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper. J. Number Theory 1 (1969), 161-162. MR 39 ≠≠ 1426

4. E.R. Berlekamp, Factoring polynomials over finite fields. Bell System Tech. J. 46 (1967) 1853-1859. MR 36 ≠≠ 2314.

5. _____, On the factorization of polynomials over very large finite fields. Bell Telephone Lab., Inc., Murray Hill, New Jersey, 1968.

6. _____, How to find the factorization of polynomials over very large finite fields. Bell Telephone Lab., Inc., Murray Hill, New Jersey, 1968.

7. K.K. Billevič, On units of algebraic fields of third and fourth degree. Mat. Sb., N.S., 40 (82) (1956), 123-136. MR 19, 533.

8. _____, Letter to the editors. Mat. Sb., N.S., 48 (90) (1959), 256.

9. _____, On the equivalence of two ideals in an algebraic field of order n. Mat. Sb., N.S., 58 (100) (1962), 17-28. MR 25 ≠≠ 5049.

10. _____, A theorem on unit elements of algebraic fields of order n. Mat. Sb., N. S., 64 (106) (1964), 145-152. MR 29 ≠≠ 1201.

11. B.J. Birch and H.P.F. Swinnerton-Dyer, Notes on elliptic curves I, II. J. Reine Angew. Math. 212 (1963), 7-25. MR 26 ≠≠3669; 218 (1965), 79-108. MR 31 ≠≠ 3419.

12. D.G. Cantor, An algorithm for finding the intersection of two Z-modules. Manuscript, Univ. of Calif., Los Angeles, 1970.

13. J.W.S. Cassels, The rational solutions of the Diophantine equation $y^2 = x^3 - D$. Acta Math. 82 (1950), 243-273. MR 12, 11; 84 (1951), 299. MR 12, 481.

14. J.A. Chang and H.J. Godwin, A table of irreducible polynomials and their exponents. Proc. Cambridge Philos. Soc. 65 (1969), 513-522. MR 38 ≠≠ 3249.

15. E.J. Cockayne, Computation of Galois group elements of a polynomial equation. Math. Comp. 23 (1969), 425-428. MR 39 ≠≠3733.

16. H. Cohn, Some experiments in ideal factorization on the MIDAC. J. Assoc. Comp. Mach. 2 (1955), 111-116. MR 16, 866.

17. _____ and S. Gorn, A computation of cyclic cubic units. J. Res. Nat. Bur. Standards 59 (1957), 155-168. MR 19, 732.

18. _____, A numerical study of Dedekind's cubic class number formula. J.Res. Nat. Bur. Standards 59 (1957), 265-271. MR 19, 944.

19. _____, A numerical study of units in composite real quartic and octic fields. Atlas Sympos. No. 2, Oxford, England, 1969.

20. J.H. Conway, Tabulation of some information concerning finite fields. "Computers in Math. Research", North-Holland, Amsterdam, 1968, 37-50. MR 38 ≠≠ 5749.

21. E.C. Dade, O. Taussky and H. Zassenhaus, On the semigroup of ideal classes in an order of an algebraic number field. Bull. Amer. Math. Soc. 67 (1961), 305-308. MR 25 ≠≠ 65.

22. _____, On the theory of orders, in particular on

the semigroup of ideal classes and genera of an order in an algebraic number field. Math Ann. 148 (1962), 31-64. MR 25 ≠≠ 3962.

23. E.C. Dade and H. Zassenhaus, How programming difficulties can lead to theoretical advances. Proc. Sympos. Appl. Math. XV, Amer. Math. Soc., Providence, R.I., 1963, 87-94. MR 28 ≠≠ 2662.

24. H. Davenport, Bases for finite fields. J. London Math. Soc. 43 (1968), 21-39. MR 37 ≠≠ 2729.

25. L. Elsner und H. Hasse, Numerische Ergebnisse zum Jacobischen Kettenbruchalgorithmus in rein-kubischen Zahlkörpern. Math. Nachr. 34 (1967), 95-97. MR 36 ≠≠ 2589.

26. E. Frank, Computer use in continued fraction expansions. Math. Comp. 23 (1969), 429-435. MR 39 ≠≠ 6815.

27. A. Fröhlich and J.C. Shepherdson, On the factorization of polynomials in a finite number of steps. Math. Z. 62 (1955), 331-334. MR 17, 119.

28. _____, Effective procedures in field theory. Philos. Trans. Roy. Soc. London, Ser. A 248 (1956), 407-432. MR 17, 570.

29. H.J. Godwin and P.A. Samet, A table of real cubic fields. J. London Math. Soc. 34 (1959), 108-110. MR 20 ≠≠ 7009.

30. _____, The determination of units in totally real cubic fields. Proc. Cambridge Philos. Soc. 56 (1960), 318-321. MR 22 ≠≠ 7998.

31. _____, The determination of the class-numbers of totally real cubic fields. Proc. Cambridge Philos. Soc. 57 (1961), 728-730. MR 23 ≠≠ A 3733.

32. H. Hasse, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern. Abh. Deutsch. Akad. Wiss. Berlin, Math.-Nat. Kl. (1948)2(1950), 95 pp. MR 11, 503.

33. _____, Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante -47. Acta Arith. 9 (1964), 419-434. MR 30 ≠≠ 3082; 16 (1969), 89-97. MR 40 ≠≠ 4237.

34. O. Hemer, Notes on the Diophantine equation $y^2 - k = x^3$. Ark. Mat. 3 (1954), 67-77. MR 15, 776.

35. A. Hollkott, Finite Konstruktion geordneter algebraischer Erweiterungen von geordneten Grundkörpern. Dissertation, Hamburg, Germany, 1941.

36. E.L. Ince, Cycles of reduced ideals in quadratic fields. Brit. Assoc. Advancement Sci., Math. Tables IV (1934). Zbl 10, 292.

37. K. Iwasawa and C.C. Sims, Computation of invariants in the theory of cyclotomic fields. J. Math. Soc. Japan 18 (1966), 86-96. MR 34 ≠≠ 2560.

38. H. Kempfert, On sign determination in real algebraic number fields. Numer. Math. 11 (1968), 170-174. MR 37 ≠≠ 1355.

39. H. Kempfert, On the factorization of polynomials. J. Number Theory 1 (1969), 116-120. MR 38 ≠≠ 6764.

40. S. Kuroda, Über die Zerlegung rationaler Primzahlen in gewissen nicht-abelschen Galoisschen Körpern. J. Math. Soc. Japan 3 (1951), 148-156. MR 13, 442.

41. H.W. Leopoldt, Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper. Abh. Deutsch. Akad. Wiss. Berlin, Math-Nat. Kl. (1953)2(1954), 48 pp. MR 16,799.

42. _____, Über ein Fundamentalproblem der Theorie der Einheiten algebraischer Zahlkörper. Bayer. Akad. Wiss., Math.-Nat. Kl., S.-B.,1956, 41-48 (1957). MR 19, 395.

43. _____, Klassenzahlen und Klassengruppen imaginär-quadratischer Zahlkörper mit Primzahldiskriminante $q \equiv -1 \bmod 4$. Manuscript, Univ. (TH) Karlsruhe, Germany.

44. W. Ljunggren, On the Diophantine equation $y^2 - k = x^3$. Acta Arith. 8 (1962/63 451-463. MR 28 ≠≠ 2082.

45. D.B. Lloyd, The use of finite polynomial rings in the factorization of the general polynomial. J. Res. Nat. Bur. Standards, Sect. B 69 (1965), 189-212. MR 32 ≠≠ 5643.

46. H. Matzat, Zahlentheoretische Programme und einige Ergebnisse. Manuscript, Univ. (TH) Karlsruhe, Germany, 1969.

47. R.J. Mc Eliece, Factorization of polynomials over finite fields. Math. Comp. 23 (1969), 861-868.

48. J.v. Neumann and B. Tuckerman, Continued fraction expansion of $2^{1/3}$. Math. Tables Aids Comp. 9 (1955), 23-24. MR 16, 961.

49. M. Newman, Bounds for class numbers. Proc. Symp. Math. VIII, 1965, Amer. Math. Soc., 70-77, Providence, R.I. MR 31 ≠≠ 4778.

50. _____, Tables of the class number h(-p) for p prime, $p \equiv 3 \pmod 4$, $101{,}987 \leq p \leq 166{,}807$. UMT 50, Math. Comp. 23 (1969), 683.

51. E.T. Ordman, Tables of class numbers for negative prime discriminants. UMT 29, Math. Comp. 23 (1969), 458.

52. V.D. Podsypanin, On the indeterminate equation $x^3 = y^2 + Az^6$. Mat. Sb., N.S., 24 (66) (1949), 391-403. MR 11, 81.

53. K.P. Popović, Integral polynomials irreducible mod p. Rev. Math. Pure Appl. 4 (1959), 369-379. MR 22 ≠≠ 4704.

54. E. Rowlinson and H. Schwerdtfeger, Polynomials with certain prescribed conditions on the Galois group. Canadian J. Math. 21 (1969), 262-273. MR 38 ≠≠ 5753.

55. K. Schaffstein, Tafel der Klassenzahlen der reellen quadratischen Zahlkörper mit Primzahldiskriminante unter 12,000 und zwischen 100,000-101,000 und 1,000,000-1,001,000. Math. Ann. 98 (1928), 745-748.

56. E.S. Selmer, Tables for the purely cubic field $K(\sqrt[3]{m})$. Avh. Norske Vid. Akad.Oslo I

1955, No. 5 (1956), 38pp. MR 18, 286.

57. E.S. Selmer, On Cassels' conditions for rational solubility of the Diophantine equation $\eta^2 = \xi^3 - D$. Arch. Math. Naturvid. 53 (1956), 115-137. MR 18, 285.

58. _____, The rational solutions of the Diophantine equation $\eta^2 = \xi^3 - D$ for $|D| \leq 100$. Math. Scand. 4 (1956), 281-286. MR 19, 120.

59. D.L. Smith, The calculation of simple continued-fraction expansions of real algebraic numbers. Master Thesis, Ohio State Univ., Columbus, 1969.

60. J. Sonn and H. Zassenhaus, On the theorem on the primitive element. Amer. Math. Monthly 74 (1967), 407-410. MR 35 ## 4201

61. H.M. Stark, On the "gap" in a theorem of Heegner. J. Number Theory 1 (1969), 16-27. MR 39 ## 2724.

62. _____, An explanation of some exotic continued fractions found by J. Brillhart. Atlas Sympos. No. 2, Oxford, England, 1969.

63. N.M. Stephens, The Diophantine equation $X^3 + Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer. J. Reine Angew. Math. 231 (1968), 121-162. MR 37 ## 5225.

64. _____, Completion of tables for $y^2 = x^3 + k$ $(-100 \leq k < 0)$ by a method of Ljunggren. Atlas Sympos. No. 2, Oxford, England, 1969.

65. J.D. Swift, Construction of Galois fields of characteristic 2 and irreducible polynomials. Math. Comp. 14 (1960), 99-103. MR 22 ## 2602.

66. H.P.F. Swinnerton-Dyer, An application of computing to class field theory."Algebraic Number Theory". Proc. Instructional Conf., Brighton, 1965, 280-291, Thompson, Washington D.C., 1967. MR 36 ## 2595.

67. _____, The conjectures of Birch and Swinnerton-Dyer, and of Tate. Proc. Conf. Local Fields, Driebergen, 1966, 132-157. Springer, 1967. MR 37 ## 6287.

68. J. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. Sem. Bourbaki 306 (1966), 1-26.

69. O. Taussky, Some computational problems in algebraic number theory."Survey of numerical analysis", ed. J. Todd, 549-557. Mc Graw-Hill, New York, 1962. MR 24 ## A 3149.

70. _____, A remark concerning Hilbert's Theorem 94. J. Reine Angew. Math. 239/240 (1969), 435-438.

71. _____, Hilbert's Theorem 94. Atlas Sympos. No. 2, Oxford, England, 1969.

72. W. Trinks, Ein Beispiel eines Zahlkörpers mit der Galoisgruppe $PSL(3, \mathbb{F}_2)$ über $\mathbb{Q}$. Diploma Thesis, Univ. (TH) Karlsruhe, Germany, 1968.

73. J.V. Uspensky, A method for finding units in cubic orders of a negative discriminant. Trans. Amer. Math. Soc. 33 (1931), 1-22. Zbl 1, 121.

74. H. Zassenhaus, The sum intersection method. Manuscript, Ohio State Univ., Columbus, 1966.

75. _____ and H. Kempfert, The modified algorithm for the maximal order over a commutative order. Manuscript, Ohio State Univ., Columbus.

76. _____, Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung. ISNM 7 (1967), 90-103. MR 37 ## 2720.

77. _____, The group of an equation. Nachr. Akad. Wiss. Göttingen II, Math.-Phys. Kl., 1967, Nr. 11, 147-166. MR 37 ## 5191.

78. _____, Über die Fundamentalkonstruktionen der endlichen Körpertheorie. Jahresber. Deutsch. Math. Ver. 70 (1968), 177-181. MR 39 ## 175.

79. _____, Continued fraction development of irrational real algebraic numbers. Manuscript, Ohio State Univ., Columbus, 1968.

80. _____ and J. Liang, On a problem of Hasse. Math. Comp. 23 (1969), 515-519. MR 40 ## 122.

81. _____, On Hensel factorization,I. J. Number Theory 1 (1969), 291-311. MR 39 ## 4120.

82. _____, A real root calculus. "Computational problems in abstract algebra", ed. J. Leech. 383-392. Pergamon, Oxford and New York, 1969.

83. H.G. Zimmer, Factorization of polynomials according to a method of Zassenhaus. Manuscript, Univ. of California, Los Angeles, 1969.

Additional reference:

84. D.G. Cantor, P.H. Galyean, and H.G. Zimmer, A continued fraction algorithm for real algebraic numbers. To appear.