UNIQUENESS OF THE DECOMPOSITION INTO PRIME FACTORS IN QUADRATIC NUMBER FIELDS.

GEORG RABINOWITSCH, ODESSA

In his dissertation, Jakob Schatunowski[1] has shown that the Euclidean algorithm for the greatest common divisor in quadratic number fields with discriminant of the form $D = 1 - 4m$, where $m > 3$, generally doesn't reach its goal; he has given there another algorithm which is applicable to all the quadratic number fields in which each integer can only be expressed in one way in terms of prime numbers[2] (I will call in the sequel such a number field a simple field). Encouraged by this work, I also tried to find such an algorithm by generalizing Euclid's algorithm, as we know one step of the Euclidean algorithm is to replace the pair of numbers a, b by the pair of numbers b, r where r is the remainder of the division of a by b, i. e. a number of the form $a - by$, which is absolutely smaller than b. Both pairs have the same common divisors. In some quadratic fields, however, it is not always possible, if α and β are given, to find an integer η such that $\alpha - \beta\eta$ is less than β in norm. So, I tried to take a number of the form $\alpha\xi - \beta\eta$ and to choose the numbers ξ and η such that, first, the inequality

$$N(\alpha\xi - \beta\eta) < N(\beta)$$

and the two pairs $\{a, \beta\}$, and $\{\beta, \alpha\xi - \beta\eta\}$ have the same common divisors. It turned out that fulfilling the first requirement, i. e., the solvency of the inequality, can serve as a characteristic condition of simplicity (in the sense defined above) of a field. The necessity of this condition is proved in §4 of this article, where the algorithm is also discussed and the equation of the greatest common divisor is established. It §1 it will be shown that this condition is sufficient, and in §2 and §3 I deal with another characteristic condition, which leads the question of the simplicity of a quadratic number field to a question about the distribution of (rational) primes. In the following, Latin letters always denote rational numbers, Greek always (in general) irrationals. A fraction is never called a letter. For the conjugation of α, the name $\bar{\alpha}$ is used. $N\alpha$ denotes the norm of the integer α.

1. A condition for simplicity.

Lemma 1. *In a non-simple field, there is a number which is divisible by a prime number π, but which can be represented as a product of two factors, none of which is divisible by π.*

Date: 1913.

I SUMMARIZED THE MAIN RESULTS OF THIS WORK IN A LECTURE WHICH I DELIVERED AT THE 5TH INTERNATIONAL CONGRESS OF MATHEMATICIANS AT CAMBRIDGE IN AUGUST 1912.

[1] "The greatest common divisor of second-order algebraic numbers with negative discriminant and the decomposition of these numbers into prime factors." Leipzig, 1912.

[2] Here, as in the mentioned lecture, "prime number" denotes one integer of the field, which is not divisible by any other integer of the field except the units.

Proof. A non-simple field is one in which the decomposition into prime factors is not always unique. In such a field, therefore, there must be an integer which can be decomposed into two different strings of primes. It may happen that the same prime numbers occur in the two decompositions, but there is certainly a prime number π which occurs in one decomposition more often than in the second (otherwise both decompositions were identical). If we consider all the remaining primes of the second decomposition (or, if π does not occur in the second decomposition, all primes of this decomposition), then their product $\sigma_1 \cdot \sigma_2 \cdot \sigma_3 \cdots$ must be divisible by π. We now split these prime numbers into two groups and form the products of the primes of each group. It may happen that neither of these partial products are divisible by π, then the product of these products, i. e. $\sigma_1 \cdot \sigma_2 \cdot \sigma_3 \cdots$ is the sought number. But if a subproduct $\sigma_1' \cdot \sigma_2' \cdot \sigma_3' \cdots$ is divisible by π, then we proceed with it the same way as with the original product $\sigma_1 \cdot \sigma_2 \cdot \sigma_3 \cdots$. We thus obtain a sequence of products $\sigma_1 \cdot \sigma_2 \cdot \sigma_3 \cdots$, $\sigma_1' \cdot \sigma_2' \cdot \sigma_3' \cdots$, $\sigma_1'' \cdot \sigma_2'' \cdot \sigma_3'' \cdots$, which are all divisible by π and each of which consists of fewer primes than the previous one. If we did not find the number we were looking for earlier, then we must come finally to a product of two primes, neither of which is equal to π, but whose product is divisible by π. This is the sought number. □

Theorem 1. *If it is possible, whenever two integers α and β of a field are given, neither of which is divisible by the other, to find two integers ξ and η of the same field, such that the inequality*

$$0 < N(\alpha\xi - \beta\eta) < N\beta \tag{1}$$

then the field is simple.

Proof. In a non-simple field, the proposition provides products of two factors which are divisible by some prime integer π, without either of factors being so. If we consider the norms of our products which have this property with respect to π, then there must be a smallest among these norms (since the norms are all rational numbers). Let $\lambda \cdot \Lambda$ be the one of the products that has this smallest norm. According to the hypothesis, two numbers ξ and η must exist with the property that the number

$$\mu = \pi\xi - \lambda\eta \tag{2}$$

satisfies the two conditions

$$N\mu < N\pi \tag{3}$$

and

$$N\mu < N\lambda. \tag{4}$$

If we multiply equation (2) by Λ, we get that

$$\mu\Lambda = \pi\xi\Lambda - \lambda\Lambda \cdot \eta.$$

Since $\lambda\Lambda$ is divisible by π, so is $\mu\Lambda$. Furthermore, neither of the two factors is divisible by π (μ because of the inequality (3), Λ because it is also a factor of the product $\lambda \cdot \Lambda$). So $N(\mu \cdot \Lambda)$ is one of the norms among which $N(\lambda \cdot \Lambda)$ is the smallest. We have because of (4)

$$N(\mu \cdot \Lambda) = N\mu \cdot N\Lambda[3] < N\lambda \cdot N\Lambda,$$

so

$$N(\mu \cdot \Lambda) < N(\lambda \cdot \Lambda).$$

[3] Typo corrected from the original here, where lowercase λ appears at this character.

This contraction proves the theorem. □

If we call two integers, neither of which is divisible by the other, and which have the property that the inequality (1) has no solutions a *disturbing pair* of integers, then we can also state the theorem just proved in the following way: In a non-simple field there is at least one disturbing pair of integers. If we divide both sides of the inequality (1) by $N\beta$ (as Mr. Schatunowsky does in a similar case), we get that

$$0 < N(\frac{\alpha}{\beta}\xi - \eta) < 1. \tag{5}$$

We can also say that in non-simple field must give *disturbing fractions.* Here we call a fraction $\frac{\alpha}{\beta}$ disturbing if it is impossible to satisfy the inequality (5).

It is immediately clear that if $\frac{\alpha}{\beta}$ is disturbing fraction, then the fraction $\frac{\alpha}{\beta} + \xi$ is also disturbing.

Further, if there is a disturbing fraction $\frac{\alpha}{\beta}$, an integer ξ, and $\frac{\alpha}{\beta}\xi$ is not an integer, then $\frac{\alpha}{\beta} \cdot \xi$ is a disturbing fraction.

2. The simplest disturbing fraction.

We now use the last two results to find the simplest among the disturbing fractions. This happens in the following.

Theorem 2. *In a non-simple field, there is at least one disturbing fraction of the form*

$$\frac{p-\theta}{q},$$

where $p < q$ and q is prime.

Proof. Since the field is not simple, a disturbing fraction must occur in it. By multiplying its two terms by the conjugate of the denominator, we can give this fraction the form

$$\frac{P + R\theta}{q}.$$

In doing so, we consider the possible shared rational divisors of numerator and denominator; the numbers P, R and q have no common divisors. (In what follows, when we speak of divisors of rational numbers, we mean rational divisors, and when we speak of a rational number as a prime number, it means that it has no rational divisors, etc.) We can further assume that q is a prime, because if it were not, we could make it so by multiplying the fraction by a suitable integer.

1. We first prove that R and q are relatively prime numbers. For this purpose we denote by d the greatest common divisor of these numbers and form the expression

$$\frac{P + R\theta}{q} \cdot \frac{q}{d} = \frac{P + R\theta}{d} = \frac{P}{d} + \frac{R}{d}\theta.$$

Suppose that d is different from 1, then P is not divisible by d (otherwise the numbers P, R, and q would have a common divisor). The written expression is a fraction. On the other hand, $\frac{q}{d}$ is also an integer. So this fraction is disturbing (see end of §1). Further, $\frac{R}{d}\theta$ is also an integer, so the fraction

$$\frac{P + R\theta}{d} - \frac{R}{d}\theta = \frac{P}{d}$$

is disturbing as well. But that can not be the case because it is a rational fraction. (If $\frac{\alpha}{\beta}$ is a rational fraction and y the largest integer contained in it[4], we need only set $\xi = 1$, $\eta = y$, to satisfy the inequality (5)) So our assumption is false, d is equal to 1, and the numbers R and q are relatively prime.

2. It follows that there are two numbers, x and y, that satisfy the equation

$$Rx - qy = -1.$$

Let us form the expression

$$\frac{P + R\theta}{q}x - y\theta = \frac{Px + (Rx - qy)\theta}{q} = \frac{Px - \theta}{q},$$

so it is again a disturbing fraction.

3. Now we divide Px by q and denote the quotient by z and the (positive) remainder with p. Then, too, is

$$\frac{Px - \theta}{q} - z = \frac{p - \theta}{q}$$

a disturbing fraction. Here $p < q$, so the statement is proved. □

Everything that has been said so far applies to every quadratic field. From now on, we restrict ourselves to fields with (negative) discriminants of the form

$$D = 1 - 4m$$

If we designate

$$\theta = \frac{1 + \sqrt{D}}{2},$$

it is known that every integer of the field can be represented as $\xi = x + y\theta$, and conversely, each number of this form is an integer of the field. The norm of this integer is

$$N\xi = x^2 + xy + my^2.$$

If a fraction is disturbing, its norm is not less than 1, otherwise the numbers $g = 1$, $\eta = 0$ would satisfy the inequality (5). If the fraction $\frac{p-\theta}{q}$ is disturbing, then we have the inequality

$$\frac{p^2 - p + m}{q^2} \geq 1$$

or

$$p^2 - p + m \geq q^2.$$

If q is still greater than p, then a fortiori there is the inequality which we obtain from this, if we replace p with q:

$$q^2 - q + m > q^2.$$

But from this follows $q < m$. So we proved the following statement:

Theorem 3. *If a fraction of the form $\frac{p-\theta}{m}$ is disturbing (and is $p < q$), then also $q < m$. (The condition in parentheses is, as it's easy to show, superfluous.)*

Now we can instead say of Theorem 2:

[4] Here, the author seems to mean the floor of the absolute value of $\frac{\alpha}{\beta}$, with sign matching that of the fraction.

Theorem (2^{a}). *In a non-simple field, there is at least one disturbing fraction of the shape*

$$\frac{p-\theta}{q},$$

where $p < q < m$ and q is prime.

Here, I like to point out again that theorem 2 applies in all quadratic fields; theorem 2^{a} applies only in quadratic fields with the discriminant $D = 1 - 4m$.

3. The test numbers.

With our previous result we can also say a field is simple if among the fractions

$$\frac{p-\theta}{q}, \qquad (p < q < m)$$

none are disturbing.

So, we have a closer look at these fractions. The norms of the numerators of these fractions are the $m - 2$ numbers,

$$p^2 - p + m. \qquad (p = 1, \dots, m-2)$$

If $p^2 - p + m$ is a prime number, then the numbers $p^2 - p + m$ and q are either equal to each other or relatively prime. The first one can not be the case, otherwise the fraction would have the norm $\frac{1}{q}$[6] and consequently the fraction would not be disturbing; so the second one holds, and there are two numbers, x and y, such that the equation

$$(p^2 - p + m)x - qy = 1$$

is satisfied. The number $p^2 - p + m$, however, is the norm of the number $p - \theta$, i. e. equal to the product of this number with its conjugate $p - \bar{\theta}$. So we can put the equation just written in the form

$$\frac{p-\theta}{q} \cdot (p - \bar{\theta})x - y = \frac{1}{q}$$

and in this form it shows (see inequality (5)), that the fraction $\frac{p-\theta}{q}$ is not disturbing, because the norm of $\frac{1}{q}$ is $\frac{1}{q^2}$, which is smaller that 1. From what has been said follows:

Theorem 4. *The fraction $\frac{p-\theta}{q}$, where $p < q < m$ and q is prime, can not be disturbing if the number $p^2 - p + m$ is a prime number.*

If all such numbers are prime numbers, then there are no disturbing fractions of the form $\frac{p-\theta}{q}$, where $p < q < m$ and q is a prime number. But according to theorem 2^{a}, in every non-simple field such fractions must be present, giving:

Theorem 5. *If all numbers*

$$p^2 - p + m \qquad (p = 1, \dots, m-2)$$

are prime, then the field with the discriminant $D = 1 - 4m$ is simple.

[6] The norm of q is q^2.

We will now examine the case where not all of these numbers are primes to see if the inverse of this proposition holds. But before we go over to it, we have to prove the following two lemmas.

Lemma 2. *The norm of an irrational number can not be less than m.*

Proof. The proof is based on the following two obvious facts. First, the sum of two positive integers can exceed their product by at most 1. Second, if x, y are two integers and y is different from 0, then

$$x^2 + xy + y^2 \geq 1.$$

If we take our irrational number of the form $x + y\theta$, then its norm is $x^2 + xy + my^2$, and y is not equal to zero here (otherwise the number would not be irrational), so y^2 is positive. Now, by applying the two said facts, we get

$$x^2 + xy + my^2 > x^2 + xy + m + y^2 - 1$$

$$x^2 + xy + y^2 - 1 + m > m.$$

From these inequalities follows the statement. □

We only need this to help prove the following.

Lemma 3. *If $p < m$, then $p - \theta$ is a prime number.*

Proof. The number $p - \theta$ can not have a rational divisor; if it were composite, then it could be represented as a product of two irrational numbers. The product of the norms of these numbers would be equal to $N(p - \theta) = p^2 - p + m$, which is smaller than m^2. One of these numbers should therefore have a norm which is smaller than m which is impossible according to lemma 2. So the statement is proved. □

With the help of this theorem we will now investigate the case where not all numbers $p^2 - p + m$ are prime numbers. This happens in the following:

Theorem 6. *If one of the numbers*

$$p^2 - p + m \qquad (p = 1, \ldots, m - 1)$$

is (rationally) composite, then the field with the discriminant $D = 1 - 4m$ not simple.

Proof. It suffices to find a number which can be decomposed into two different collections of primes. Such is the one of the numbers $p^2 - p + m$ which is rationally composed. It decomposes, on one hand, into the factors $p - \theta$ and $p - \bar{\theta}$, which are primes according to the just-proved lemma, and on the other hand, it decomposes according to the hypothesis into rational factors, so that we have an equation of the form

$$(p - \theta)(p - \bar{\theta}) = abc \cdots.$$

Here a, b, c, ... do not need to be primes of our field, but it is clear that if we continue to divide them, we will have a different decomposition on the right than on the left. □

From theorems 5 and 6 we see that the numbers

$$p^2 - p + m \qquad (p = 1, \ldots, m-1)$$

play a major role in deciding the question of the simplicity of a field. It is therefore convenient to have a special name for them, and it seems fitting to call them *test* numbers of the field with the discriminant $D = 1 - 4m$. On the basis of theorems 5 and 6 we can then pronounce the following characterization:

A field is simple or not depending on whether or not all of the test numbers are prime.

This characterization allows the question of whether a given field is simple to be resolved very quickly! To make the calculation of the test numbers more convenient, we notice that the difference between two consecutive test numbers is the form

$$(x+1)^2 - (x+1) + m - x^2 + x - m = 2x,$$

and we can therefore calculate these numbers successively according to the formula

$$m_{i+1} = m_i + 2i, \quad m_1 = m. \tag{6}$$

For $m = 17$, we get e. g.: $m_1 = 17$, $m_2 = 17 + 2 = 19$, $m_3 = 19 + 4 = 23$, $m_4 = 23 + 6 = 29$, $29 + 8 = 37$, $37 + 10 = 47$, $47 + 12 = 59$, $59 + 14 = 73$, $73 + 16 = 89$, $89 + 18 = 107$, $107 + 20 = 127$, $127 + 22 = 149$, $149 + 24 = 173$, $173 + 26 = 199$, $199 + 28 = 227$, $227 + 30 = 257 = m_{16}$. All these numbers are prime numbers, so the field with the discriminant $D = 1-4\cdot17 = -67$ is a simple field. In addition to the number 17, the numbers 2, 3, 5, 11, 41 have the same property[8]. It is, as far as I know, unknown, if there are more such numbers. The number fields with the corresponding discriminants -7, -11, -19, -43, -67, -163 are also known as the only simple fields of their kind[9]. For all values of m other than 2, 3, 5, 11, 17, 41, there are, it seems, always composite numbers among the test numbers. If m is composite, we need not form any other test numbers, for m is itself the first test number. If m is a prime number and its last digit is 3, then m_2 is divisible by 5, so composite; if the last digit is 9, then m_3 will be. If m is a prime whose last digit is 1 or 7, then we must use the formula (6) and check the numbers obtained for their compositeness. In most cases, we quickly come up with composite numbers.

Not only does this method allow for the simplicity of a given field to be decided, it is also quite easy to determine, with a table of primes in hand, that among the fields with the discriminant $D = 1 - 4m$, where m is below a given limit (e. g. 6000), apart from the previously mentioned ones there are no simple fields. But the questions of whether there are any more such fields, and whether they are finite or infinite in number, have not been solved in this way, and we must content ourselves with having recognized the equivalence of the following two questions:

(1) Is the number of simple quadratic fields with a negative discriminant of the form $D = 1-4m$ finite or infinite?
(2) Is there a finite or an infinite number of numbers m, which have the property that all numbers

$$x^2 - x + m \qquad (x = 1, \ldots, m-1).$$

are primes?

[8] This property of the numbers 41 and 17 was already known by *Euler* (Mémoires de Berlin, 1772, p. 36) and *Legendre* (Thèorie des Nombres, 1830, p. 13).

[9] See *H. Weber*, Algebra, Vol. 3, 1908, p. 460.

Before we move on, I would like to point out a side result. Theorem 6 represents, in fact, more than a converse of theorem 5. It deals with all $m-1$ test numbers, instead of (in theorem 5) only the first $m-2$ of them. So the matter is this: if the first $m-2$ test numbers are primes, the field is simple; but if the field is simple, then all test numbers, including the last one, are prime numbers. So, if we leave the quadratic fields aside, we can pronounce the following sentence:

If the numbers

$$x^2 - x + m \qquad (x = 1, \dots, m-2)$$

are primes, so is the number

$$(m-1)^2 - (m-1) + m = m2 - 2m + 2.$$

4. The algorithm.

With the help of the results obtained in §2 and §3, it is possible to prove the converse of theorem 1.

Theorem 7. *When in a simple field two integers α and β are given, neither divisible by the other, it is always possible to find in the same field two integers ξ and η such that the inequality*

$$0 < N(\alpha\xi - \beta\eta) < N\beta$$

is satisfied.

Proof. If the inequality could not be solved, the pair α, β would become a disturbing one, and $\frac{\alpha}{\beta}$ would represent a disturbing fraction. If we treat this fraction exactly as in the proof of theorem 2, thus we obtain a disturbing fraction of the form $\frac{p-\theta}{q}$, where $p < q < m$. By theorem 4, $p^2 - p + m$ would then be a composite number, and according to theorem 6, the field would not be simple, which contradicts the hypothesis of the theorem to be proved. □

Thus we have proved that in a simple field the inequality (1) is solvable, and in the preceding (namely, in the proof of theorems 2 and 4), a method is given to actually calculate the numbers ξ and η when the numbers α and β are given. Now, the resolution of this inequality was originally intended as a step in an algorithm that has to replace the Euclidean algorithm. First, however, the calculations that lead to the actual solution of (1) are generally not very simple, and second, there are further complications from the fact that the numbers ξ and η must satisfy another requirement beyond this inequality, which is that the pairs a, β and β, $\alpha\xi - \beta\eta$ have the same common divisors. But if the procedure is unusable for practical purposes[11], it theoretically does the same thing that division does with the remainders of rational numbers, namely, it makes it possible to establish the equation of the greatest common divisor. We now want to examine this more closely.

We consider all numbers of the form $\alpha\xi - \beta\eta$. Among the norms of these numbers, there must be a smallest. If δ is one of these numbers, which has the smallest norm, then it is easy to show that δ divides

[11] It often happens that the number found for ξ is relatively prime to β, then, as you can easily see, the requirement is self-fulfilling. Sometimes, if this is the case in all steps, then it can be really quite quick to find the greatest common divisor.

each of the two numbers α and β. For if δ is not a divisor of α, for example, then there are two numbers ζ and τ such that

$$N(\alpha\zeta - \delta\tau) < N\delta$$

is. But the number $\alpha\zeta - \delta\tau$ is equal to $\alpha(\zeta - \tau\xi) + \beta\tau$, so it is again a number of the form $\alpha\xi - \beta\eta$, and its norm can not be smaller than $N\delta$. So δ is a common divisor of α and β, and every other divisor of these numbers divides

$$\delta = \alpha\xi - \beta\eta,$$

so δ is the greatest common divisor. The equation just described thus represents the equation of the greatest common divisor.

Hence, if α and β are non-prime numbers of a simple field, the equation

$$\alpha\xi - \beta\eta = 1$$

has solutions.