On the Numbers of the Form $x^2 + 11y^2$

joint work with Martin Kreuzer

Gerhard Rosenberger
gerhard.rosenberger@math.uni-hamburg.de

University of Hamburg

Medford 2020

Topics

Topics

Introduction

L. Euler considers *convenient numbers*, that is, numbers N for which a positive integer n has a unique representation of the form

$$n = x^2 + Ny^2 \text{ with } \gcd(x^2, Ny^2) = 1 \text{ if and only if } n \text{ is a prime,}$$

a prime power, twice one of these, or a power of 2. The set of known convenient numbers, that is, the set

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, \ldots, 1848\}$$

consists of 65 numbers, and it is conjectured that these are all of them. When we look at this set, we see that 11 is the first *inconvenient* number. So, it is a natural question to ask which positive integers have a representation of the form $n = x^2 + 11y^2$ with $\gcd(x, 11y) = 1$, and when this representation is unique.

Introduction

For the study of prime numbers of the form $p = x^2 + Ny^2$, there is a huge literature, and many deep results have been found. In particular, using these results, we can characterize prime numbers of the form $p = x^2 + 11y^2$ as in Theorem 29.
However, for general positive integers of the form $n = x^2 + 11y^2$, much less seems to be known. An algorithm for computing such a representation, if it exists, is given by Özgür, but no characterization is given when such a representation exists. One reason for these difficulties may be that, since the quadratic form $x^2 + 11y^2$ has discriminant -44 and its form class number is $h(-44) = 3$, one should not expect simple congruence relations that decide whether n is or is not of the form $n = x^2 + 11y^2$.

In another vein, B. Fine proved Fermat's two-square theorem, that is, the characterization of primes representable by $x^2 + y^2$, using the modular group $\mathrm{PSL}_2(\mathbb{Z})$. The second author, together with G. Kern-Isberner, extended this method to all forms $x^2 + Ny^2$ such that $h(-4N) \leq 2$ and $N \neq 15$. In particular, they showed that, in these cases, one may in essence characterize numbers of the form $x^2 + Ny^2$ by the conditions that $-N$ is a quadratic residue modulo n, that n is a quadratic residue modulo N, and possibly a simple congruence condition. This approach met with some obstacles for the convenient number $N = 15$, because the underlying class group G_{15} has a more complicated structure. Notwithstanding such impediments, we attempt to generalize these group theoretic methods further to the first *inconvenient* case $N = 11$, and the central idea by Kern-Isberner and Rosenberger of the current paper is to follow the approach in order to deduce as many results about positive integers of the form $n = x^2 + 11y^2$ as possible.

Let us have a closer look at the contents of the paper. In Section 2 we lay the group theoretic foundation. Our main goal here is to introduce the class group G_{11} of level 11 and to give a detailed description of its structure. In particular, we prove that there are four conjugacy classes of elliptic elements of order 2, we provide concrete matrices t_1, t_2, t_3, t_4 representing these conjugacy classes, and we give an explicit presentation of G_{11} in terms of these elements (see Corollary 8).

This allows us in Section 3 to initiate the study of the numbers of the form $x^2 + 11y^2$ as follows: by conjugating the matrix $t_1 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ with an element of G_{11}, we get a matrix whose top right entry is of the form $x^2 + 11y^2$, where $x, y \in \mathbb{Z}$ and $\gcd(x, 11y) = 1$. Conversely, given a number n such that $11 \nmid n$, such that n is a quadratic residue modulo 11, and such that -11 is a quadratic residue modulo n, we construct an elliptic element $A_n(\ell)$ of order 2 in G_{11}.

Then $A_n(\ell)$ is conjugated to exactly one of the matrices t_i, and n is of the form $n = x^2 + 11y^2$ if and only if $A_n(\ell)$ is conjugated to t_1. For $i = 1, \ldots, 4$, let S_i be the set of integers n for which the top right corner of $A_n(\ell)$ is n and $A_n(\ell)$ is conjugated to t_i. Thus we are interested in

$$S_1 \; = \; \{n = x^2 + 11y^2 \mid x, y \in \mathbb{Z};\; \gcd(x, 11y) = 1\}$$

We prove that $S_2 = S_3$ and $S_4 = 2\, S_2$ (see Proposition 17) and that S_4 is easily discernible, since its elements n are exactly the ones satisfying $n \equiv 2 \pmod 4$. Consequently, the main task is to distinguish S_1 from

$$S_2 \; = \; \{n = 4x^2 + 22xy + 33y^2 \mid x, y \in \mathbb{Z};\; \gcd(x, 11y) = 1\}$$

inside $C = S_1 \cup S_2$. We also show that the even numbers in C are precisely the fourfolds of the odd numbers in C (see Proposition 21) and that the set of odd numbers in C is multiplicatively closed (see Proposition 22).

In order to move on, we need to introduce some methods of Algebraic Number Theory in Section 4. More precisely, since $x^2 + 11y^2 = (x + y\sqrt{-11})(x - y\sqrt{-11})$, we look at the algebric number field $\mathbb{Q}(\sqrt{-11})$, its ring of integers $\mathbb{Z}[\omega]$, where $\omega = (-11 + \sqrt{-11})/2$, and its order $\mathbb{Z}[\sqrt{-11}]$ of conductor 2. We describe the structure of $\mathbb{Z}[\omega]$, and in particular which products of its elements are contained in $\mathbb{Z}[\sqrt{-11}]$ (see Proposition 25). By realizing the elements of S_1 and S_2 as the norms of elements in $\mathbb{Z}[\omega]$, we get basic properties of products of elements in S_1 and S_2 (see Corollary 26). Moreover, we describe how various prime numbers split in $\mathbb{Z}[\omega]$ (see Proposition 27).

Next we turn our attention to special types of numbers in S_1 which occur in our main theorem: prime numbers and cubic numbers. In Section 5 we characterize prime numbers of the form $x^2 + 11y^2$. This case has been studied extensively before, so that it suffices to recall and simplify some results from Cox in order to get a good characterization (see Theorem 29). We also show that every prime is either in S_1 or in S_2 (see Proposition 30).

As for cubic numbers in $C = S_1 \cup S_2$, we prove in Section 6 that they are all odd and contained in $S_1 \setminus S_2$ (see Proposition 37.a). More precisely, the numbers m such that $m^3 \in S_1$ are of the form $m = p^\alpha \, \tilde{m}$, where p is a prime in S_2, where $\alpha \in \{0, 1, 2\}$, and where $\tilde{m}$ is of the form $\tilde{m} = x^2 + 11y^2$ (see Proposition 37.b).

Finally, in Section 7, we provide a detailed decomposition of the set S_1 in Theorem 42. It says that every number n with a primitive representation $n = x^2 + 11y^2$ such that $x, y \in \mathbb{Z}$ and $\gcd(x, 11y) = 1$ is of one of the following types:

(1) If n is even, it is of the form $n = 4\,\tilde{n}$ with an odd number $\tilde{n} \in S_2$.

(2) The number n is a product of powers of primes in S_1.

(3) The number n is a cubic number.

(4) The number n is an odd number in $S_1 \cap S_2$.

Here only the second and third sets intersect non-trivially and in the obvious way. For the odd numbers in S_1 and S_2, we then remove cubic factors and go on to provide a detailed characterization when they are in $S_1 \setminus S_2$ or $S_2 \setminus S_1$ or $S_1 \cap S_2$ based on their prime factors (see Corollary 45).

Since we apply methods from a number of different areas, we tried to keep this paper as self-contained as possible. The knowledgeable readers may bear with us for including some down-to-earth proofs which could have been replaced by high-level references. Many characterizations and properties of the sets of numbers we study were found and checked using the computer algebra system ApCoCoA.

Topics

The Class Group of Level 11

In the following we consider the subgroup G_{11} of $\mathrm{PSL}_2(\mathbb{R})$ consisting of the matrices of one of the types

$$U = \begin{pmatrix} a & b\sqrt{11} \\ c\sqrt{11} & d \end{pmatrix} \text{ with } a, b, c, d \in \mathbb{Z} \text{ and } ad - 11bc = 1,$$
$$V = \begin{pmatrix} a\sqrt{11} & b \\ c & d\sqrt{11} \end{pmatrix} \text{ with } a, b, c, d \in \mathbb{Z} \text{ and } 11ad - bc = 1.$$

where a matrix is identified with its negative. Equivalently, we consider a matrix of one of these types as a linear fractional transformation. This group is called the **class group of level 11**. The matrices of type U form a normal subgroup H_{11} of index 2 in G_{11}, and we have $G_{11} = H_{11} \cup T \cdot H_{11}$, where $T = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Since $T \cdot \left(\begin{smallmatrix} a & b\sqrt{11} \\ c\sqrt{11} & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} c\sqrt{11} & d \\ -a & b\sqrt{11} \end{smallmatrix}\right)$, the matrices in $T \cdot H_{11}$ are precisely the matrices of type V.

The group H_{11} can also be described as follows.

Remark 1

By conjugating G_{11} with the matrix $X = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{11} \end{pmatrix}$, we get the discrete group

$$G'_{11} = XG_{11}X^{-1} = H'_{11} \cup T' \cdot H'_{11}$$

where $H'_{11} = \{\begin{pmatrix} a & b \\ c' & d \end{pmatrix} \mid ad - bc = 1,\ c' \equiv 0 \pmod{11}\}$ and $T' = XTX^{-1} = \begin{pmatrix} 0 & 1/\sqrt{11} \\ -\sqrt{11} & 0 \end{pmatrix}$. Thus H'_{11} is the **Hecke congruence subgroup of level 11**

$$\Gamma_0(11) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \text{ such that } ad - bc = 1 \text{ and } c \equiv 0 \pmod{11}\right\}$$

of the **(inhomogeneous) modular group** $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$.

In the following we first determine the structure of the group G'_{11} and then we translate everything back to the group G_{11}. In particular, we want to determine the conjugacy classes of the elliptic elements of order 2 in $G_{11} \subset \mathrm{PSL}_2(\mathbb{Z})$. Clearly, they have to be residue classes of matrices of the form V. Notice that a matrix V of this form satisfies $V^2 = -I_2$ if and only if $d = -a$. (Here I_2 denotes the identity matrix of size 2×2, and we may use $-I_2$, since we work in $\mathrm{PSL}_2(\mathbb{Z})$.) It is known that the number of these conjugacy classes is $m(11) = 4$ (cf. [**?**], p. 152). Our goal in this section is to find explicit representatives of these conjugacy classes. Recall that the group

$$\Gamma(11) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{11} \right\}$$

is called the **(inhomogeneous) principal congruence subgroup of level 11** of the modular group $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$.

Remark 2 (The index and cosets of $\Gamma_0(11)$)

The principal congruence subgroup $\Gamma(11)$ of Γ is a normal subgroup, and it satisfies $\Gamma/\Gamma(11) \cong \mathrm{PSL}_2(\mathbb{F}_{11})$. Hence the index of $\Gamma(11)$ in Γ is $\frac{1}{2}\,11^3\,(1-\frac{1}{11^2}) = 660$.

(a) The group $\Gamma(11)$ is clearly a subgroup of $\Gamma_0(11)$. Under the hypothesis that $c \equiv 0 \pmod{11}$, the condition $ad - bc = 1$ implies that the residue classes of a and d in $\mathbb{F}_{11}$ are inverses of each other, and the residue class of b can be chosen freely. Hence the congruence $ad - bc \equiv 1 \pmod{11}$ has 110 incongruent solutions for (a, b, d). Since we identify a matrix with its negative, it follows that the index of $\Gamma(11)$ in $\Gamma_0(11)$ is 55. Altogether, we see that the index of $\Gamma_0(11)$ in Γ is 12.

(b) It is well-known that, as a system of representatives of $\Gamma/\Gamma_0(11)$, we can use $\{S_{-5}, S_{-4}, \ldots, S_5, T\}$, where $S_i = S^i = \left(\begin{smallmatrix} 1 & 0 \\ -i & 1 \end{smallmatrix}\right)$ with $S = \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$, and where $T = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

Next we want to determine generators for $\Gamma_0(11)$ via geometric arguments. For this it is more convenient to use the isomorphic group

$$\Gamma^0(11) = T\cdot\Gamma_0(11)\cdot T^{-1} = \{\left(\begin{smallmatrix} d & -c \\ -b & a \end{smallmatrix}\right) \mid ad-bc = 1,\ -c \equiv 0 \pmod{11}\}$$

The conjugation of the above decomposition of $\Gamma_0(11)$ yields

$$\Gamma^0(11) \ = \ \bigcup_{i=-5}^{5} \Gamma^0(11)\cdot U_i \ \cup \ \Gamma^0(11)\cdot T$$

where $U_i = U_1^i = \left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right)$ and $U_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

Remark 3 (A Fundamental Domain for $\Gamma^0(11)$)

Let $\mathbb{H} = \{\tau \in \mathbb{C} \mid \Im(\tau) > 0\}$ denote the upper half plane, as usual. Recall that the fundamental domain of the modular group Γ is given by

$$\begin{aligned} D_\Gamma \;=\; & \{\tau \in \mathbb{H} \mid |\Re(\tau)| < \tfrac{1}{2},\ |\tau| > 1\} \;\cup\; \{i\infty\} \\ & \cup \{\tau \in \mathbb{H} \mid \Re(\tau) = -\tfrac{1}{2},\ |\tau| \geq 1\} \\ & \cup \{\tau \in \mathbb{H} \mid |\tau| = 1,\ -\tfrac{1}{2} \leq \Re(\tau) \leq 0\} \end{aligned}$$

Then a fundamental domain of $\Gamma^0(11)$ is given by

$$D_{\Gamma^0(11)} \;=\; \bigcup_{i=-5}^{5} U_i(D_\Gamma) \;\cup\; T(D_\Gamma).$$

In order to get a geometric presentation of $\Gamma^0(11)$, we need to study the boundary correspondence for $D_{\Gamma^0(11)}$ next. For $i = -5, -4, \ldots, 5$, we let E_i be the circular arc of radius 1 centered at i, that is, we let $E_i = \{\tau \in \mathbb{H} \mid |\tau - i| = 1\}$.

Proposition 4

Under the action of $\Gamma^0(11)$, there are precisely the following boundary corespondences:

$$E_{-5} \leftrightarrow E_{-2}, \quad E_5 \leftrightarrow E_2, \quad E_{-4} \leftrightarrow E_3, \quad E_4 \leftrightarrow E_{-3}, \quad E_{-1} \leftrightarrow E_1$$

Now we can read off the structure of $\Gamma^0(11)$ and $\Gamma_0(11)$.

Corollary 5

The groups $\Gamma^0(11)$ and $\Gamma_0(11)$ have genus 1 and are free groups of rank 3.

(a) The group $\Gamma^0(11)$ is freely generated by $\tilde{A} = \begin{pmatrix} 2 & 11 \\ -1 & -5 \end{pmatrix}$, $\tilde{B} = \begin{pmatrix} 3 & -11 \\ -1 & 4 \end{pmatrix}$, and $\tilde{P} = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}$.

(b) The group $\Gamma_0(11)$ is freely generated by $A = \begin{pmatrix} -5 & 1 \\ -11 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 4 & 1 \\ 11 & 3 \end{pmatrix}$, and $P = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$.

Notice that P is a parabolic element of $\Gamma_0(11)$. A further parabolic element can be found via $Q = P \cdot [A, B^{-1}] = \begin{pmatrix} -21 & -11 \\ 44 & 23 \end{pmatrix}$.

Next we determine the structure of the group G'_{11}.

Remark 6 (The Signature of G'_{11})

From the preceding corollary and the fact that $H'_{11} = \Gamma_0(11)$ has index 12 in the modular group Γ, it follows that H'_{11} is a co-finite Fuchsian group.
In general, a co-finite Fuchsian group F has a presentation of the form

$$F = \langle s_1, \ldots, s_r, p_1, \ldots, p_t, a_1, b_1, \ldots, a_g, b_g \mid$$
$$s_1^{m_1} = \cdots = s_r^{m_r} = s_1 \cdots s_r \cdot p_1 \cdots p_r \cdot \prod_{i=1}^{g} [a_i, b_i] = 1 \rangle$$

where $m_i \geq 2$, where the elements s_i represent the conjugacy classes of maximal elliptic cyclic subgroups, where the elements p_j represent the conjugacy classes of maximal parabolic cyclic subgroups, and where g is the genus of F.

The group F can be described by the symbol $(g; m_1, \ldots, m_r; t)$ which is called the **signature** of F. Moreover, the (finite) **hyperbolic area** for F is given by

$$\mu(F) \; = \; 2\pi \left(2g - 2 + t + (1 - \frac{1}{m_1}) + \cdots + (1 - \frac{1}{m_r}) \; > \; 0\right.$$

A subgroup F' of F of finite index is also a co-finite Fuchsian group, and its hyperbolic area satisfies the Riemann-Hurwitz relation $\mu(F') = [F : F'] \cdot \mu(F)$.
In our setting, the corollary says that H'_{11} is a co-finite Fuchsian group with signature $(1; 0; 2)$ and we get $\mu(H'_{11}) = 2\pi(2 - 2 + 2) = 4\pi$. Clearly, the group G'_{11} is also a co-finite Fuchsian group. Let $(g; m_1, \ldots, m_r; g)$ be its signature. Then $[G'_{11} : H'_{11}] = 2$ implies $t = 1$ and $m_1 = \cdots = m_r = 2$. Moreover, we get $\mu(G'_{11}) = 2\pi$, and hence $2g - 2 + \frac{r}{2} = 0$. This is possible only if $g = 0$ and $r = 4$, so that altogether we obtain the signature $(0; 2, 2, 2, 2; 1)$ for G'_{11}.

Using the information gathered above, we are ready to construct a nice presentation of G'_{11}.

Proposition 7

In G'_{11}, consider the following elements:

$$T_1 = \begin{pmatrix} 0 & 1/\sqrt{11} \\ -\sqrt{11} & 0 \end{pmatrix}, \; T_2 = \begin{pmatrix} -\sqrt{11} & 4/\sqrt{11} \\ -3\sqrt{11} & \sqrt{11} \end{pmatrix},$$

$$T_3 = \begin{pmatrix} \sqrt{11} & -3/\sqrt{11} \\ 4\sqrt{11} & -\sqrt{11} \end{pmatrix}, \; T_4 = \begin{pmatrix} -\sqrt{11} & -6/\sqrt{11} \\ 2\sqrt{11} & \sqrt{11} \end{pmatrix}, \; \textit{and } P = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$$

Then the group G'_{11} has the presentation

$$G'_{11} = \langle T_1, T_2, T_3, T_4, P \mid T_1^2 = T_2^2 = T_3^2 = T_4^2 = T_2 T_3 T_1 T_4 P = 1 \rangle$$

where T_1, T_2, T_3, T_4 are elliptic elements of order 2 representing the conjugacy classes of such elements, and where P is a parabolic element.

The last step is to translate the above presentation of G'_{11} to a presentation of G_{11} This is easily achieved by conjugating back using the matrix X of Remark 1.

Corollary 8

The group G_{11} has a presentation

$$G_{11} \;=\; \langle t_1, t_2, t_3, t_4, p \mid t_1^2 = t_2^2 = t_3^2 = t_4^2 = t_2 t_3 t_1 t_4 p = 1 \rangle$$

where $t_1 = X^{-1}T_1X = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $t_2 = X^{-1}T_2X = \begin{pmatrix} -\sqrt{11} & 4 \\ -3 & \sqrt{11} \end{pmatrix}$, $t_3 = X^{-1}T_3X = \begin{pmatrix} \sqrt{11} & -3 \\ 4 & -\sqrt{11} \end{pmatrix}$, $t_4 = X^{-1}T_4X = \begin{pmatrix} -\sqrt{11} & -6 \\ 2 & \sqrt{11} \end{pmatrix}$, and $p = X^{-1}PX = \begin{pmatrix} -1 & \sqrt{11} \\ 0 & -1 \end{pmatrix}$.
Here t_1, t_2, t_3, t_4 are elliptic elements of order 2 representing the conjugacy classes of such elements, and p is a parabolic element.

Topics

Representing Numbers in the Form $x^2 + 11y^2$

In this section we want to represent numbers in the form $n = x^2 + 11y^2$ with $x, y \in \mathbb{Z}$ using the matrices in the class group of level 11. Let us begin with some easy observations.

Remark 9

In the following we let $n \in \mathbb{Z}$.

(a) Suppose that n is divisible by 11, and write $n = 11\,\tilde{n}$ with $\tilde{n} \in \mathbb{Z}$. Then n is of the form $n = x^2 + 11y^2$ if and only of $\tilde{n}$ is of this form.
Namely, if $\tilde{n} = x^2 + 11y^2$, then $n = 11\,\tilde{n} = (11y)^2 + 11x^2$.
Conversely, if $n = x^2 + 11y^2$ is divisible by 11, then x is divisible by 11 and we can write $x = 11\,\tilde{x}$ with $\tilde{x} \in \mathbb{Z}$.
Consequently, we have $\tilde{n} = y^2 + 11\tilde{x}^2$. So, from now on we shall assume that n is not divisible by 11.

(b) Clearly, $n \equiv x^2 \pmod{11}$ says that n is a quadratic residue modulo 11. So, from now on we only consider numbers n which are quadratic residues modulo 11.

Representing Numbers in the Form $x^2 + 11y^2$

(c) If $n = x^2 + 11y^2$ and $\gcd(n, x, y) = 1$, we say that (n, x, y) is a **primitive representation** of n. Clearly, if $\gcd(n, x) > 1$ or $\gcd(n, y) > 1$ or $\gcd(x, y) > 1$ then the representation is not primitive. Moreover, it suffices to check whether n has a primitive representation, as all representations can be obtained by multiplying a primitive representation by a square number. To check whether a number n has a representation of the form $n = x^2 + 11\,y^2$, it suffices to check whether n, or a number n/s with a square number s dividing n, has a primitive representation. Therefore we will be interested only in primitive representations.

(d) If n has a primitive representation of the form $n = x^2 + 11y^2$ then -11 is a quadratic residue modulo n. In effect, we have $x^2 + 11y^2 \equiv 0 \pmod{n}$ and $\gcd(y, n) = 1$. Hence y is a unit modulo n and $-11 \equiv (x/y)^2 \pmod{n}$ is a quadratic residue modulo n.

Altogether, we are led to define the following sets.

Notation 10

The set $\mathbb{D}$ of all positive integers n such that $11 \nmid n$, and such that -11 is a quadratic residue modulo n, is called the *domain* of our investigation. We have

$$\mathbb{D} = \{1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 23, 25, 27, 30, 31, 36, 37, 45, 46, 47, 50, \ldots\}$$

Moreover, the set of all numbers $n \in \mathbb{D}$ which have a primitive representation $n = x^2 + 11y^2$ with $x, y \in \mathbb{Z}$ is denoted by

$$\begin{aligned} S_1 &= \{n \in \mathbb{D} \mid n = x^2 + 11y^2 \text{ for some } x, y \in \mathbb{Z} \text{ with } \gcd(x, y) = 1\} \\ &= \{1, 12, 15, 20, 27, 36, 45, 47, 53, 60, 69, 75, 92, 93, 100, 103, 111, 115, 124, \ldots\} \end{aligned}$$

Notice that, if -11 is a quadratic residue modulo n, then n is a quadratic residue modulo 11, so that the second condition in the definition of $\mathbb{D}$ is actually superfluous. For prime numbers n, both conditions are equivalent by the Quadratic Reciprocity Theorem, since $11 \equiv 3 \pmod 4$. The following construction is the key for representing numbers in the form $x^2 + 11y^2$.

Remark 11

Let $n \in \mathbb{D}$. Consider the following steps:

(a) Since -11 is a unit modulo n, we can calculate $b = (-11)^{-1} \pmod{n}$.

(b) Then b is a square modulo n, that is, we can find a number $\ell \in \mathbb{Z}$ such that $\ell^2 \equiv b \pmod{n}$.

(c) In particular, we have $(-11)\,\ell^2 \equiv 1 \pmod{n}$. Hence we find $q \in \mathbb{Z}$ such that $-11\,\ell^2 + n\,q = 1$.

(d) Now we form the matrix $A_n(\ell) = \begin{pmatrix} \ell\sqrt{11} & n \\ -q & -\ell\sqrt{11} \end{pmatrix}$.

In this way we obtain a matrix $A_n(\ell) \in G_{11}$ which satisfies $A_n(\ell)^2 = -I_2$. Consequently, the matrix $A_n(\ell)$ is conjugate in G_{11} to exactly one of the matrices t_1, t_2, t_3, t_4 in Corollary 8.

Notice that, for a given number n, there exist infinitely many different matrices $A_n(\ell)$. In order to find out which of the matrices t_1, t_2, t_3, t_4 is conjugate to a given matrix $A_n(\ell)$, we first calculate the general shapes of the conjugates of these matrices.

Lemma 12

Let the elements of G_{11} be described by the matrices of type $U = \begin{pmatrix} a & b\sqrt{11} \\ c\sqrt{11} & d \end{pmatrix}$ and $V = \begin{pmatrix} a\sqrt{11} & b \\ c & d\sqrt{11} \end{pmatrix}$ as at the beginning of Section 2. Then the following equalities hold:

(a) $U\, t_1\, U^{-1} = \begin{pmatrix} (-ac-bd)\sqrt{11} & a^2+11b^2 \\ -11c^2-d^2 & (ac+bd)\sqrt{11} \end{pmatrix}$

(b) $V\, t_1\, V^{-1} = \begin{pmatrix} (-ac-bd)\sqrt{11} & 11a^2+b^2 \\ -c^2-11d^2 & (ac+bd)\sqrt{11} \end{pmatrix}$.

(c) $U\, t_2\, U^{-1} = \begin{pmatrix} (-4ac-11bc-ad-3bd)\sqrt{11} & 4a^2+22ab+33b^2 \\ -44c^2-22cd-3d^2 & (4ac+11bc+ad+3bd)\sqrt{11} \end{pmatrix}$.

(d) $V\, t_2 V^{-1} = \begin{pmatrix} (-4ac-bc-11ad-3bd)\sqrt{11} & 44a^2+22ab+3b^2 \\ -4c^2-22cd-33d^2 & (4ac+bc+11ad+3bd)\sqrt{11} \end{pmatrix}$.

(e) $U\, t_3\, U^{-1} =$
$-\begin{pmatrix} (-3ac-11bc-ad-4bd)\sqrt{11} & 3a^2+22ab+44b^2 \\ -33c^2-22cd-4d^2 & (3ac+11bc+ad+4bd)\sqrt{11} \end{pmatrix}$.

(f) $V\, t_3\, V^{-1} =$
$$-\begin{pmatrix} (-3ac-bc-11ad-4bd)\sqrt{11} & 33a^2+22ab+4b^2 \\ -3c^2-22cd-44d^2 & (3ac+bc+11ad+4bd)\sqrt{11} \end{pmatrix}.$$

(g) $U\, t_4\, U^{-1} =$
$$-\begin{pmatrix} (-6ac+11bc+ad-2bd)\sqrt{11} & 6a^2-22ab+22b^2 \\ -66c^2+22cd-2d^2 & (6ac-11bc-ad+2bd)\sqrt{11} \end{pmatrix}.$$

(h) $V\, t_4\, V^{-1} =$
$$-\begin{pmatrix} (-6ac+bc+11ad-2bd)\sqrt{11} & 66a^2-22ab+2b^2 \\ -6c^2+22cd-22d^2 & (6ac-bc-11ad+2bd)\sqrt{11} \end{pmatrix}.$$

The following proposition lies at the heart of our method.

Proposition 13

For $n \in \mathbb{D}$, the following conditions are equivalent:

(a) The number n has a primitive representation $n = x^2 + 11y^2$ with $x, y \in \mathbb{Z}$.

(b) There exists a number $\ell \in \mathbb{Z}$ such that $\ell^2 \equiv (-11)^{-1} \pmod{n}$ and such that the matrix $A_n(\ell) = \begin{pmatrix} \ell\sqrt{11} & n \\ -q & -\ell\sqrt{11} \end{pmatrix}$ is conjugate to $t_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in G_{11}, where $q = (1 + 11\,\ell^2)/n$.

The following example shows that different choices of ℓ may yield matrices which are conjugate to different matrices t_i.

Example 14

Consider the number $n = 12$. It is a quadratic residue modulo 11, $-11 \equiv 1 \pmod{12}$ is a quadratic residue modulo n, and it has representations $n = x^2 + 11y^2$ with $x = y = 1$ as well as $n = 4a^2 + 22ab + 33b^2$ with $a = -5$ and $b = 2$. Let us examine the conjugacy classes of the following matrices $A_n(\ell)$.

(a) For $U = \begin{pmatrix} 1 & \sqrt{11} \\ \sqrt{11} & 12 \end{pmatrix}$, we see that $U\, t_1 U^{-1} = \begin{pmatrix} -13\sqrt{11} & 12 \\ -155 & 13\sqrt{11} \end{pmatrix} = A_n(\ell)$ for $\ell = -13$. Thus $A_n(-13)$ is conjugate to t_1 in G_{11}.

(b) For $U = \begin{pmatrix} -5 & 2\sqrt{11} \\ 2\sqrt{11} & -9 \end{pmatrix}$, we see that $U\, t_2 U^{-1} = \begin{pmatrix} 5\sqrt{11} & 12 \\ -23 & -5\sqrt{11} \end{pmatrix} = A_n(\ell)$ for $\ell = 5$. Thus $A_n(5)$ is conjugate to t_2 in G_{11}.

Indeed, both $\ell = -13$ and $\ell = 5$ satisfy $\ell^2 \equiv (-11)^{-1} \equiv 1 \pmod{12}$.

To get the dependency of the conjugacy class of $A_n(\ell)$ in ℓ under control, we may use the following proposition.

Proposition 15

Let $n \in \mathbb{D}$, let $\ell \in \mathbb{Z}$ be chosen such that $\ell^2 \equiv (-11)^{-1} \pmod{n}$, and let $i \in \{1, \ldots, 4\}$ be such that $A_n(\ell)$ is in the conjugacy class of t_i in G_{11}.

(a) The matrices $A_n(\ell - n)$ and $A_n(\ell + n)$ are in the conjugacy class of t_i.

(b) The matrix $A_n(-\ell)$ is in the conjugacy class of t_1 if and only if $A_n(\ell)$ is in the conjugacy class of t_1.

This proposition allows us to characterize primes of the form $x^2 + 11y^2$ as follows.

Corollary 16

For an odd prime number $p \in \mathbb{D}$, the following conditions are equivalent.

(a) The number p has a primitive representation $p = x^2 + 11y^2$ with $x, y \in \mathbb{N}$.

(b) There exists a number $\ell \in \mathbb{Z}$ such that $\ell^2 \equiv (-11)^{-1} \pmod{p}$ and such that $A_p(\ell)$ is in the conjugacy class of t_1 in G_{11}.

(c) For every number $\ell \in \mathbb{Z}$ such that $\ell^2 \equiv (-11)^{-1} \pmod{p}$, the matrix $A_p(\ell)$ is in the conjugacy class of t_1 in G_{11}.

The following proposition collects some properties of the numbers represented by the quadratic forms in the top right corners of the matrices in Lemma 12.

Proposition 17

Consider the following six quadratic forms:
$u_2 = 4x^2 + 22xy + 33y^2$, $v_2 = 44x^2 + 22xy + 3y^2$,
$u_3 = 3x^2 + 22xy + 44y^2$, $v_3 = 33x^2 + 22xy + 4y^2$,
$u_4 = 6x^2 - 22xy + 22y^2$, and $v_4 = 66x^2 - 22xy + 2y^2$.

(a) For $x, y \in \mathbb{Z}$ and $(x, y) \neq (0, 0)$, these quadratic forms represent positive integers.

(b) Let
$S_2 = \{u_2(x, y) \mid x, y \in \mathbb{Z};\ (x, y) \neq (0, 0);\ \gcd(x, 11y) = 1\}$
be the set of numbers represented by u_2, and let
$S_2' = \{v_2(x, y) \mid x, y \in \mathbb{Z};\ (x, y) \neq (0, 0);\ \gcd(11x, y) = 1\}$
be the set of numbers represented by v_2. Then we have
$S_2' = S_2$.

(c) Both the set of numbers represented by u_3 and the set of numbers represented by v_3 agree with S_2.

(d) Let
$S_4 = \{u_4(x, y) \mid x, y \in \mathbb{Z};\ (x, y) \neq (0, 0);\ \gcd(x, 11y) = 1\}$
be the set of numbers represented by u_4. This set agrees with the set of numbers represented by v_4, and we have
$S_4 = \{2n \mid n \in S_2\} \cup \{2\}$.

(e) The domain $\mathbb{D}$ is the disjoint union of $S_1 \cup S_2$ and S_4. More precisely, the numbers in S_4 are precisely those numbers n in $\mathbb{D}$ which satisfy $n \equiv 2 \pmod 4$.

Thus we can now write down a simple characterization of the numbers in $S_1 \cup S_2$.

Corollary 18

For a number $n \in \mathbb{N}_+$, the following conditions are equivalent.

(a) The number n is of the form $n = x^2 + 11y^2$ or of the form $n = 4x^2 + 22xy + 33y^2$ with $x, y \in \mathbb{Z}$ and $\gcd(x, 11y) = 1$.

(b) We have $n \in \mathbb{D}$ and $n \not\equiv 2 \pmod 4$.

The preceding proposition and its corollary suggest to introduce the following notation.

Notation 19

The set of all positive integers n of the form $n = 4x^2 + 22xy + 33y^2$ with $x, y \in \mathbb{Z}$ and $\gcd(x, 11y) = 1$ is denoted by

$$S_2 = \{3, 4, 5, 9, 12, 15, 20, 23, 25, 31, 36, 37, 45, 59, 60, 67, 69, 71, 75, 81, 89, 92, \dots\}$$

The union $S_1 \cup S_2$ is called the set of *candidate* numbers and denoted by

$$\begin{aligned} C =& S_1 \cup S_2 \\ =& \{1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 23, 25, 27, 30, \\ & 31, 36, 37, 45, 46, 47, 50, 53, \dots\} \end{aligned}$$

Thus we are left with the task of distinguishing between the sets S_1 and S_2 inside the candidate set C. For further usage, let us describe the sets S_2 and C in different ways.

Proposition 20

The set S_2 defined above is equal to each of the following sets.

(a) $S_{2,a} = \{4x^2 + 22xy + 33y^2 \mid x, y \in \mathbb{Z},\ \gcd(x, 11y) = 1\}$

(b) $S_{2,b} = \{3x^2 + 22xy + 44y^2 \mid x, y \in \mathbb{Z},\ \gcd(x, 11y) = 1\}$

(c) $S_{2,c} = \{3x^2 + 2xy + 4y^2 \mid x, y \in \mathbb{Z},\ \gcd(x, y) = 1,\ 11 \nmid (3x^2 + 2xy + 4y^2)\}$

Proposition 21

The set $C = S_1 \cup S_2$ is the disjoint union of the following two sets:

$$C_1 = \{n \in \mathbb{Z} \mid n = x^2 + 11xy + 33y^2;\ x, y \in \mathbb{Z};\ \gcd(x, 11y) = 1\}$$
$$C_2 = \{n \in \mathbb{Z} \mid n = x^2 + 11xy + 33y^2;\ x, y \in \mathbb{Z};\ \gcd(x, 11y) = 2\}$$

Here the numbers in C_1 are odd and the numbers in C_2 are divisible by 4. The numbers in C_1 will be called the *odd candidates* and the numbers in C_2 the *even candidates*.

Another useful property is the fact that C_1 is multiplicatively closed, as the following proposition shows.

Proposition 22

For odd numbers $n_1, n_2 \in C$, we have $n_1 n_2 \in C$. In particular, the set of odd candidates C_1 is a multiplicative submonoid of $\mathbb{N}_+$.

At this point we need to insert further background material.

Topics

The Ring of Integers of $\mathbb{Q}(\sqrt{-11})$

In this section we provide some basic material from Algebraic Number Theory. Since we have $x^2 + 11y^2 = (x + y\sqrt{-11})(x - y\sqrt{-11})$, it is natural to study the quadratic field $\mathbb{Q}(\sqrt{-11})$ and its ring of integers. Let us collect some well-known facts.

Proposition 23

Let $K = \mathbb{Q}(\sqrt{-11})$, and let $\mathcal{O}_K$ be the ring of integers of K.

(a) The ring of integers of K is given by $\mathcal{O}_K = \mathbb{Z}[(1 + \sqrt{-11})/2] = \mathbb{Z}[\omega]$, where $\omega = (-11 + \sqrt{-11})/2$. It is a free $\mathbb{Z}$-module of rank 2 with basis $\{1, \omega\}$.

(b) The minimal polynomial of ω is $\mu_\omega(x) = x^2 + 11x + 33$. In particular, we have $\mathcal{O}_K \cong \mathbb{Z}[x]/\langle x^2 + 11x + 33\rangle$.

(c) The Galois group of $K/\mathbb{Q}$ has two elements. The non-trivial automorphism maps $\sqrt{-11}$ to $-\sqrt{11}$ and ω to $\overline{\omega} = (-11 - \sqrt{-11})/2$.

The Ring of Integers of $\mathbb{Q}(\sqrt{-11})$

(d) We have $\omega + \overline{\omega} = -11$ and $\omega \cdot \overline{\omega} = 33$.

(e) The ideal class number of $\mathbb{Z}[\omega]$ is 1, that is, this ring is a PID. In particular, it is a factorial ring.

(f) The unit group of $\mathcal{O}_K$ is $\{1, -1\}$.

(g) The norm map $N_{\mathcal{O}_K} : \mathcal{O}_K \to \mathbb{Z}$ is given by $N_{\mathcal{O}_K}(a + b\omega) = (a + b\omega)(a + b\overline{\omega}) = a^2 - 11ab + 33b^2$ for all $a, b \in \mathbb{Z}$. It turns the ring $\mathbb{Z}[\omega]$ into a Euclidean domain.

As the factorization $x^2 + 11y^2 = (x + y\sqrt{-11})(x - y\sqrt{-11})$ actually takes place in the ring $\mathbb{Z}[\sqrt{-11}]$, let us also introduce its properties and its relation to $\mathbb{Z}[\omega]$.

Remark 24

Let $K = \mathbb{Q}(\sqrt{-11})$ and $\mathcal{O}_K = \mathbb{Z}[\omega]$ with $\omega = (-11 + \sqrt{11})/2$.

(a) The ring $\mathcal{O} = \mathbb{Z}[\sqrt{-11}]$ is the order of conductor 2 in $\mathbb{Z}[\omega]$. In particular, we have $\mathcal{O} = \mathbb{Z} + 2\omega\mathbb{Z}$.

(b) The ring $\mathbb{Z}[\sqrt{-11}]$ is a free $\mathbb{Z}$-module with basis $\{1, \sqrt{-11}\}$, the ring $\mathbb{Z}[\omega]$ is a $\mathbb{Z}[\sqrt{-11}]$-module which is generated by $\{1, \omega\}$, and $2\omega \in \mathbb{Z}[\sqrt{-11}]$. Thus the elements of $\mathbb{Z}[\omega]$ are either in $\mathbb{Z}[\sqrt{-11}]$ or in $\omega + \mathbb{Z}[\sqrt{-11}]$.

Using this remark, we can analyze products of elements of $\mathbb{Z}[\omega]$ as follows.

Proposition 25

Let $a + b\omega$, $a' + b'\omega$ be elements of $\mathbb{Z}[\omega]$, where $a, a', b, b' \in \mathbb{Z}$ and $\omega = (-11 + \sqrt{-11})/2$.

(a) The element $a + b\omega$ is contained in $\mathbb{Z}[\sqrt{-11}]$ if and only if b is even.

(b) For $a + b\omega \in \mathbb{Z}[\sqrt{-11}]$ and $a' + b'\omega \notin \mathbb{Z}[\sqrt{-11}]$ we have $(a + b\omega)(a' + b'\omega) \in \mathbb{Z}[\sqrt{-11}]$ if and only if a is even, that is, if and only if $a + b\omega$ is a multiple of 2.

(c) For $a + b\omega, a' + b'\omega \notin \mathbb{Z}[\sqrt{-11}]$, we have $(a + b\omega)(a' + b'\omega) \in \mathbb{Z}[\sqrt{-11}]$ if and only if $a + a'$ is odd.

(d) For every element $a + b\omega \in \mathbb{Z}[\omega]$ with $a, b \in \mathbb{Z}$, we have $(a + b\omega)^3 \in \mathbb{Z}[\sqrt{-11}]$.

This proposition yields the following properties of products of elements in C.

Corollary 26

In the setting of the proposition, let $\overline{S}_1$ be the set of all numbers of the form $c^2 n$ where $c \in \mathbb{Z}$ and $n \in S_1$. Then the following statements hold.

(a) The element $N_{\mathcal{O}_K}(a + b\omega) = (a + b\omega)(a + b\overline{\omega})$ is contained in C if and only if $\gcd(a, 11b) = 1$.

(b) The element $N_{\mathcal{O}_K}(a + b\omega) = (a + b\omega)(a + b\overline{\omega})$ is contained in S_1 if and only if b is even and $\gcd(a, 11b) = 1$.

(c) Assume that we have $a + b\omega, a' + b'\omega \in \mathbb{Z}[\sqrt{-11}]$. Then the element $N_{\mathcal{O}_K}((a + b\omega)(a' + b'\omega))$ is in $\overline{S}_1$. Consequently, the product of two numbers in S_1 is contained in $\overline{S}_1$.

(d) Assume that we have $a + b\omega \in \mathbb{Z}[\sqrt{-11}]$ and $a' + b'\omega \notin \mathbb{Z}[\sqrt{-11}]$. Then the element $N_{\mathcal{O}_K}((a + b\omega)(a' + b'\omega))$ is in $\overline{S}_1$ if and only if a is even, that is, if and only if 2 divides $a + b\omega$. Consequently, the product of a number n in S_1 and a number in $S_2 \setminus S_1$ is contained in $\overline{S}_1$ if and only if n is even.

(e) Assume that we have $a + b\omega, a' + b'\omega \notin \mathbb{Z}[\sqrt{-11}]$. Then the element $N_{\mathcal{O}_K}((a + b\omega)(a' + b'\omega))$ is in $\overline{S}_1$ if and only if $a + a'$ is an odd integer.

(f) A number $n \in C$ is contained in S_2 if and only if we have a representation $n = N_{\mathcal{O}_K}(a + b\omega)$ with $a, b \in \mathbb{Z}$ and $\gcd(a, 11b) = 1$, an even number a and an odd number b.

Finally, we collect results about the splitting of primes in the factorial ring $\mathbb{Z}[\omega]$.

Proposition 27

Consider the ring of integers $\mathcal{O}_K = \mathbb{Z}[\omega]$ of the quadratic number field $K = \mathbb{Q}(\sqrt{-11})$, where $\omega = (-11 + \sqrt{-11})/2$.

(a) The only ramified prime in $\mathcal{O}_K$ is $p = 11$.

(b) The prime 2 is inert in $\mathcal{O}_K$

(c) An odd prime $p \neq 11$ splits in $\mathcal{O}_K$ if and only if -11 is a quadratic residue modulo p. In particular, all primes in $S_1 \cup S_2$ split in $\mathcal{O}_K$.

(d) Let p be an odd prime in $C = S_1 \cup S_2$. Then p is contained in S_1 if and only if the two factors of p are already contained in $\mathbb{Z}[\sqrt{-11}]$.

For powers of primes in S_1, this proposition implies the following result.

Corollary 28

Given a prime number $p \in S_1$, we have $p^\alpha \in S_1$ for every $\alpha \geq 1$.

As a byproduct of the proof of Proposition 27, we see that $p \in S_2$ implies $p \notin S_1$. A better criterion for distinguishing the primes in S_1 and S_2 is coming up next.

Topics

The next task is to characterize the prime numbers of the form $x^2 + 11y^2$. This problem has been explored intensively using Class Field Theory and other methods of Algebraic Number Theory. As mentioned in the preceding section, the form $x^2 + 11y^2$ splits in the ring $\mathcal{O} = \mathbb{Z}[\sqrt{-11}]$ which is the order of conductor 2 in the ring of integers $\mathcal{O}_K$ of the field $K = \mathbb{Q}(\sqrt{-11})$. Thus it is not a Dedekind domain. The discriminant of this order is -44. As a result of these studies, we have the following theorem.

Theorem 29 (Characterization of Primes of the Form $x^2 + 11y^2$)

A prime number $p \geq 13$ is of the form $p = x^2 + 11y^2$ with $x, y \in \mathbb{Z}$ if and only if the following two conditions are satisfied:

(a) The number -11 is a quadratic residue modulo p.

(b) The polynomial $f_{11}(x) = x^3 - 2x^2 + 2x - 2$ has a zero modulo p.

Notice that the polynomial f_{11} actually splits into linear factors in $\mathbb{F}_p$, if p is a prime of the form $p = x^2 + 11y^2$.

To distinguish the prime numbers of the form $p = x^2 + 11y^2$ from the prime numbers of the form $p = 3x^2 + 2xy + 4y^2$, we need one further ingredient.

Proposition 30

Let S_1 and S_2 be the sets defined in the preceding section. Then every prime number in $S_1 \cup S_2$ lies either in the set S_1 or in the set S_2, but not in both.

As an immediate consequence of this proposition and the above theorem, we obtain the following characterization of primes of the form $p = 3x^2 + 2xy + 4y^2$.

Corollary 31

A prime number $p \geq 3$ with $p \neq 11$ is of the form $p = 3x^2 + 2xy + 4y^2$ with $x, y \in \mathbb{Z}$ if and only if the following conditions hold:

(a) The number -11 is a quadratic residue modulo p.

(b) The polynomial $f_{11}(x) = x^3 - 2x^2 + 2x - 2$ is irreducible modulo p.

Finally, we point out that for the primes of the forms in the theorem and the corollary, we have the following uniqueness property.

Proposition 32

Let $p \geq 3$ with $p \neq 11$ be a prime number such that -11 is a quadratic residue modulo p.

(a) If $f_{11}(x) = x^3 - 2x^2 + 2x - 2$ splits in $\mathbb{F}_p[x]$ into linear factors, then there exists a unique pair of numbers $(x, y) \in \mathbb{N}^2$ such that $p = x^2 + 11y^2$.

(b) If $f_{11}(x) = x^3 - 2x^2 + 2x - 2$ is irreducible in $\mathbb{F}_p[x]$, then there exists a unique pair of numbers $(x, y) \in \mathbb{N} \times \mathbb{Z}$ such that $p = 3x^2 + 2xy + 4y^2$.

Topics

1. Introduction
2. The Class Group of Level 11
3. Representing Numbers in the Form $x^2 + 11y^2$
4. The Ring of Integers of $\mathbb{Q}(\sqrt{-11})$
5. Primes of the Form $x^2 + 11y^2$
6. **Cubic Numbers of the Form** $x^2 + 11y^2$
7. Classifying Numbers of the Form $x^2 + 11y^2$

Cubic Numbers of the Form $x^2 + 11y^2$

In this section we examine cubic numbers m^3 of the form $m^3 = x^2 + 11y^2$ with $m, x, y \in \mathbb{N}$. Recall the sets S_1 and S_2 defined in Notation 10 and Notation 19. The following easy observations will help us.

Lemma 33

Every cubic number of the form $m^3 = x^2 + 11y^2$ with $x, y \in \mathbb{Z}$ and $\gcd(x, 11y) = 1$ is odd.

Lemma 34

For every cubic number of the form $m^3 = x^2 + 11y^2$ with $x, y \in \mathbb{Z}$ and $\gcd(x, 11y) = 1$, the number m is contained in the set $S_1 \cup S_2$.

Lemma 35

Let $\overline{S}_1$ be the set of all integers n such that $n = x^2 + 11y^2$ for some $x, y \in \mathbb{Z}$ and such that $\gcd(n, 11) = 1$, and let p_1, p_2 be prime numbers in C.

(a) If $p_1, p_2 \in S_1$ then we have $p_1^{\alpha_1} p_2^{\alpha_2} \in \overline{S}_1$ for all $\alpha_1, \alpha_2 \in \mathbb{N}$.

(b) If $p \in S_2$ then we have $p^2 \in S_2 \setminus S_1$.

(c) If $p_1 \in S_1$ and $p_2 \in S_2$ then we have $p_1^{\alpha_1} p_2^{\alpha_2} \in S_2 \setminus S_1$ for $\alpha_1, \alpha_2 \in \{1, 2\}$.

(d) If $p_1, p_2 \in S_2$ are distinct primes, then we have $p_1^{\alpha_1} p_2^{\alpha_2} \in S_1 \cap S_2$ for $\alpha_1, \alpha_2 \in \{1, 2\}$.

Lemma 36

Let $a \in \mathbb{Z}$ be even and $b \in \mathbb{Z}$ be odd. Then $\gcd(a + b\omega, a + b\overline{\omega}) = 1$ holds in $\mathbb{Z}[\omega]$.

Finally, we can characterize cubic numbers of the form $x^2 + 11y^2$ as follows.

Proposition 37

Let the sets S_1, S_2, and C be defined as in Section 3, let $\bar{S}_1 = \{x^2 + 11y^2 \mid x, y \in \mathbb{Z};\ \gcd(x, 11) = 1\}$, and let S_1^{cube} be the set of cubic numbers in C. Then the following statements hold.

(a) Every cube of a number in C is contained in $S_1 \setminus S_2$, that is, we have $S_1^{\mathrm{cube}} \subset S_1 \setminus S_2$.

(b) Every number m such that $m^3 \in S_1^{\mathrm{cube}}$ is of the form $m = p^{\alpha}\, \tilde{m}$ with a prime number $p \in S_2$, with $0 \leq \alpha \leq 2$, and with $\tilde{m} \in \bar{S}_1$.

(c) The set S_1^{cube} is the multiplicative monoid generated by the cubes of the prime numbers in $S_1 \cup S_2$.

The next example shows that it is possible that m^3 has a primitive representation of the form $x^2 + 11y^2$, while $m \in \bar{S}_1$ does not.

Example 38

The number $m = 675 = 25 \cdot 27$ is not contained in S_1, since the only representations $m = 20^2 + 11 \cdot 5^2 = 24^2 + 11 \cdot 3^2$ are not primitive. However, $675^3 = 12136^2 + 11 \cdot 3817^2$ is a primitive representation, and thus we have $675^3 \in S_1$.

Topics

In this section we prove several decompositions of the set S_1. To simplify the discussion, we introduce the following abbreviations.

Notation 39

Let the sets C, S_1, and S_2 be defined according to Notation 10 and Notation 19. For $i \in \{1, 2\}$, we define

$$\begin{aligned}
S_i^{\text{even}} &= \{n \in S_i \mid n \text{ is even}\} \\
S_i^{\text{odd}} &= \{n \in S_i \mid n \text{ is odd}\} \\
S_i^{\text{prim}} &= \{n \in S_i \mid n \text{ is a prime}\} \\
S_1^{\text{cube}} &= \{n \in S_1 \mid n \text{ is a cubic number}\}
\end{aligned}$$

Proposition 40

The even numbers in S_1 satisfy $S_1^{\text{even}} = 4 \cdot S_2^{\text{odd}}$.

In view of this proposition, our task of decomposing S_1 is reduced to decomposing S_1^{odd} and S_2^{odd}. In order to move to the main theorem of this section, we need one final ingredient.

Lemma 41

Let $p \in S_2^{\mathrm{prim}}$ and $\alpha \geq 1$. Then we have $p^\alpha \in S_1$ if α is divisible by 3, and $p^\alpha \in S_2$ otherwise.

The following decomposition is one of the main results of this paper.

Theorem 42

The set S_1 is the union

$$S_1 \;=\; S_1^{\mathrm{even}} \;\cup\; \langle S_1^{\mathrm{prim}} \rangle \;\cup\; S_1^{\mathrm{cube}} \;\cup\; (S_1^{\mathrm{odd}} \cap S_2^{\mathrm{odd}})$$

where $\langle S_1^{\mathrm{prim}} \rangle$ is the multiplicative monoid generated by the prime numbers in S_1, and where the only non-trivial intersection is

$$\langle S_1^{\mathrm{prim}} \rangle \;\cap\; S_1^{\mathrm{cube}} = \{p_1^{3\alpha_1} \cdots p_s^{3\alpha_s} \mid p_i \in S_1^{\mathrm{prim}};\; \alpha_i \geq 1\}.$$

Remark 43

Using the theory of modular functions, several formulas for the number $a(n, 11)$ of representations of a given number n of the form $n = x^2 + 11y^2$ are derived by Petersson. They are based on Fourier expansions of theta series and count primitive as well as imprimitive representations. In particular, it is shown that

$$a(n, 11) \;=\; \tfrac{2}{3}\,\alpha(n, 11) \;+\; \tfrac{4}{3}\,\beta(n, 11)$$

where $\alpha(n, 11) = \sum_{d|n}(-1)^{(d-1)(n/d-1)}\left(\frac{d}{11}\right)$ involves Legendre symbols, and where $\beta(n, 11) = \sum_{(x,y)\in M} \operatorname{sign}(xy)\left(\frac{-1}{|xy|}\right)$ involves Jacobi symbols. Here the sum extends over the set M of all pairs $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ such that $x \equiv y \equiv 1 \pmod 6$ and $x^2 + 11y^2 = 12n$. Clearly, this formula is hard to evaluate in general, because it involves finding particular solutions of the equation $x^2 + 11y^2 = 12n$.

In comparison, the above theorem describes the set of numbers n having a primitive representation of the form $n = x^2 + 11y^2$ as the disjoint union of several special cases which are studied in greater detail in other parts of this paper.

As a consequence of the proof of this theorem, we can decompose S_1^{odd} further. We shall use the following subsets.

Definition 44

A number $n \in C$ is called **cubically reduced** if there is no cubic number $c \in S_1^{\mathrm{cube}} \setminus \{1\}$ such that $c \mid n$. For $i = 1, 2$, we denote the set of cubically reduced numbers in S_i^{odd} by S_i^{cro}.

With this terminology, we can decompose S_1^{odd} as follows.

Corollary 45

In the above setting, the following claims hold.

(a) Every number $n \in S_1^{\mathrm{odd}}$ has a uniquely determined decomposition $n = c\,\tilde{n}$ with $c \in S_1^{\mathrm{cube}}$ and $\tilde{n} \in S_1^{\mathrm{cro}}$.

(b) Every number $n \in S_1^{\mathrm{cro}} \cup S_2^{\mathrm{cro}}$ has a prime decomposition $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \cdot q_1^{\beta_1} \cdots q_t^{\beta_t}$ where $p_i \in S_1^{\mathrm{prim}}$, where $q_j \in S_2^{\mathrm{prim}}$, and where $\alpha_i, \beta_j \in \{1, 2\}$.

(c) A number n as in (b) is contained in $S_1^{\mathrm{cro}} \setminus S_2^{\mathrm{cro}}$ if and only if $t = 0$.

(d) A number n as in (b) is contained in $S_2^{\mathrm{cro}} \setminus S_1^{\mathrm{cro}}$ if and only if $s = 0$.

(e) A number n as in (b) is contained in $S_1^{\mathrm{cro}} \cap S_2^{\mathrm{cro}}$ if and only if $s \geq 1$ and $t \geq 1$.

To complete the discussion, we formulate a similar decomposition for the set S_2. Since the proof of the next proposition uses the same tools from Section 4 and proceeds in analogy to the proof of the above theorem and its corollary, we leave it to the interested reader.

Proposition 46

For the set S_2, the following claims hold.

(a) We have

$$S_2^{\mathrm{even}} \;=\; S_1^{\mathrm{even}} \cup 4\,S_1^{\mathrm{cube}} \cup 4\,\langle S_1^{\mathrm{prim}}\rangle \;=\; 4\,S_2^{\mathrm{odd}} \cup 4\,S_1^{\mathrm{cube}} \cup 4\,\langle S_1^{\mathrm{prim}}\rangle$$

where the unions are disjoint except for the union of S_1^{cube} and $\langle S_1^{\mathrm{prim}}\rangle$.

(b) The set S_2^{odd} is the disjoint union of $S_1^{\mathrm{odd}} \cap S_2^{\mathrm{odd}}$ and the set of all numbers $p_1^{\alpha_1} \cdots p_s^{\alpha_s} \cdot q_1^{\beta_1} \cdots q_s^{\beta_s}$ such that $p_i \in S_1^{\mathrm{prim}}$, $q_j \in S_2^{\mathrm{prim}}$, and $\beta_j = 3\gamma_j + \delta_j$ with $\delta_j \in \{0, 1, 2\}$ satisfying $\delta_1 + \cdots + \delta_t \equiv 1 \pmod 2$.