Journal of Mathematical Sciences 3 (2016) 107-119 **Betty Jones & Sisters Publishing**
ISSN 2372-5214 **http://www.bettyjonespub.com**

Linear Groups and Square Properties in Rings

Benjamin Fine[1], Gerhard Rosenberger[2]

1. Department of Mathematics, Fairfield University, Fairfield, Connecticut 06430, United States

2. Fachbereich Mathematik, University of Hamburg, 20146 Hamburg, Germany

Abstract: In [1] a proof was given of Fermat's Two-Square Theorem using the group theoretical structure of the classical modular group. This has been extended in many directions and to other square properties in general rings. In particular in [2] a two-square theorem was given for the Gaussian integers in terms of when i is a quadratic residue. In this note we examine and survey this technique and the corresponding results and extensions.

Keywords: Picard Group, Fermat's Two-Square Theorem, Gaussian Integers, sums of squares.

1. Introduction

The study of representations of natural numbers by quadratic forms is a fundamental area of elementary number theory. Classically the starting off point for this study was Fermat's Two-Square Theorem. This well-known result can be stated in several different equivalent ways (see [2]) but the version we start with in this article says that for a natural number n, then -1 is a quadratic residue modulo n if and only if there exists $a, b \in \mathbb{Z}$ with $(a, b) = 1$ and $n = a^2 + b^2$. In [3] a proof was given of Fermat's Two-Square Theorem using the structure of the classical modular group $M = PSL(2, \mathbb{Z})$ and was in some sense independent of anything but the most basic number theory. The method used in this proof was generalized in several different directions. Kern-Isberner and Rosenberger [4] and [5] considered representations of integers by the more general form $x^2 + Ny^2$ for various values of N. Fine [1], [6] and [7] using the classification of trace classes in M handled representations by many different quadratic forms. In [7] similar techniques using the generalized Picard group $\Gamma_1 = PGL(2, \mathbb{Z}[i])$ were utilized to prove a two-square theorem for the Gaussian integers. In particular it was shown that if $\alpha \in \mathbb{Z}[i]$ then i is a quadratic residue modulo α if and only if there exist relatively prime Gaussian integers a, b with $\alpha = a^2 + ib^2$. In addition the technique showed that any Gaussian integer can be written as a sum $a^2 + b^2$ or $i(a^2 + b^2)$ with $a, b \in \mathbb{Z}[i]$ and $(a, b) = 1$.

Finally in [6], [7] the sum of squares property in the integers $\mathbb{Z}$ was extended to a wider class of rings called **sum of squares rings**.

The purpose of this article is to describe the technique and to survey the many results. In section 2 we give the basic proof of Fermat's Two-Square Theorem which utilizes the free product structure of the classical modular group M. In section 3 we extend the method to handle a two-square theorem in the Gaussian integers. This involves the structure of the Picard group $PSL(2, \mathbb{Z}[i])$. In section 4 we present the result of Kern-isberner and Rosenberger on representations by the form $x^2 + Ny^2$. In section 5 we show how the classification of the trace classes in M leads to similar results for an infinite class of quadratic forms which are algorithmically computable. In the final section we look at extensions called sum of squares rings.

2. Fermat's Two-Square Theorem

Fermat's Two-Square Theorem can be stated in several different but equivalent ways (see [2]). Recall that an integer m is a **quadratic residue** modulo n if

Corresponding author: Benjamin Fine, Ph.D., research fields: group theory, number theory, cryptography. E-mail: ben1902@aol.com.

there exists a solution for $x^2 \equiv m \bmod n$. Fermat's two square theorem characterizes those integers n for which -1 is a quadratic residue modulo n. There are several versions of this result. For this article we recall the following.

Theorem 2.1. Let $n \in \mathbb{N}$. Then -1 is a quadratic residue modulo n if and only if there exists $a, b \in \mathbb{Z}$ with $(a, b) = 1$ such that $n = a^2 + b^2$.

In the standard proofs (see for example [2]) the congruence $x^2 \equiv -1$ is considered modulo primes and the difference in the situation for $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$ is examined. In [3] a direct proof of this result was given using the structure of the classical modular group (see also [2]). We first recall the standard proofs. After this we give some preliminary material on the Modular Group and then give the proof which shows the basic technique to be followed. This second proof is interesting since it is in some sense independent of number theory.

The standard proof of Fermat's Two-Square theorem, found in most textbooks (see [2]) has the following outline. In the course of developing this outline the several equivalent formulations of the theorem are presented. Detailed proofs of these preliminary results are in [2].

Considered first the case of primes.

Lemma 2.1. -1 is a quadratic residue modulo a prime p if and only if $p = 2$ or $p \equiv 1 \bmod 4$.

This result is now tied to sums of squares.

Lemma 2.2. If $p \equiv 1 \bmod 4$ then $p = a^2 + b^2$ with $(a, b) = 1$.

The result is then differentiated whether $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$.

Lemma 2.3. Suppose $n = a^2 + b^2$ and q is a prime divisor of n. If $q \equiv 3 \bmod 4$ then $q^2 | n$.

Putting these results together we get the following version of Fermat's Two-Square Theorem

Theorem 2.2. Suppose $n \geq 2$ has the prime decomposition

$$n = 2^{\alpha} p_1^{\beta_1} \cdots p_k^{\beta_k} q_1^{\gamma_1} \cdots q_t^{\gamma_t}$$

where $p_i \equiv 1 \bmod 4$ for $i = 1, \ldots, k$ and $q_j \equiv 3 \bmod 4$ for $j = 1, \ldots, t$. Then n can be expressed as the sum of two squares if and only if all the exponents γ_j of the primes congruent to $3 \bmod 4$ are even.

We now present a simple proof based on the structure of the classical Modular Group. The group $SL_2(\mathbb{Z})$ consists of 2×2 integral matrices of determinant one:

$$G = SL_2(\mathbb{Z}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix}; a, b, c, d \in \mathbb{Z}, ad - bc = 1\}.$$

$SL_2(\mathbb{Z})$ is called the **homogeneous modular group** and an element of $SL_2(\mathbb{Z})$ is called a **unimodular matrix**.

It is easy to see that the center $Z(G)$ consists of just $\pm I$ where I is the identity matrix. The **projective special linear group** denoted $PSL(2, \mathbb{Z})$ is the quotient

$$SL_2(\mathbb{Z})/Z(SL_2(\mathbb{Z})) = SL_2(\mathbb{Z})/\{I, -I\}.$$

Commonly $PSL_2(\mathbb{Z})$ is referred to as the **Modular Group** and denoted by M.

M arises in many different areas of mathematics including number theory, complex analysis and Riemann surface theory and the theory of automorphic forms and functions. M is perhaps the most widely studied single finitely presented group. Complete discussions of M and its structure can be found in the books **Integral Matrices** by M. Newman [8] and **Algebraic Theory of the Bianchi Groups** by B. Fine [9].

Since $M = PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{I, -I\}$ it follows that each element of M can be considered as $\pm A$ where A is a unimodular matrix. A **projective unimodular matrix** is then

$$\pm\begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}, ad - bc = 1.$$

The elements of M can also be considered as linear fractional transformations over the complex numbers

$$z' = \frac{az + b}{cz + d}, a, b, c, d \in \mathbb{Z}, ad - bc = 1.$$

Thought of in this way, M forms a **Fuchsian group** which is a discrete group of isometries of the non-Euclidean hyperbolic plane. The book by Katok [10]

gives a solid and clear introduction to such groups. This material can also be found in condensed form in [11].

We describe the abstract structure of the group M. First though we use it to give a direct proof of Fermat's Two-Square Theorem. We need the following lemma. Recall that the **trace** of a matrix A is the sum of its diagonal elements. Trace is preserved under conjugation so that $tr(A) = tr(T^{-1}AT)$ for any square matrices A and invertible T. Recall also that in a group G two elements g, g_1 are **conjugate** if there exists an $h \in G$ such that $h^{-1}gh = g_1$. Conjugation is an equivalence relation on a group and the equivalence classes are called **conjugacy classes**.

Lemma 2.4. Let A be a projective unimodular matrix with $tr(A) = 0$. Then A is conjugate within M to $X = \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. That is there exists $T \in M$ with $T^{-1}XT = A$.

Proof. Let $A = \pm\begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix}$. Let S be the set of conjugates of A within M so that

$$S = \{T^{-1}AT; T \in M\}.$$

Since conjugation preserves trace, S consists of matrices of trace zero. Let

$$Y = \pm\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

be an element of S with $|a|$ minimal. This exists from the well-ordering of $\mathbb{N} \cup \{0\}$. We show that a must equal zero.

Suppose $a \neq 0$ then

$$-a^2 - bc = 1 - bc = a^2 + 1|b||c| = a^2 + 1.$$

It follows then that $b \neq 0, c \neq 0$ and either $|b| < |a|$ or $|c| < |a|$. Assume first that $|c| < |a|$. We may assume that $a > 0$ and $c > 0$ since we may replace $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ by $\begin{pmatrix} -a & b \\ c & a \end{pmatrix}$. It follows then, that

$$0 < a - c < a.$$

Now conjugate Y by $T = \pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then $T^{-1} = \pm\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ and

$$T^{-1}YT = \pm\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & -a \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$
$$= \pm\begin{pmatrix} a - c & 2a + b - c \\ c & c - a \end{pmatrix}.$$

But then $0 < a - c < a$ contradicting the minimality of $|a|$.

If $b < a$ assuming $a > 0, b > 0$ conjugate Y by $T = \pm\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. Then $T^{-1} = \pm\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and

$$T^{-1}YT = \pm\begin{pmatrix} a - b & b \\ 2a + c - b & b - a \end{pmatrix}.$$

Again $0 < a - b < a$ contradicting the minimality of $|a|$.

Therefore in a minimal conjugate of A we must have $a = 0$ and hence $-bc = 1$. It follows that $b = \pm 1$ and $c = \mp 1$ and therefore

$$Y = \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = X$$

completing the proof. □

Now consider conjugates of X within M. Let $T = \pm\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then

$$T^{-1} = \pm\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

and

$$TXT^{-1} = \pm\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$
$$= \pm\begin{pmatrix} -(bd + ac) & a^2 + b^2 \\ -(c^2 + d^2) & bd + ac \end{pmatrix} \quad (1)$$

Therefore any conjugate of X must have form (1).

We now reprove Fermat's Two-Square Theorem.

Theorem 2.3. (Fermat's Two-Square Theorem) Let $n > 0$ be a natural number. Then $n = a^2 + b^2$ with $(a, b) = 1$ if and only if -1 is a quadratic residue modulo n.

Proof. Suppose -1 is a quadratic residue mod n. Then there exists an x with $x^2 \equiv -1 \bmod n$ or $x^2 = -1 + mn$. This implies that $-x^2 - mn = 1$ so that there must exist a projective unimodular matrix

$$A = \pm\begin{pmatrix} x & n \\ m & -x \end{pmatrix}.$$

The trace of A is zero so by Lemma 2.4 A is conjugate within M to X and therefore A must have form (1). Therefore $n = a^2 + b^2$ since $n > 0$. Further $(a, b) = 1$ since in finding form (1) we had $ad - bc = 1$.

Conversely suppose $n = a^2 + b^2$ with $(a, b) = 1$. Then there exists $c, d \in \mathbb{Z}$ with $ad - bc = 1$ and hence there exists a projective unimodular matrix

$$T = \pm\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then

$$TXT^{-1} = \pm\begin{pmatrix} \alpha & a^2 + b^2 \\ \gamma & -\alpha \end{pmatrix} = \pm\begin{pmatrix} \alpha & n \\ \gamma & -\alpha \end{pmatrix}.$$

This then has determinant one so

$$-\alpha^2 - n\gamma = 1\alpha^2 = -1 - n\gamma\alpha^2 \equiv -1 \bmod n.$$

Therefore -1 is a quadratic residue mod n. □

We now describe the group theoretical structure of both $SL_2(\mathbb{Z})$ and $M = PSL_2(\mathbb{Z})$. This structure can be developed with only minimal number theory.

Theorem 2.4. The group $SL_2(\mathbb{Z})$ is generated by the elements

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } Y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Further a complete set of defining relations for the group in terms of these generators is given by

$$X^4 = Y^3 = YX^2Y^{-1}X^{-2} = I.$$

In the language of combinatorial group theory we say that $SL_2(\mathbb{Z})$ has the **presentation**

$$< X, Y; X^4 = Y^3 = YX^2Y^{-1}X^{-2} = I >.$$

Proof. We first show that $SL_2(\mathbb{Z})$ is generated by X and Y, that is every matrix A in the group can be written as a product of powers of X and Y.

Let

$$U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then a direct multiplication shows that $U = XY$ and we show that $SL_2(\mathbb{Z})$ is generated by X and U which implies that it is also generated by X and Y. Further

$$U^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

so that U has infinite order.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Then we have

$$XA = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \text{ and } U^kA = \begin{pmatrix} a + kc & b + kd \\ c & d \end{pmatrix}$$

for any $k \in \mathbb{Z}$. We may assume that $|c| \leq |a|$ otherwise start with XA rather than A. If $c = 0$ then $A = \pm U^q$ for some q. If $A = U^q$ then certainly A is in the group generated by X and U. If $A = -U^q$ then $A = X^2U^q$ since $X^2 = -I$. It follows that here also A is in the group generated by X and U.

Now suppose $c \neq 0$. Apply the Euclidean algorithm to a and c in the following modified way:

$$a = q_0c + r_1$$
$$-c = q_1r_1 + r_2$$
$$r_1 = q_2r_2 + r_3$$

...

$$(-1)^n r_{n-1} = q_n r_n + 0$$

where $r_n = \pm 1$ since $(a, c) = 1$. Then

$$XU^{-q_n} \cdots XU^{-q_0}A = \pm U^{q_{n+1}} \text{ with } q_{n+1} \in \mathbb{Z}.$$

Then

$$A = X^m U^{q_0} XU^{q_1} \cdots XU^{q_n} XU^{q_{n+1}}$$

with $m = 0,1,2,3$; $q_0, q_1, \ldots, q_{n+1} \in \mathbb{Z}$ and $q_0 \cdots q_n \neq 0$. Therefore X and U and hence X and Y generate $SL_2(\mathbb{Z})$.

We must now show that

$$X^4 = Y^3 = YX^2Y^{-1}X^{-2} = I \qquad (2)$$

is a complete set of defining relations for $SL_2(\mathbb{Z})$ or that every relation on these generators is derivable from these (see [11] or [12] for a description of group presentations). It is straightforward to see that X and Y do satisfy these relations. Assume then that we have a relation

$$S = X^{\epsilon_1}Y^{\alpha_1}X^{\epsilon_2}Y^{\alpha_2} \ldots Y^{\alpha_n}X^{\epsilon_{n+1}} = I$$

with all $\epsilon_i, \alpha_j \in \mathbb{Z}$. Using the relations (2) we may transform S so that

$$S = X^{\epsilon_1}Y^{\alpha_1} \cdots Y^{\alpha_m}X^{\epsilon_{m+1}}$$

with $\epsilon_1, \epsilon_{m+1} = 0, 1, 2$ or 3 and $\alpha_i = 1$ or 2 for $i = 1, \ldots, m$ and $m \geq 0$. Multiplying by a suitable power of X we obtain

$$Y^{\alpha_1}X \cdots Y^{\alpha_m}X = X^{\alpha} = S_1$$

with $m \geq 0$ and $\alpha = 0,1,2$ or 3. Assume that $m \geq 1$ and let

$$S_1 = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}.$$

We show by induction that

$$a, b, c, d \geq 0, b + c > 0$$

or

$$a, b, c, d \leq 0, b + c < 0.$$

This claim for the entries of S_1 is true for

$$YX = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \text{ and } Y^2X = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Suppose it is correct for $S_2 = \begin{pmatrix} a_1 & -b_1 \\ -c_1 & d_1 \end{pmatrix}$. Then

$$YXS_2 = \begin{pmatrix} a_1 & -b_1 \\ -(a_1 + c_1) & b_1 + d_1 \end{pmatrix} \text{ and}$$

$$Y^2XS_2 = \begin{pmatrix} -a_1 - c_1 & b_1 + d_1 \\ c_1 & d_1 \end{pmatrix}.$$

Therefore the claim is correct for all S_1 with $m \geq 1$. This gives a contradiction, for the entries of X^α with $\alpha = 0,1,2$ or 3 do not satisfy the claim. Hence $m = 0$ and S can be reduced to a trivial relation by the given set of relations. Therefore they are a complete set of defining relations and the theorem is proved. □

Corollary 2.1. The Modular Group $M = PSL_2(\mathbb{Z})$ has the presentation

$$M = < x, y; x^2 = y^3 = 1 >.$$

Further x, y can be taken as the linear fractional transformations

$$x: z' = -\frac{1}{z} \text{ and } y: z' = -\frac{1}{z+1}.$$

Proof. The center of $SL_2(\mathbb{Z})$ is $\pm I$. Since $x^2 = -I$ setting $x^2 = I$ in the presentation for $SL_2(\mathbb{Z})$ gives the presentation for M. Writing the projective matrices as linear fractional transformations gives the second statement. □

We now give a different and direct proof of Corollary 2.1 using a ping-pong argument. First observe that $x(r) > 0$ if $r \in \mathbb{R}$ with $r < 0$ and $y(s) < 0$, $y^2(s) < 0$ if $s \in \mathbb{R}$ and $s > 0$.

Now let $g \in M$ and g not conjugate to a power of x or y. Using the relations $x^2 = y^3 = 1$ we may transform g so that, possibly after a suitable conjugation,

$$g = y^{\epsilon_1} x \cdots x y^{\epsilon_{n+1}}, n \in \mathbb{N}$$

with $1 \leq \epsilon_i \leq 2$ for $i = 1, \ldots, n+1$.

Let $t \in \mathbb{R}$ with $t > 0$. Then $y^{\epsilon_{n+1}}(t) < 0$ and $xy^{\epsilon_{n+1}}(t) > 0$. Further $y^{\epsilon_n} xy^{\epsilon_{n+1}}(t) < 0$. Finally

$$g(t) = y^{\epsilon_1} x \cdots x y^{\epsilon_{n+1}}(t) < 0.$$

This shows that $g \neq 1$ and proves Corollary 2.1.

Further a straightforward calculation shows that a projective unimodular matrix has order 2 if and only if its trace is zero. Combining these two facts gives an easy proof of Lemma 2.4 which was the crux of the proof of Fermat's Two-Square Theorem.

3. i as a Quadratic Residue in $\mathbb{Z}[i]$

The **Gaussian integers** or **complex integers** are the ring $\mathbb{Z}[i]$. Using the standard complex norm, these form a Euclidean domain and hence a unique factorization domain.

The **Picard group** is the group $\Gamma = PSL(2, \mathbb{Z}[i])$. This consists of linear fractional transformations

$$z' = \frac{az + b}{cz + d} \text{ with } a, b, c, d \in \mathbb{Z}[i], ad - bc = 1.$$

Since -1 has a square root within $\mathbb{Z}[i]$, linear transformations with determinant -1, such as $z' = -z$, are also in Γ.

Each linear transformation corresponds to a projective matrix

$$\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PSL}(2, \mathbb{Z}[i]) \text{ with } ad - bc = 1.$$

Multiplication of linear transformations is done via matrix multiplication. For further information on these see [2] or [9].

Within the Gaussian integers $\mathbb{Z}[i]$ we have $i^2 = -1$. Hence -1 is a quadratic residue modulo any Gaussian integer α. Using the technique employed in section 2 for the Modular group, Fine and Rosenberger [13] obtain a two-square result for Gaussian integers α for which i is a quadratic residue. In particular:

Theorem 3.1. Let $\alpha \in \mathbb{Z}[i]$. Then i is a quadratic residue modulo α if and only if there exists relatively prime Gaussian integers a, b such that $\alpha = a^2 + ib^2$.

We let $\Gamma_1 = PGL(2, \mathbb{Z}[i])$, the extended Picard group. Note that if $A \in \Gamma_1$ then $\det(A) = 1$ or $\det(A) = i$. For the proof, we first need the following lemma.

Lemma 3.1. Let $A \in PGL(2, \mathbb{Z}[i])$. Then if trace $(A) = 0$ and $\det(A) = i$ we have that A is conjugate within Γ_1 to

$$X = \pm\begin{pmatrix} 0 & i \\ -1 & 0 \end{pmatrix}.$$

That is, there exists $T \in \Gamma_1$ with $T^{-1}XT = A$.

Proof. Let $A = \pm\begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix}$ with $-\alpha^2 - \beta\gamma = i$.

Let S be the set of conjugates of A within Γ_1 so that

$$S = \{T^{-1}AT; T \in M\}.$$

Since conjugation preserves both trace and determinant, S consists of matrices of trace zero and determinant i. Let

$$Y = \pm\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

and

$$-a^2 - bc = i$$

be an element of S with $|a|$ minimal. This exists since the norms of Gaussian integers are rational integers and then from the well-ordering of $\mathbb{N} \cup \{0\}$. We show that a must equal zero.

Assume that $a \neq 0$. If either $b = 0$ or $c = 0$ then $a^2 = -i$. However $\sqrt{i}$ is not a Gaussian integer and therefore we may assume that $b \neq 0$ and $c \neq 0$.

We then have

$$-a^2 - bc = i - bc = a^2 + i|b||c| = |a^2 + i| \leq |a|^2 + 1.$$

It follows then that $b \neq 0, c \neq 0$ and either $|b| \leq |a|$ or $|c| \leq |a|$. Assume first that $|c| \leq |a|$.

By the division algorithm within $\mathbb{Z}[i]$ we have $a - qc = r$ with $r = 0$ or $|r| < |c| \leq |a|$.

Now conjugate Y by $T = \pm\begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}$. Then $T^{-1} = \pm\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}$ and

$$T^{-1}YT = \pm\begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & -a \end{pmatrix}\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} = \pm\begin{pmatrix} a - cq & * \\ & cq - a \end{pmatrix}.$$

But then $0 \leq |a - qc| < |c| \leq |a|$ contradicting the minimality of $|a|$.

If $|b| \leq |a|$ then we have $a - qb = r$ with $r = 0$ or $|r| < |b| \leq |a|$. Now conjugate Y by $T = \pm\begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix}$. Then $T^{-1} = \pm\begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix}$ and

$$T^{-1}YT = \pm\begin{pmatrix} a - qb & * \\ & qb - a \end{pmatrix}.$$

Again $0 < |aq - b| < |a|$ contradicting the minimality of $|a|$.

Therefore in a minimal conjugate of A we must have $a = 0$ and hence $-bc = i$. It follows that $b = \pm i$ and $c = \mp 1$ or $b = \pm 1$ and $c = \mp i$ and . If $b = \mp i$ and $c = \pm 1$ then

$$\pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -i & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \pm\begin{pmatrix} 0 & i \\ -1 & 0 \end{pmatrix}.$$

Hence let $b = \pm i$ and $c = \mp 1$. Then

$$y = \pm\begin{pmatrix} 0 & i \\ -1 & 0 \end{pmatrix} = x$$

completing the proof. □

Using an analogous proof of the previous lemma applied to matrices of trace 0 and determinant 1 gives the following result.

Lemma 3.2. Let $A \in PGL(2, \mathbb{Z}[i])$. Then if trace $(A) = 0$ and $\det(A) = 1$ we have that A is conjugate within Γ_1 to

$$X = \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

That is there exists $T \in \Gamma_1$ with $T^{-1}XT = A$.

We can now prove the two-square theorem for thr Gaussian integers. It follows the same format as the Modular group proof of Fermat's Two-Square theorem.

Proof. (Theorem 3.1) Let $\alpha \in \mathbb{Z}[i]$ and suppose that i is a quadratic residue modulo α. Then there exists $x \in Z[i]$ such that $x^2 \equiv i \bmod \alpha$ so that there exists

$\gamma \in \mathbb{Z}[i]$ with $x^2 - i = \alpha\gamma$ or $-x^2 - \alpha\gamma = i$. This implies that the projective matrix

$$A = \pm\begin{pmatrix} x & \alpha \\ \gamma & -x \end{pmatrix}$$

is in Γ_1 with determinant i. Since it has trace 0, then from Lemma 3.1 it follows that A is conjugate within Γ_1 to

$$X = \pm\begin{pmatrix} 0 & i \\ -1 & 0 \end{pmatrix}.$$

Now consider conjugates of X within Γ_1. Let

$$T = \pm\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Assume first that $\det(T) = 1$ so that

$$T^{-1} = \pm\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Then computing the conjugate of X by T we find

$$TXT^{-1} = \pm\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & i \\ -1 & 0 \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$= \pm\begin{pmatrix} * & b^2 + ia^2(1) \\ -(d^2 + ic^2) & * \end{pmatrix} \qquad (1)$$

Therefore any conjugate of X by a projective matrix of determinant 1 must have form (1).

It follows that if $\det(T) = 1$ the matrix A must have this form so that $\alpha = b^2 + ia^2$ or $\alpha = -b^2 - ia^2 = (ib)^2 + i(ia)^2$. Further since $ad - bc = 1$ it follows that $(a, b) = 1$.

Assume next that $\det(T) = i$ so that

$$T^{-1} = \pm(-i)\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Then computing the conjugate of X by T we find

$$TXT^{-1} = \pm(-i)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & i \\ -1 & 0 \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$= \pm\begin{pmatrix} * & a^2 - ib^2 \\ -(c^2 - id^2) & * \end{pmatrix} \qquad (2)$$

Therefore any conjugate of X by a projective matrix of determinant i must have form (3).

It follows that if $\det(T) = i$ the matrix A must have this form so that $\alpha = a^2 - ib^2$ or $\alpha = (ia)^2 - i(ib)^2$. Further since $ad - bc = i$ it follows that $(a, b) = 1$.

Putting both cases together we have that if $\alpha \in \mathbb{Z}[i]$ and i is a quadratic residue modulo α then there exists $a, b \in \mathbb{Z}[i]$ with $(a, b) = 1$ and $\alpha = a^2 + ib^2$ or $\alpha = a^2 - ib^2$. However if $\alpha = a^2 - ib^2$ then $lpha = a^2 + i(ib)^2$. Therefore α is always of the form

$$\alpha = a^2 + ib^2 \text{ with } a, b \in \mathbb{Z}[i].$$

Conversely suppose that

$$\alpha = b^2 + ia^2$$

with $(a, b) = 1$. Since $(a, b) = 1$ there exists $x, y \in \mathbb{Z}[i]$ with $ax + by = 1$. It follows that the projective matrix

$$T = \pm\begin{pmatrix} a & b \\ -y & x \end{pmatrix}$$

is in Γ_1 with determinant 1. Hence $TXT^{-1} \in \Gamma_1$ with $X = \begin{pmatrix} 0 & i \\ -1 & 0 \end{pmatrix}$. Conjugating X by T and computing we get.

$$TXT^{-1} = \pm\begin{pmatrix} a & b \\ -y & x \end{pmatrix}\begin{pmatrix} 0 & i \\ -1 & 0 \end{pmatrix}\begin{pmatrix} x & -b \\ y & a \end{pmatrix})$$

$$= \begin{pmatrix} * & b^2 + ia^2 \\ -(x^2 + iy^2) & * \end{pmatrix}.$$

Therefore there exists a matrix S with determinant i and trace 0 such that S is conjugate to X which has α in its upper right hand entry; that is,

$$S = \pm\begin{pmatrix} x & \alpha \\ \gamma & -x \end{pmatrix}.$$

Since the determinant is i we have

$$x^2 - \alpha\gamma = i \text{ so that } x^2 = i + \alpha\gamma.$$

Hence i is a quadratic residue modulo α, completing the theorem. □

Within the Gaussian integers, $i^2 = -1$ and therefore -1 is a quadratic residue modulo α for any $\alpha \in \mathbb{Z}[i]$ with $\alpha \neq 0$ and α not a unit. Applying exactly the same proofs we obtain further that every nonzero, nonunit Gaussian integer is either the sum of two relatively prime squares or i times the sum of two relatively prime squares.

Theorem 3.2. Let $\alpha \in \mathbb{Z}[i]$ with $\alpha \neq 0$ and α not a unit. Then there exists $a, b \in \mathbb{Z}[i]$ with $(a, b) = 1$ so that $\alpha = a^2 + b^2$ or $\alpha = i(a^2 + b^2)$.

Proof. Suppose that $\alpha \in \mathbb{Z}[i]$ with $\alpha \neq 0$ and α not a unit. Then -1 is a quadratic residue mod α and hence there exists $x, \gamma \in \mathbb{Z}[i]$ with $x^2 = -1 + \alpha\gamma$. Therefore the projective matrix

$$S = \pm\begin{pmatrix} x & \alpha \\ -\gamma & -x \end{pmatrix} \in \Gamma_1.$$

Since the determinant is 1, and the trace is 0, it follows from Lemma 3.2 that S must be conjugate within Γ_1 to

$$Y = \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

First conjugate Y by $T \in \Gamma_1$ with $\det(T) = 1$ so that

$$T^{-1} = \pm\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Then we find

$$\begin{aligned} S &= TYT^{-1} \\ &= \pm\begin{pmatrix} a & b(5) \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1(6) \\ -1 & 0 \end{pmatrix}\begin{pmatrix} d & -b(7) \\ -c & a \end{pmatrix} \\ &= \pm\begin{pmatrix} * & b^2 + a^2 \\ -(d^2 + c^2) & * \end{pmatrix} \end{aligned} \quad (3)$$

Therefore any conjugate of Y by a projective matrix of determinant 1 must have form (3).

It follows that if $\det(T) = 1$ the matrix A must have this form so that $\alpha = a^2 + b^2$ or $\alpha = (ia)^2 + (ib)^2$. Further since $ad - bc = 1$ it follows that $(a, b) = 1$.

Next conjugate Y by $T \in \Gamma_1$ with $\det(T) = i$ so that

$$T^{-1} = \pm(-i)\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Then we find

$$\begin{aligned} S = TYT^{-1} &= \pm(-i)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= \pm\begin{pmatrix} * & i(b^2 + a^2) \\ -i(d^2 + c^2) & * \end{pmatrix} \end{aligned} \quad (4)$$

Therefore any conjugate of Y by a projective matrix of determinant 1 must have form (4).

It follows that if $\alpha \neq 0$ and α is not a unit then the result follows; that is,

$$\alpha = a^2 + b^2 \text{ or } \alpha = i(a^2 + b^2)$$

for some $a, b \in \mathbb{Z}[i]$ with $(a, b) = 1$. □

The crux of the proof of both the original Fermat Two-Square Theorem and the analogous result in the Gaussian integers was the classification of the conjugacy class of elements of trace 0. We will extend this further in section 5 however in section 2 we discussed that this could also be discerned from the group theoretical structure of the Modular group as a free product. In a similar manner the result in the Gaussian integers can also be recovered from the gorup theoretical structure of the Picard group which is more complicated.

The Picard group $\Gamma = PSL(2, \mathbb{Z}[i])$ has the presentation (see [9] and [11])

$$\begin{aligned} < a, \ell, t, u; a^2 = \ell^2 = (a\ell)^2 = (t\ell)^2 = (u\ell)^2 = (at)^3 \\ = (ua\ell)^3 = 1, [t, u] = 1 > \end{aligned}$$

where the transformations a, ℓ, t, u are

$$a: z' = -\frac{1}{z}, \ell: z' = -z, t: z' = z + 1, u: z' = z + i.$$

From this presentation it was proved that (see [9]) that Γ has a free product with amalgamation structure built up from finite groups. In the following theorem, S_3 is the symmetric group on 3 symbols, A_4 is the alternating group on 4 symbols, D_2 is the dihedral group of order 4 and M is the classical modular group $PSL(2, \mathbb{Z})$.

Theorem 3.3. The group $\Gamma = PSL(2, \mathbb{Z}[i])$ is given group theoretically as the free product with amalgamation

$$\Gamma = G_1 \underset{M}{\star} G_2$$

where

$$G_1 = S_3 \underset{\mathbb{Z}_3}{\star} A_4$$

$$G_2 = S_3 \underset{\mathbb{Z}_2}{\star} D_2$$

and M is the classical modular group with $M = \mathbb{Z}_2 \star \mathbb{Z}_3$.

In [6] and [9] this presentation was used to do an extensive examination of the group theoretical properties of Γ. For more information on this presentation see [11].

Using this structure, the classification of elements of trace zero can be reobtained,

4. The Diophantine Equation $n = x^2 + Ny^2$

These types of group theoretical proofs of two-square results can be extended in several directions. Kern-Isberner and Rosenberger [4], [5] considered groups $G(\sqrt{N})$ consisting of all projective matrices of U of the following two types:

$$(1)U = \begin{pmatrix} a & b\sqrt{N} \\ c\sqrt{N} & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}, N \in \mathbb{N}, ad - Nbc = 1$$

or

$$(2)U = \begin{pmatrix} a\sqrt{N} & b \\ c & d\sqrt{N} \end{pmatrix}, a, b, c, d \in \mathbb{Z}, N \in \mathbb{N}, Nad - bc = 1.$$

If $N \geq 2$ then

$$H(\sqrt{N}) = \{U \in G(\sqrt{N}) : U \text{ is of type } (1)\}$$

is a normal subgroup of index 2 in $G(\sqrt{N})$. That is:

$G(\sqrt{N}) = H(\sqrt{N}) \cup XH(\sqrt{N})$ where $X = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

The group $G(\sqrt{N})$ is a Fuchsian group and group theoretically a free product of cyclic groups.

They then proved the following results.

Theorem 4.1. Let $N \in \{1,2,3,4\}$ and let n be a positive integer relatively prime to N.

(1) Let $N \in \{1,2,4\}$. If $-N$ is a quadratic residue mod n then n can be written as $n = x^2 + Ny^2$ with $x, y \in \mathbb{Z}$.

(2) Let $N = 3$. If -3 is a quadratic residue mod n and n is a quadratic residue mod 3 then n can be written as $n = x^2 + 3y^2$ with $x, y \in \mathbb{Z}$.

Conversely if $n = x^2 + Ny^2$ with $x, y \in \mathbb{Z}$ and $(x, y) = 1$ then $-N$ is a quadratic residue mod n and n is a quadratic residue mod N.

The proof is quite straightforward and follows the lines of the Modular group proof. For $N = 3$ the condition that n is a quadratic residue mod 3 is necessary to exclude the conjugates of $\pm \begin{pmatrix} \sqrt{3} & 2 \\ -2 & -\sqrt{3} \end{pmatrix}$. Hence, with the given conditions, every element of order 2 is conjugate to X.

Theorem 4.2. If

$N \in \{5,6,7,8,9,10,12,13,16,18,22,25,28,37,58\}$

and $n \in \mathbb{N}$ with $(n, N) = 1$ then:

(1) Suppose $N \neq 7$. If $-N$ is a quadratic residue mod n and n is a quadratic residue mod N then n can be written as $n = x^2 + Ny^2$ with $x, y \in \mathbb{Z}$. Conversely if $n = x^2 + Ny^2$ with $x, y \in \mathbb{Z}$ and $(x, y) = 1$ then $-N$ is a quadratic residue mod n and n is a quadratic residue mod N.

(2) Suppose $N = 7$. If n is odd and -7 is a quadratic residue mod n then n can be written as $n = x^2 + 7y^2$ with $x, y \in \mathbb{Z}$.

Conversely if $n = x^2 + 7y^2$ with $x, y \in \mathbb{Z}$ and $(x, y) = 1$ then -7 is a quadratic residue mod n.

The key point in proof of Theorem 4.2 is the following lemma.

Lemma 4.1. (see [4]) Let $N \geq 5$ and let $m(N)$ be the number of conjugacy classes of elements of order 2 in $XH(\sqrt{N})$. The the following hold:

(1) $m(n) = 4\epsilon(n)h(-4N)$ where

$\epsilon(n) = \frac{1}{4}$ if N is not congruent to 3 mod 4

$\epsilon(n) = \frac{1}{3}$ if $N \equiv 3 \bmod 4$

$\epsilon(n) = \frac{1}{2}$ if $N \equiv 7 \bmod 8$

and $h(-4N)$ is the number of integral primitive positive definite binary quadratic forms of discriminant $-4N$.

(2) The following are equivalent:

(a) $m(N) = 2$

(b) $N = 5,6,7,8,9,10,12,13,16,18,22,25,28,37,58$.

The exception for $N = 7$ in Theorem 4.2 is explained by the fact that 7 is the only one among the numbers given in Theorem 4.2 with $h(-4N) = 1$.

5. Quadratic Forms Over $\mathbb{Z}$

The crux of the Modular Group proof of Fermat's Two-Square Theorem is that within M any projective matrix of trace 0 must be conjugate to

$$X = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Since conjugate matrices must have the same trace it follows that the conjugacy classes in M are all separated by trace. A **trace class** is a set of conjugate matrices all of the same trace. From the above there is only one trace class in M in trace 0 and this class has a trace class representative of X.

In [6] an effective algorithm was determined to find for any $d \in \mathbb{N}$ all the trace classes in M for trace d. Using this the following wide generalization of Fermat's Two-Square Theorem was proved.

Theorem 5.1. Given a positive integer $d \neq 2$, there exists a finite number $h(d)$ of integral quadratic forms

$$f_{1,d}(x,y), f_{2,d}(x,y), \ldots, f_{h(d),d}(x,y)$$

each of discriminant d^2-4 such that for any integer n the equation $x^2+dx+1=0$ is solvable modulo n if and only if $n = f_{i,d}(a,b)$ for some $i = 1,\ldots,h(d)$ and some integers a,b with $(a,b)=1$. Further:

(a) For each $d \neq 2$ there exists an effective procedure to explicitly determine a set of $f_{i,d}$

(b) $h(d)$ = the ideal class number of $\mathbb{Q}(\sqrt{d^2-4})$ = the number of trace classes in trace d

(c) For each d the set of the $f_{i,d}$ is unique in the following sense: If $n = f(a,b)$ for some integral quadratic form of discriminant d^2-4 then $x^2+dx+1=0$ is solvable mod n and there is an equivalence relation on quadratic forms of discriminant d^2-4 such that $f(x,y)$ is equivalent to some $f_{i,d}(x,y)$.

In this context Fermat's Two-Square Theorem is the case $d=0$ with the quadratic form $f(x,y)=x^2+y^2$. For the proof of the theorem we refer to [6]. The proof depends upon the aforementioned algorithm to determine trace classes. We discuss this a bit and then give an example exhibiting the quadratic forms.

As mentioned in section 2, group theoretically the Modular Group is the free product

$$M = < x; x^2 = 1 > * < y; y^3 = 1 >.$$

Here we can identify x,y with the projective matrices $x = \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, y = \pm\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$.

For material on combinatorial group theory we refer to [12].

Group theoretically this implies that any element $g \in M$ has a unique representation as a word $W(x,y)$ in x and y. That is

$$g = x^{i_1}y^{j_1}\cdots x^{i_1}y^{j_n}$$

where $i_k = 0,1$ and $j_k = 0,1,2$ for $k = 1,\ldots,n$. A non-trivial word $W(x,y)$ in M is **cyclically reduced** If $W \neq W_1W_2W_1^{-1}$ for other non-trivial words W_1, W_2, In the Modular group M this is equivalent to $W(x,y)$ not beginning with x and ending with x or beginning with y and ending with $y^2 = y^{-1}$ or beginning with y^{-1} and ending with y. An element of M is conjugate to a word in cyclically reduced form. Further if two words W_1, W_2 are cyclically reduced then they are conjugate if and only if w_1 is a cyclic permutation of W_2 (see [12]).

We say that a word $W(x,y) \in M$ is in **block reduced form** if $W(x,y)$ begins with x and ends with either y or y^2. A piece of the form (xy) or (xy^2) is called a **block**. The **block length** of a word $W(x,y)$ in block reduced form is the number of blocks in $W(x,y)$. We first have

Lemma 5.1. Every element of M is conjugate to either x or y or y^2 or a word in block reduced form.

A word $W(x,y) \in M$ is in **standard block reduced form** if $W(x,y)$ if it has one of the following forms,

(a) $W = (xy)^n$ for some integer n

(b) $W = (xy^2)^n$ for some integer n

(c) $W = ((xy)^n(xy^2)^k)^t$ for some integers n,k,t

(d) $W = (xy)^{a_1}(xy^2)^{b_1}\cdots(xy)^{a_k}(xy^2)^{b_k}$ where $a_1 = \max\{a_i\}$. If $a_1 = a_i$ for some i then $b_1 \geq b_i$. If $b_i = b_1$ then b $_2 \geq b_{i+1}$ and so on. (The largest occurrence of (xy) is in the front and then the ordering goes to the occurences of (xy^2).)

This definition imposes an ordering on words in standard block reduced form. Any word in block reduced form is a cyclic permutation of some word in stanbdard block reduced form. Therefore we have the following classification of the trace clsses in M.

Theorem 5.2. The trace classes in M are in one to one correspondence with words in standard block reduced form together with $\{x\},\{y\},\{y^2\}$.

The matrices corresponding to standard block reduced words together with the matrices for $\{x\},\{y\},\{y^2\}$ provide class representatives of each trace class.

What is left to present the trace class algorithm is to tie block length to trace. This is done in the following theorem (cite{F3).

Theorem 5.3. Let $W(x,y)$ be a word in M in block reduced form and of block length n then:

(a) The projective matrix corresponding to W has only positive entries.

(b) If $W \neq (xy)^b$ and $W \neq (xy^2)^k$ then the trace of W is greater than or equal to $n+1$

We then get the following algorithm which effectly finds a minimal trace class representative for each trace class.

Theorem 5.4. Given $d \in \mathbb{N}$ the following algorithm provides a trace class represenative for each trace class in trace d.

(a) If $d = 0$ the representative is x.

(b) If $d = 1$ the representatives are y and y^2.

(c) If $d = 2$ there an infinitely many trace classes. The distinct words $(xy)^n$ and $(xy^2)^n$ as n runs over the positve integers provide the representatives.

(d) If $d > 2$ then:

(i) List all words in standard block reduced form of length $(d-1)$ or less.

(ii) Determine the traces of each word on the list determined in (i). Each word in the list which has trace d determines a representative and this gives a complete list.

We note that in a private communication (see [6]) R. Kulkarni described an alternative algorithm.

In trace d, by examing the form of each trace class representative, as was done for the proof of Fermat's Two-Square Theorem in trace 0, we obtain the quadratic forms given in Theorem 3.1. Here we present an example (proofs are in [6]).

Trace	Number of Classes	Represenatives	Quadratic Forms
1	1	$\pm\begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}$	x^2+xy+y^2
3	1	$\pm\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}$	x^2-xy-y^2
4	2	$\pm\begin{pmatrix}3 & 1\\ 1 & 1\end{pmatrix}$	$x^2-2xy-2y^2$
		$\pm\begin{pmatrix}3 & 2\\ 1 & 1\end{pmatrix}$	$2x^2-2xy-y^2$
5	2	$\pm\begin{pmatrix}4 & 1\\ 3 & 1\end{pmatrix}$	$x^2-3xy-3y^2$
		$\pm\begin{pmatrix}4 & 3\\ 1 & 1\end{pmatrix}$	$3x^2-3xy-y^2$
6	3	$\pm\begin{pmatrix}5 & 1\\ 4 & 1\end{pmatrix}$	$x^2-4xy-4y^2$
		$\pm\begin{pmatrix}5 & 4\\ 1 & 1\end{pmatrix}$	$4x^2-4xy-y^2$
		$\pm\begin{pmatrix}5 & 2\\ 2 & 1\end{pmatrix}$	$2x^2-4xy-2y^2$

6. Sum of Squares Rings

For many commutative rings with identity R the structure of $PSL(2,R)$ has many similarities with the classicial Modular Group M. This was exploited in [7] to examine what were called sum of squares rings. These are rings which satisfy Fermat's Two-Square Theorem in the form of Theorem 1.1. In [6] it was proved that the class of sum of squares rings is extensive. A **gcd ring** is a commutative ring with identity where

any two elements have a greatest common divisor. Note that the concept of quadratic residues can be defined in any gcd ring.

A **sum of squares ring** is a gcd ring R satisfying:

(1) SS1: If $r \in R$ and -1 is a quadratic residue mod r then $r = \pm(u^2 + v^2)$ for some elements $u, v \in R$.

(2) SS2: If $r = u^2 + v^2$ for elements $u, v \in R$ with $(u, v) = 1$, then -1 is a quadratic residue mod r.

Hence Fermat's Two-Square Theorem asserts that the integers $\mathbb{Z}$ are a sum of squares ring. Following the analogous proof of Fermat's Two-Square Theorem using the Modular Group it can be shown that for any ring R for which $PSL(2, R)$ has only one trace class in trace 0, then R satisfies SS1 and further in any ring R where gcd's are linearly expressible then R satisfies SS2. From this we get the following.

Theorem 6.1. A Euclidean domain D with trivial units and char$(D) \neq 2$ is a sum of squares ring if its norm function is subadditive and $0 \neq N(b) \leq N(a)$ implies $N(a + kb) \leq N(a)$ for some $k \in D$.

In examining this theorem carefully we can provide a wide array of concrete examples of sum of squares rings. For proofs in each of the individual cases we refer to [6]. In particular:

Theorem 6.2. The following are all sum of squares rings:

(1) $\mathbb{Z}_{p^n}$ the ring of integers modulo p^n where p is a prime congruent to $3 \bmod 4$.

(2) The polynomial ring $K[x]$ where K is a field with -1 not a square and for which $PSL(2, K)$ has only one conjugacy class in trace 0.

(3) The polynomial ring $\mathbb{Z}_p[x]$ where p is a prime congruent to $3 \bmod 4$ and $\mathbb{Z}_p$ is the finite field of order p.

(4) The polynomial ring $F[x]$ where F is an ordered field in which every positive element has a square root. In particular $\mathbb{R}[x]$ and $A[x]$ where $\mathbb{R}$ is the real field and A is the field of real algebraic numbers over $\mathbb{Q}$.

Finally we would like to thank Anja Moldenhauer for her assistance in preparing and editing the paper.

References

[1] B. Fine. Sums of squares rings, Can. J. Math 29 (1977) 159-160.

[2] B. Fine, G. Rosenberger, Number Theory: An Introduction via the Distribution of Primes, Birkhauser, 2006.

[3] B. Fine, A note on the two-square theorem, Can. Math. Bulletin 20 (1977) 93-94.

[4] G. Kern-Isberner, G. Rosenberger A note on numbers of the form $n = x^2 + Ny^2$, Arch. Math. 43 (1984) 148-156.

[5] G. Kern-Isberner, G. Rosenberger, Einige Bemerkungen über Untergruppen der PSL (2,ℂ), Resultate der Mathematik 6 (1983) 40-47.

[6] B. Fine. Trace classes and quadratic forms in the modular group, Can. Math, Bull. 37 (1994) 202-212.

[7] B. Fine, Cyclotomic equations and square properties in rings, Int. J. Nath. and Math. Sci. 9 (1986) 89-95.

[8] M. Newman, Integral Matrices, Academic Press, 1972.

[9] B. Fine, The Algebraic Theory of the Bianchi Groups, Marcel Dekker, 1989

[10] S. Katok, Fuchsian Groups, Chicago Lecture Notes in Mathematics, 1992

[11] B. Fine, G. Rosenberger, Algebraic Generalizations of Discrete Groups, Marcel Dekker, 2001.

[12] W. Magnus, A. Karrass, D. Solitar, Combinatorial Group Theory, Wiley-Interscience, 1966.

[13] B. Fine, G. Rosenberger, i as a Quadratic Residue in the Gaussian Integers: Computational Models of Rationality Tributes, College Publications 29 (2016) 23-31.