NATIONAL BUREAU OF STANDARDS REPORT

3052

Some Computational Problems in Algebraic Number Theory

by

Olga Taussky

NBS

U. S. DEPARTMENT OF COMMERCE
NATIONAL BUREAU OF STANDARDS

U. S. DEPARTMENT OF COMMERCE
Sinclair Weeks, *Secretary*

NATIONAL BUREAU OF STANDARDS
A. V. Astin, *Director*

THE NATIONAL BUREAU OF STANDARDS

The scope of activities of the National Bureau of Standards is suggested in the following listing of the divisions and sections engaged in technical work. In general, each section is engaged in specialized research, development, and engineering in the field indicated by its title. A brief description of the activities, and of the resultant reports and publications, appears on the inside of the back cover of this report.

Electricity. Resistance Measurements. Inductance and Capacitance. Electrical Instruments. Magnetic Measurements. Applied Electricity. Electrochemistry.

Optics and Metrology. Photometry and Colorimetry. Optical Instruments. Photographic Technology. Length. Gage.

Heat and Power. Temperature Measurements. Thermodynamics. Cryogenics. Engines and Lubrication. Engine Fuels. Cryogenic Engineering.

Atomic and Radiation Physics. Spectroscopy. Radiometry. Mass Spectrometry. Solid State Physics. Electron Physics. Atomic Physics. Neutron Measurements. Infrared Spectroscopy. Nuclear Physics. Radioactivity. X-Rays. Betatron. Nucleonic Instrumentation. Radiological Equipment. Atomic Energy Commission Instruments Branch.

Chemistry. Organic Coatings. Surface Chemistry. Organic Chemistry. Analytical Chemistry. Inorganic Chemistry. Electrodeposition. Gas Chemistry. Physical Chemistry. Thermochemistry. Spectrochemistry. Pure Substances.

Mechanics. Sound. Mechanical Instruments. Aerodynamics. Engineering Mechanics. Hydraulics. Mass. Capacity, Density, and Fluid Meters.

Organic and Fibrous Materials. Rubber. Textiles. Paper. Leather. Testing and Specifications. Polymer Structure. Organic Plastics. Dental Research.

Metallurgy. Thermal Metallurgy. Chemical Metallurgy. Mechanical Metallurgy. Corrosion.

Mineral Products. Porcelain and Pottery. Glass. Refractories. Enameled Metals. Concreting Materials. Constitution and Microstructure. Chemistry of Mineral Products.

Building Technology. Structural Engineering. Fire Protection. Heating and Air Conditioning. Floor, Roof, and Wall Coverings. Codes and Specifications.

Applied Mathematics. Numerical Analysis. Computation. Statistical Engineering. Machine Development.

Electronics. Engineering Electronics. Electron Tubes. Electronic Computers. Electronic Instrumentation.

Radio Propagation. Upper Atmosphere Research. Ionospheric Research. Regular Propagation Services. Frequency Utilization Research. Tropospheric Propagation Research. High Frequency Standards. Microwave Standards.

Ordnance Development. Electromechanical Ordnance. Ordnance Electronics. These three divisions are engaged in a broad program of research and development in advanced ordnance. Activities include basic and applied research, engineering, pilot production, field testing, and evaluation of a wide variety of ordnance matériel. Special skills and facilities of other NBS divisions also contribute to this program. The activity is sponsored by the Department of Defense.

Missile Development. Missile research and development: engineering, dynamics, intelligence, instrumentation, evaluation. Combustion in jet engines. These activities are sponsored by the Department of Defense.

- Office of Basic Instrumentation
- Office of Weights and Measures.

NATIONAL BUREAU OF STANDARDS REPORT

NBS PROJECT **NBS REPORT**

1102-10-1104 January 15, 1954 3052

Some Computational Problems in Algebraic Number Theory

by

Olga Taussky

The preparation of this paper was supported (in part) under a contract between the National Science Foundation and the National Bureau of Standards.

NBS

U. S. DEPARTMENT OF COMMERCE
NATIONAL BUREAU OF STANDARDS

Some Computational Problems in Algebraic Number Theory

by

Olga Taussky

It is frequently claimed that many facts in ordinary number theory can be fully understood only through their generalization to algebraic number fields. A typical fact is the exceptional role played by the prime number 2 in many cases. However, in number fields one proves with ease that all numbers $1 - \zeta$ play an exceptional role when ζ is a root of unity. Another example is the quadratic law of reciprocity for which a really illuminating proof is only found by using number fields. Also the Fermat problem is frequently attacked via number fields.

However, the study of number theory in these fields provides its own difficulties and has still to deal with many open problems. Progress in this subject is particularly hindered by the greatly increased difficulties of numerical examples compared to the rational field.

In this brief report concerning computational problems in algebraic number theory only problems concerning the most fundamental concepts are mentioned. A list of table work concerning algebraic number fields - there is not much of it -

---

The preparation of this paper was supported (in part) under a contract between the National Science Foundation and the National Bureau of Standards.

can be found in Lehmer's Guide [1]. Many other problems have come up (see e.g. [2]).

1. Integral bases. It is known that for fields of degree ≥ 3 an integral base cannot always be found which consists of the powers of a single algebraic integer only. Although the existence of an integral base for any field is easily established, its construction presents difficulties (see e.g. [3]).

2. Factorization of rational primes in number fields. An ordinary prime number p will, in general, not remain a prime number in a given algebraic number field F, but split up into a product of powers of prime ideals:

$$p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} .$$

Apart from a finite number of primes p, namely the divisors of the discriminant of F, we have $e_i = 1$.

The question is: what are the possible values of r and of the e_i? Further, since norm $\mathfrak{p}_i = p^{f_i}$, what are the f_i? The laws which govern these numbers are not known to full extent in all fields. A great number of important facts are known about them and their structure is completely clarified in cyclotomic fields and their subfields. The extensions of class field theory to general algebraic extensions have not yet cleared up the decomposition laws of rational primes in arbitrary fields. So special numerical work in this

connection is very desirable. Recently Kuroda [4] computed some results concerning non-abelian fields of degree 2^n.

Like many other computations in algebraic number theory, the splitting of rational primes can be treated by <u>rational</u> methods only. This fact matters very much if computation by automatic computing machinery is considered. Only the knowledge of the irreducible polynomial f(x) a zero of which generates the field in question is needed.

For, the following facts hold for all but a finite number of primes [5]. Let

$$f(x) = P_1^{e_1} \dots P_r^{e_r} \quad (p)$$

where P_i is an irreducible polynomial mod p and $P_i \not\equiv P_k$ mod p, $i \neq k$. Then p splits up in the form

$$p = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$$

where $\mathfrak{p}_i \neq \mathfrak{p}_k$. If the degree of P_i is f_i then norm $\mathfrak{p}_i = p^{f_i}$.

Ö. Ore [6,7] extended the method just described to include all prime numbers by considering congruences mod p^r where r is sufficiently large.

3. <u>Units</u>. Other important problems arise in connection with the units in fields. To find the units is not always easy. The main problem is to find a set of base units.

In complex quadratic fields there are no units apart from roots of unity. In real quadratic fields there is one ε -

base unit ε and all other units are of the form $\pm\ \varepsilon^n$, $n = 0, \pm 1, \pm 2, \ldots$. If d is the discriminant of the field then the unit ε is of the form $(x + y\sqrt{d})/2$ where x, y are the smallest positive solutions of $(x^2 - dy^2)/4 = \pm 1$. There is a rational routine method for finding ε by means of continued fractions. It is being used on SEAC, the National Bureau of Standards Eastern Automatic Computer.

A routine method for finding a unit in cyclic cubic fields which together with its conjugates generates all the units was given by Hasse [8].

Units in non cyclic cubic fields were treated by several authors (see [9] where more references can be found, see also [1]).

Let $p > 2$, be a prime number. The base unit of the field generated by $\sqrt{p}$ can be put into the form $(t + u\sqrt{p})/2$. Recently Ankeny, Artin, Chowla [10] inquired whether $u \not\equiv 0(p)$. They verified this for $p = 5(8)$ and $p < 2000$. This conjecture was later verified by K. Goldberg on SEAC up to $p < 100{,}000$.

4. Ideal classes and class numbers. Tables for the class numbers of real quadratic fields have been made by Ince [11] and for the cyclic cubic fields by Hasse [8]. Hasse has a routine method for finding the class numbers in cyclic cubic fields, but it is rather complicated.

If no routine method is aimed at, the work is sometimes simpler. A bound for the class number and a method for com-

puting it is given by the known theorem:

In each class there is an ideal whose norm does not exceed $\sqrt{|d|}$ where d is the discriminant of the field. A sharper bound is $\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|}$, (see [12]). It is further known that

$$h\,K = \lim_{s \to 1} (s - 1)\,\zeta(s)$$

where h is the class number, and

$$K = \frac{2^{r_1}(2\pi)^{r_2}}{w} \frac{R}{\sqrt{|d|}} .$$

Here R is the regulator of the field, d the discriminant, w the number of roots of unity, r_1 the number of real conjugate fields, $2r_2$ the number of complex ones, and

$$\zeta(s) = \sum \frac{1}{(\text{norm}\ \mathfrak{a})^s},$$

where $\mathfrak{a}$ runs through all ideals in the field. [This sum converges for all s > 1].

Although this expression for the class number is very complicated it is yet very useful.

Further, there are many facts whose knowledge can cut down the work considerably in special cases. Quite a number of facts are known about the class number in cyclotomic fields and their subfields. These fields have been investigated more closely, partly because they are more accessible,

partly because of their importance to the Fermat problem. Many results concerning class numbers in these fields go back to Kummer and to H. Weber. Later P. Furtwängler [13,14] generalized some of their results, e.g., he proved that the class number of the field generated by the ℓ^r-th root of unity is divisible by ℓ if and only if the class number of the field generated by the ℓ-th root of unity is. Let further f, F be two subfields of the field of the ℓ^r-th root of unity and $f \subset F$. He then proved that the class number of f divides that of F. Recently a book by Hasse [15] appeared which is concerned with the class number in these fields and their largest real subfields. It contains many new theorems and tables.

A. Scholz [16], E. Inaba [17], O. Taussky [18] and others studied the subfields of prime degree ℓ of cyclotomic fields. The subfield of degree ℓ of the field generated by the p-th root of unity (p a prime $\equiv 1$ (ℓ)) has a class number prime to ℓ. On the other hand, a subfield of degree ℓ of the field generated by the $p_1 p_2$-th roots of unity has always a class number divisible by ℓ if $p_1 \equiv 1(\ell)$, $p_2 \equiv 1(\ell)$ are two different primes and if the field is not contained in the field of the p_1-th or the p_2-th roots of unity. The class number of such a field is not divisible by ℓ^2 if one, at least, of

the two congruences

$$x^{\ell} \equiv p_1(p_2), \quad x^{\ell} \equiv p_2(p_1)$$

has no rational solutions.

An example of such a case is $\ell = 3$, $p_1 = 7$, $p_2 = 13$. This means that the class number of a cubic subfield of the field of the 91-st root of unity (which is not a subfield of the field of the 7-th or 13-th root of unity) is divisible by 3, but not by 9. For one of these fields it will now be shown that its class number is actually 3.

It can easily be checked that

$$f(x) \equiv x^3 - 7.13x + 3\cdot 7\cdot 13 = 0$$

has discriminant $11^2\cdot 7^2\cdot 13^2$ and that any of its roots θ defines a cyclic cubic field whose discriminant is $7^2\cdot 13^2$. From a refinement of Minkowski's theory (see [19], also [12], p.452 for even sharper results [20]) it follows that for a cyclic cubic field with discriminant D there is in every ideal class an ideal $\mathfrak{n}$ such that

$$\text{norm}\,\mathfrak{n} \leq \frac{2}{9}\sqrt{D}.$$

In our case this gives norm $\mathfrak{n} \leq 20$. The prime numbers 3, 11, 19 split up into 3 factors in the field while 2,5,17 remain prime numbers. It is therefore only necessary to examine in what classes the prime ideal factors of 3,11,19 lie. Since

the class number is divisible by 3, but not by 9, only the class numbers 3, 6, 12, 15 come in question. The class numbers 6 or 15 are impossible, since in such a case the 2-class group or the 5-class group of the field would have to be cyclic. In this case let $\mathfrak{y}$ be a prime ideal belonging to a class of order 2 or 5. Let e.g., the 2-class group be cyclic. In this case we would have

$$\mathfrak{y}^{s} \sim \mathfrak{y}^{a}$$

where s is a generating automorphism of the Galois group of the field and a is a rational integer. Hence

$$\mathfrak{y}^{s^3} \sim \mathfrak{y}^{a^3}.$$

This implies $a^3 \equiv 1(2)$ which implies $a \equiv 1(2)$. This means that $\mathfrak{y}^3 \sim 1$ and hence $\mathfrak{y} \sim 1$. The same argument applies for the 5-class group.

In order to show that the class number 12 cannot occur, we prove that the prime numbers 3, 11, 19 are norms of numbers or their third powers are. For this purpose we compute the norms of some numbers $x + y\theta$ by means of the formula:

$$\text{norm } (x + y\theta) = x^3 - ax^2y + bxy^2 - cy^3$$

$$\text{if} \quad \theta^3 + a\theta^2 + b\theta + c = 0.$$

We obtain:

$$\text{norm } (1 + \theta) = -3 \cdot 11^2$$

$$\text{norm } (2 - \theta) = 3^2 \cdot 11$$

$$\text{norm } (5 - \theta) = -3 \cdot 19$$

$$\text{norm } (3 - \theta) = 3^3.$$

These facts imply that the class number of the field is 3.

A treatment by rational methods is also possible for the classes, at least in many cases [21], [22], [23]. If the field admits an integral base which consists of the powers of a single number, then there is a 1-1 correspondence between the ideal classes and the classes of nxn matrices $S^{-1}AS$ where A is a fixed matrix with $f(A) = 0$. The elements a_{ik}, s_{ik} in $A = (a_{ik})$, $S = (S_{ik})$ are rational integers and S runs through all matrices with $|S| = \pm 1$.

In complex quadratic fields the class number exceeds unity apart from a finite number of cases. This was conjectured by Gauss and proved by Heilbronn [24]. He also proves with Linfoot [25] that for $m > 163$, at most one further m is possible such that the field $F(\sqrt{m})$ has class number unity. It is still an open question whether there is a further m. Work by Lehmer [26] indicates that probably no further m exists.

For class numbers in non-cyclic cubic fields, see again [1] and [9].

5. Principal idealization.

A rather complicated computation concerns

the application of the following famous theorem of Hilbert ([27], theorem 94, Zahlbericht). Let f be a field and F a relatively cyclic extension of relative degree ℓ of f (ℓ is a prime number). Let all prime ideals of f split up in F into different prime ideals. Then there exists an ideal in f which is not a principal ideal in f, but which is principal in F. Further, that ideal in f lies in a class of order ℓ and the class number of f is divisible by ℓ.

If the class group of f is cyclic then there is no further problem, but if the class group has at least 2 base classes then the following problem arises:

Given such an f and F, which class of f is the one that does go over into the principal class in F?

If f is a quadratic field $R(\sqrt{m})$ and $\ell = 2$ this is not too difficult. However, if $\ell = 3$ the difficulties increase. In the first place: one has to go a long way to find a field with 3-class number $\geqq 9$ and non-cyclic class group. The first imaginary quadratic field with this property is $F(\sqrt{-3299})$. It has 3-class number 27. A field with 3-class number 9 and non-cyclic class group is $F(\sqrt{-4027})$. Also for this problem a rational method was found to succeed (see [23], [29]).

BIBLIOGRAPHY

1. D. H. Lehmer, Guide to tables in the theory of numbers, National Research Council, Washington, D. C., 1941.

2. J. von Neumann and H. H. Goldstine, A numerical study of a conjecture by Kummer, MTAC, vol. 7(1953), pp. 133-134.

3. M. Hall, Indices in cubic fields, Bull. Amer. Math. Soc., vol. 43(1937), pp. 104-108.

4. S. Kuroda, Über die Zerlegung rationaler Primzahlen in gewissen nichtabelschen Körpern, Math. Soc. Japan Jn., vol. 3(1951), pp. 148-156.

5. R. Dedekind, Gesammelte math. Werke I, Vieweg and Sohn, Braunschweig, 1930, pp. 202-232.

6. Ö. Ore, Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Zahlkörpern (Erste Mitteilung), Math. Annalen, vol. 96(1927), pp. 313-352.

7. Ö. Ore, Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Zahlkörpern (Zweite Mitteilung) Math. Annalen, vol. 97(1927), pp. 569-598.

8. H. Hasse, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern, Abh. d. deutsch, Akad.d.Wiss.,Math.-naturw. Klasse, Jahrgang 1948, No. 2, Berlin, 1950.

9. J.W.S. Cassels, The rational solutions of the diophantine equation $Y^2 = X^3 - D$ Acta Math., vol. 82(1950), pp. 243-273.

10. N. C. Ankeny, E. Artin, S. Chowla, The class number of real quadratic number fields, Annals of Math., vol. 56(1952), pp. 479-493.

11. E. L. Ince, Cycles of reduced ideals in quadratic fields, British Association for the Advancement of Science, Math. Tables IV, London, 1934.

12. H. Hasse, Zahlentheorie, Akademie-Verlag, Berlin, 1949.

13. P. Furtwängler, Über die Klassenzahlen Abelscher Zahlkörper, Journ. reine angew. Math., vol. 134 (1908), pp. 91-95.

14. P. Furtwängler, Über die Klassenzahlen der Kreisteilungskörper, Journ. reine angew. Math., vol. 140 (1941), pp. 29-32.

15. H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.

16. A. Scholz, Zwei Bemerkungen zum Klassenkörperturm, Journ. reine angew. Math., vol. 161(1929), pp. 201-207.

17. E. Inaba, Über die Struktur der ℓ-Klassengruppe zyklischer Zahlkörper vom Primzahlgrad ℓ, Journ. Fac. Sci., Imp. Univ. Tokyo, vol. IV 2(1940), pp. 61-115.

18. O. Taussky, A remark on unramified class fields, J. London Math. Soc., vol. 12(1937), pp. 86-88.

19. H. Minkowski, Dichteste gitterförmige Lagerung kongruenter Körper, Gött. Nachr. 1904, pp. 311-355.

20. H. Davenport, Note on the product of three homogeneous linear forms, J. London Math. Soc., vol. 16 (1941), pp. 98-101.

21. O. Taussky, On a theorem of Latimer and MacDuffee, Can. J. Math., vol. 1(1949), pp. 300-302.

22. O. Taussky, Classes of matrices and quadratic fields, Pac. J. of Math., vol. 1(1951), pp. 127-132.

23. O. Taussky, Classes of matrices and quadratic fields II, J. London Math. Soc., vol. 27(1952), pp. 237-239.

24. H. Heilbronn, On the class-number in imaginary quadratic fields, Quart. J. Math. Oxford, vol. 5(1934), pp. 150-160.

25. H. Heilbronn and E. H. Linfoot, On the imaginary quadratic corpora of class-number one, Quart. J. Math. Oxford, vol. 5(1934), pp. 293-301.

26. D. H. Lehmer, On imaginary quadratic fields whose class number is unity, Bull. Amer. Math. Soc., vol. 39(1933), p. 360.

27. D. Hilbert, Gesammelte Abhandlungen I, Springer, Berlin, 1932.

28. A. Scholz and Olga Taussky, Die Hauptideale der kubischen Klassenkörper imaginär quadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluss anf den Klassenkörperturm, J. reine angew. Math., vol. 171(1934), pp. 19-41.

29. O. Taussky, Arnold Scholz zum Gedächtnis, Math. Nachr., vol. 7(1952), pp. 374-386.

National Bureau of Standards
Washington, D. C.

THE NATIONAL BUREAU OF STANDARDS

Functions and Activities

The functions of the National Bureau of Standards are set forth in the Act of Congress, March 3, 1901, as amended by Congress in Public Law 619, 1950. These include the development and maintenance of the national standards of measurement and the provision of means and methods for making measurements consistent with these standards; the determination of physical constants and properties of materials; the development of methods and instruments for testing materials, devices, and structures; advisory services to Government Agencies on scientific and technical problems; invention and development of devices to serve special needs of the Government; and the development of standard practices, codes, and specifications. The work includes basic and applied research, development, engineering, instrumentation, testing, evaluation, calibration services, and various consultation and information services. A major portion of the Bureau's work is performed for other Government Agencies, particularly the Department of Defense and the Atomic Energy Commission. The scope of activities is suggested by the listing of divisions and sections on the inside of the front cover.

Reports and Publications

The results of the Bureau's work take the form of either actual equipment and devices or published papers and reports. Reports are issued to the sponsoring agency of a particular project or program. Published papers appear either in the Bureau's own series of publications or in the journals of professional and scientific societies. The Bureau itself publishes three monthly periodicals, available from the Government Printing Office: The Journal of Research, which presents complete papers reporting technical investigations; the Technical News Bulletin, which presents summary and preliminary reports on work in progress; and Basic Radio Propagation Predictions, which provides data for determining the best frequencies to use for radio communications throughout the world. There are also five series of nonperiodical publications: The Applied Mathematics Series, Circulars, Handbooks, Building Materials and Structures Reports, and Miscellaneous Publications.

Information on the Bureau's publications can be found in NBS Circular 460, Publications of the National Bureau of Standards ($1.00). Information on calibration services and fees can be found in NBS Circular 483, Testing by the National Bureau of Standards (25 cents). Both are available from the Government Printing Office. Inquiries regarding the Bureau's reports and publications should be addressed to the Office of Scientific Publications, National Bureau of Standards, Washington 25, D. C.

NBS