Canad. Math. Bull. Vol. **37** (2), 1994 pp. 202–212

TRACE CLASSES AND QUADRATIC FORMS IN THE MODULAR GROUP

BENJAMIN FINE

ABSTRACT. The Modular Group M is $\mathrm{PSL}_2(\mathbb{Z})$ the group of linear fractional transformations with integral entries and determinant one. M has been of great interest in many diverse fields of Mathematics, including Number Theory, Automorphic Function Theory and Group Theory. In this paper we give an effective algorithm to determine, for each integer d, a complete set of representatives for the trace classes in trace d. This algorithm depends on the combinatorial group theoretic structure of M. It has been subsequently extended by Sheingorn to the general Hecke groups. The number $h(d)$ of trace classes in trace d is equal to the ideal class number of the field $\mathbb{Q}(\sqrt{d^2-4})$. The algorithm mentioned above then provides a new straightforward computational procedure for determining $h(d)$. Finally as an outgrowth of the algorithm we present a wide generalization of the Fermat Two-Square theorem. This last result can also be derived from classical work of Gauss.

1. **Introduction.** Fermat's two-square theorem in its general form states that -1 is a quadratic residue modulo n—or equivalently the equation $x^2+1=0$ is solvable modulo n—if and only if $n=u^2+v^2$ for some integers u,v with $(u,v)=1$. In [3] a proof of this was given which involved the group theoretical structure of the Modular Group $M = \mathrm{PSL}_2(\mathbb{Z})$ and which was in a sense independent of number theory. This was generalized in [4], [5] to show that many rings—called *sum of squares rings*—satisfy a Fermat's two-square theorem. Using similar techniques Rosenberger and Kern-Isberner [9] further generalized this to different equations.

In this paper we present an effective algorithm, based on the combinatorial group theoretic structure of M, to determine a complete set of representatives for the trace classes for any trace d. It has been pointed out to us by M. Sheingorn that this algorithm can be extended to the Hecke Groups in general [13]. This algorithm then gives a new straightforward technique for counting $h(d)$, the ideal class number of the field $\mathbb{Q}(\sqrt{d^2-4})$. While much work has gone into determining the values of $h(d)$ (see [2], [12], [15], [16]) and the structure of so-called non-parabolic subgroups this is as far as we can determine the first group theoretical algorithm to give specific hyperbolic class representatives.

As a further consequence of this algorithm we give the following wide generalization of Fermat's two-square theorem which can also be derived from work of Gauss [8]. Given a positive integer d, there exists a finite set $f_{1,d}(x,y), f_{2,d}(x,y), \ldots, f_{h(d),d}(x,y)$ of integral quadratic forms 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 and

Received by the editors September 23, 1992; revised Januay 5, 1994.
AMS subject classification: Primary: 11F06, 20H05; secondary: 11E08.
Key words and phrases: modular group, trace class, quadratic form.

https://doi.org/10.4153/CMB-1994-030-1 Published online by Cambridge University Press

some integers a, b with $(a, b) = 1$. Further the set $\{f_{i,d}\}$ are unique up to an equivalence relation on quadratic forms. The number $h(d)$ above is the ideal class number of the field $\mathbb{Q}(\sqrt{d^2 - 4})$ and we give an effective procedure given d to determine the $\{f_{i,d}(x, y)\}$. Note that Fermat's two-square theorem is precisely the above with $d = 0$ and thus the equation $x^2 + 1 = 0$. In this case $h(0) = 1$ and the quadratic form is $f(x, y) = x^2 + y^2$.

2. **Trace classes in the modular group.** Recall that the classical Modular Group M is $\mathrm{PSL}_2(\mathbb{Z})$ the group of 2×2 projective matrices with integral entries and determinant one. The elements of M can be considered as projective matrices $\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with a, b, c, d rational integers and $ad - bc = 1$. Equivalently the elements can be considered as linear fractional transformations $z' = \frac{az+b}{cz+d}$ again with $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$.

Multiplication of such transformations is done via matrix multiplication. We will use both interpretations as necessary.

We identify the following transformations:

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

Important also for our further work are the transformations

$$xy : z' = z + 1 \quad \text{and} \quad xy^2 : z' = z/z + 1.$$

Group theoretically M is generated by x and y and can be presented as (see [3], [12])

$$M = \langle x, y : x^2 = y^3 = 1 \rangle.$$

This has the structure of a free product of the cyclic group of order 2 generated by x and the cyclic group of order 3 generated by y. From this we obtain that any element $g \in M$ has a unique representation as a word $W(x, y)$ in x and y. That is $g = x^{t_1} y^{u_1} \cdots x^{t_n} y^{u_n}$ where $t_1 = 0$ or 1, $t_i = 1, i = 2, \ldots, n$ and $u_i = 0, 1$ or 2 if $i = 1, \ldots, n$. When we refer to an element of M as a word we mean the element the word represents.

Since conjugate matrices have the same trace the conjugacy classes in M break down by trace. A *trace class* in M is a conjugacy class all of the same trace. For a given positive integer d the number of trace classes in trace d is given from the Lattimer-MacDuffee Theorem by the ideal class number of the field $\mathbb{Q}(\sqrt{d^2 - 4})$ [12]. We denote by $h(d)$ the number of trace classes in trace d.

Our proofs depend on the determination of specific representatives for each trace class. Our technique then gives another procedure to count $h(d)$.

A word $W(x, y)$ in M is *cyclically reduced* if $W \neq W_1^{-1} W_2 W_1$ for other non-trivial words W_1, W_2. In 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. Clearly 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[9].

https://doi.org/10.4153/CMB-1994-030-1 Published online by Cambridge University Press

We say that a word $W(x,y)$ in M is in *block reduced form* abbreviated BRF 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*. If W is in BRF then its *block length* denoted $\mathrm{BL}(W)$ is the number of blocks in W.

An element T in M has order 2 if and only if T is conjugate to x. Further T has order 2 if and only if trace $T = \mathrm{tr}(T) = 0$ so $\{x\}$ represents the trace class of trace 0. Similarly if T has order 3 then $\mathrm{tr}\, T = \pm 1$ and T must be conjugate to y or y^2. We then have:

LEMMA 1. *Every element of M is conjugate to either x or y or y^2 or a word in* BRF.

PROOF. Since every element of M is conjugate to a cyclically reduced word we concentrate on cyclically reduced words. Let $g = W(x,y)$ be cyclically reduced and not equal to x or y or y^2. If g begins with x it must end with y or y^2 since it is cyclically reduced and therefore g is in block reduced form. If g begins with y or y^2 is must be followed by x. The word W_1 which is the cyclic permutation of W beginning with this x is conjugate to g. This must also be cyclically reduced and therefore as above must end with y or y^2 and therefore be in block reduced form.

Notice that a block reduced word is of the form

$$(xy)^{a_1}(xy^2)^{b_1}\cdots(xy^2)^{b_k}.$$

We impose an ordering on words in block reduced form. We say that a word $W(x,y)$ is in *standard block reduced form* abbreviated SBRF if it has one of the following forms.

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

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

(iii) $W = \big((xy)^n(xy^2)^k\big)^t$ for integers n,k,t

(iv) $W = (xy)^{a_1}(xy^2)^{b_1}\cdots(xy)^{a_k}(xy^2)^{b_k}$ where $a_1 = \max\{a_i\}$. If $a_1 = a_i$ for some i then $b_1 \geq b_i$. If $b_1 = b_i$ then $b_2 \geq b_{i+1}$ and so on. (The largest occurrence of (xy) is in the front and if the largest occurrence occurs more than once then the ordering goes to the occurrences of (xy^2).)

This definition imposes an ordering on words in SBRF. Notice that no two different words in SBRF are cyclic permutations of each other while any word in BRF is a cyclic permutation of some word in SBRF. Therefore:

THEOREM 1. *The trace classes in M are in one to one correspondence with words in* SBRF *together with $\{x\}, \{y\}, \{y^2\}$. The matrices corresponding to* SBRF *words together with the matrices for $\{x\}, \{y\}, \{y^2\}$ give representatives for each trace class.*

PROOF. As seen in the proof of Lemma 1, $\{x\}, \{y\}, \{y^2\}$ give representatives for the elements of finite order. If g is of infinite order it is represented by a word $W(x,y)$ not conjugate to any of the above three. Therefore from Lemma 1 and the remarks preceding the theorem it is conjugate to exactly one word in SBRF.

In enumerating the conjugacy classes it is somewhat easier to deal not with the SBRF words but rather with the sequence of exponents. With this in mind we call a finite sequence of integers a *standard block reduced sequence* or SBRS if it is one of the following forms making it the sequence of exponents for a SBRF word

https://doi.org/10.4153/CMB-1994-030-1 Published online by Cambridge University Press

(i) $(a,0)$

(ii) $(0,b)$

(iii) $(a,b,a,b,\ldots,a,b)$

(iv) $(a_1,b_1,\ldots,a_k,b_k)$ with a_i,b_i as in the definition of SBRF words.

We then have:

THEOREM 1′. *The trace classes in M for trace $d \geq 2$ are in one to one correspondence with standard block reduced sequences. The traces are uniquely defined functions of the sequences.*

PROOF. If the trace is 0 or 1 the element has finite order and is conjugate to x, y, or y^2. Otherwise it is conjugate to a SBRF word and thus related to the corresponding SBRS.

Now we separate the conjugacy classes by trace.

LEMMA 2. *If $W(x,y)$ is a word in M in* BRF *with* $\mathrm{BL}(W) \geq 1$ *then the transformation for W has only positive entries.*

PROOF. If $\mathrm{BL}(W) = 1$ then $W = xy$ represented by $\pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $W = xy^2$ represented by $\pm\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. The lemma is finished by induction. If $W = W_1xy$ with W_1 having only positive entries then multiplying by (xy) will again give only positive entries. Similarly multiplying by xy^2 will give only positive entries.

The next lemma is our key lemma.

LEMMA 3. *If $W \neq (xy)^n$ or $(xy^2)^k$ is a word in M in* BRF *and* $\mathrm{BL}(W) = n$ *then* $\mathrm{tr}(W) \geq n+1$.

PROOF. The proof is again by induction on the block length. If $\mathrm{BL}(W) = 1$ then $W = xy$ or $W = xy^2$. From above then we see that $\mathrm{tr}(W) = 2$ in both cases. Suppose that W has block length $n+1$. Then $W = W_1xy$ or $W = W_1xy^2$ with $\mathrm{BL}(W_1) = n$. Suppose first that $W_1 = (xy)^n$. Then since $W \neq (xy)^{n+1}$ it follows that $W = (xy)^n(xy^2)$. $(xy)^n$ is represented by the matrix $\pm\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ so W is represented by $\pm\begin{pmatrix} n+1 & n \\ 1 & 1 \end{pmatrix}$. This has trace $n+2$. An identical argument works if $W_1 = (xy^2)^n$. Suppose now that W_1 does not have one of those two forms. Then from the inductive hypothesis $\mathrm{tr}(W_1) \geq n+1$.

Let $W_1 = \pm\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a+d \geq n+1$. Further $c > 0$ since from Lemma 2 there are only positive entries. If $W = W_1xy$ then $W = \pm\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$. Then $\mathrm{tr}(W) = a+d+c \geq n+1+c$. Thus $\mathrm{tr}(W) \geq n+2$ since $c \geq 1$.

The identical argument works if $W = W_1xy^2$ proving the lemma.

From these two lemmas we obtain our procedure for effectively determining a representative for each trace class.

https://doi.org/10.4153/CMB-1994-030-1 Published online by Cambridge University Press

THEOREM 2. *Given a positive integer d there exists an effective procedure to determine a representative for each trace class in trace d. The procedure is as follows;*

(1) If $d = 0$ the representative is x

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

(3) If $d = 2$ there are infinitely many trace classes. The distinct words $(xy)^n$ and $(xy^2)^n$ as n runs over the positive integers give the representatives

(4) If $d > 2$ then:

(i) List all words in SBRF *of block length $(d-1)$ or less. (Equivalently list all standard block reduced sequences whose sum is $(d-1)$ or less.)*

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

Before we indicate the proof, notice that finding the representatives for trace d also determines the representatives for all traces less than d.

PROOF. The proof follows directly from the previous lemmas. If $d = 0$ or $d = 1$ the element has finite order and thus x, y, y^2 are representatives as in the proof of Theorem 1. All other elements are conjugate to elements in standard block reduced form. If the $\mathrm{tr}(W) = 2$ and $\mathrm{BL}(W) = n$ then W must be conjugate to either $(xy)^n$ or $(xy^2)^n$ or else by Lemma 2, $\mathrm{tr}(W) \geq n + 1$. Suppose then that $\mathrm{tr}(W) = d$. From Lemma 1, W is conjugate to a word in SBRF. From Lemma 2 this then must have block length $(d-1)$ or less. The procedure then follows easily.

To clarify Theorem 2 we present an example.

EXAMPLE. We find a complete set of representatives for the trace classes in trace 6. We first generate all SBRF of sum 5 or less. We then find the corresponding words (in SBRF) and their traces. This gives the following table.

Sequence	Word	Block Length	Trace
(1,1)	$xyxy^2$	2	3
(1,2)	$xy(xy^2)^2$	3	4
(2,1)	$(xy)^2xy^2$	3	4
(1,3)	$xy(xy^2)^3$	4	5
(1,1,1,1)	$xyxy^2xyxy^2$	4	7
(2,2)	$(xy)^2(xy^2)^2$	4	6
(3,1)	$(xy)^3xy^2$	4	5
(1,4)	$xy(xy^2)^4$	5	6
(1,2,1,1)	$xy(xy^2)^2xyxy^2$	5	10
(2,3)	$(xy)^2(xy^2)^3$	5	8
(2,1,1,1)	$(xy)^2xy^2xyxy^2$	5	10
(3,2)	$(xy)^3(xy^2)^2$	5	8
(4,1)	$(xy)^4xy^2$	5	6

https://doi.org/10.4153/CMB-1994-030-1 Published online by Cambridge University Press

Therefore we have found the following:

Trace	Number of Classes	Representatives
3	1	$xyxy^2 = \pm\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$
4	2	$(xy)(xy^2)^2 = \pm\begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$
		$(xy)^2(xy^2) = \pm\begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$
5	2	$(xy)(xy^2)^3 = \pm\begin{pmatrix} 4 & 1 \\ 3 & 1 \end{pmatrix}$
		$(xy)^3(xy^2) = \pm\begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix}$
6	3	$(xy)^2(xy^2)^2 = \pm\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$
		$(xy)^4(xy^2) = \pm\begin{pmatrix} 5 & 4 \\ 1 & 1 \end{pmatrix}$
		$(xy)(xy^2)^4 = \pm\begin{pmatrix} 5 & 1 \\ 4 & 1 \end{pmatrix}$

Before we move on we describe a separate related algorithm suggested by R. Kulkarni [10]. Notice from Lemma 2 that there exists a complete set of trace class representatives whose matrices have only positive entires. The alternative algorithm to that given in Theorem 2 is then the following.

ALTERNATIVE ALGORITHM FOR FINDING TRACE CLASSES. Given a trace d

(1) Determine all projective unimodular matrices with trace d and only positive entries. This can be done since there are only finitely many positive solutions to the equations $u + v = d$, $zw = 1 - uv$.

(2) Using the standard algorithm (see [7] or [12]) express each of these matrices in terms of the standard generators x, y.

(3) Among the words found in step (2) choose the ones in SBRF. These will give a complete set of representatives.

EXAMPLE. We again find the representatives for trace 6. From step (1) we obtain the following matrices.

$$\pm\begin{pmatrix} 5 & 4 \\ 1 & 1 \end{pmatrix}, \pm\begin{pmatrix} 5 & 1 \\ 4 & 1 \end{pmatrix}, \pm\begin{pmatrix} 1 & 4 \\ 1 & 5 \end{pmatrix}, \pm\begin{pmatrix} 1 & 1 \\ 4 & 5 \end{pmatrix}$$
$$\pm\begin{pmatrix} 4 & 1 \\ 7 & 2 \end{pmatrix}, \pm\begin{pmatrix} 4 & 7 \\ 1 & 2 \end{pmatrix}, \pm\begin{pmatrix} 2 & 1 \\ 7 & 4 \end{pmatrix}, \pm\begin{pmatrix} 2 & 7 \\ 1 & 4 \end{pmatrix}$$
$$\pm\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}, \pm\begin{pmatrix} 3 & 1 \\ 8 & 3 \end{pmatrix}, \pm\begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix}$$

Expressed in terms of the standard generators with the respective SBRF's indicated these are:

$$\pm\begin{pmatrix} 5 & 4 \\ 1 & 1 \end{pmatrix} = (xy)^4(xy^2), \quad \pm\begin{pmatrix} 5 & 1 \\ 4 & 1 \end{pmatrix} = (xy)(xy^2)^4$$

https://doi.org/10.4153/CMB-1994-030-1 Published online by Cambridge University Press

$$\pm\begin{pmatrix} 1 & 4 \\ 1 & 5 \end{pmatrix} = (xy^2)(xy)^4 \sim (xy)^4(xy^2)$$

$$\pm\begin{pmatrix} 1 & 1 \\ 4 & 5 \end{pmatrix} = (xy^2)^4(xy) \sim (xy)(xy^2)^4$$

$$\pm\begin{pmatrix} 4 & 1 \\ 7 & 2 \end{pmatrix} = (xy^2)(xy)(xy^2)^3 \sim (xy)(xy^2)^4$$

$$\pm\begin{pmatrix} 4 & 7 \\ 1 & 2 \end{pmatrix} = (xy)^3(xy^2)(xy) \sim (xy)^4(xy^2)$$

$$\pm\begin{pmatrix} 2 & 1 \\ 7 & 4 \end{pmatrix} = (xy^2)^3(xy)(xy^2) \sim (xy)(xy^2)^4$$

$$\pm\begin{pmatrix} 2 & 7 \\ 1 & 4 \end{pmatrix} = (xy)(xy^2)(xy)^3 \sim (xy)^4(xy^2)$$

$$\pm\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} = (xy)^2(xy^2)^2$$

$$\pm\begin{pmatrix} 3 & 1 \\ 8 & 3 \end{pmatrix} = (xy^2)^2(xy)(xy^2)^2 \sim (xy)(xy^2)^4$$

$$\pm\begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix} = (xy)^2(xy^2)(xy)^2 \sim (xy)^4(xy^2)$$

By choosing the SBRF's we see that as in the previous table there are three trace classes with representatives given by $(xy)(xy^2)^4$, $(xy)^4(xy^2)$, $(xy)^2(xy^2)^2$.

Although this sceond algorithm has the advantage of only finding the trace classes for a single trace the difficulty in expressing a matrix in terms of the standard generators (especially for larger entries) makes the first algorithm somewhat easier to work with.

3. **The generalized Fermat's theorem.** We now obtain our result on quadratic forms. We note that this can also be derived from work in Gauss [8].

THEOREM 3. *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 $f'_{i,d}$s.*

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

(c) *The $f'_{i,d}$s are unique in the following sense: If $n = (a,b)$ 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 is equivalent to some $f_{i,d}(x,y)$.*

As an immediate corollary:

COROLLARY 1. *The equation $x^2+dx+1=0$ is solvable modulo n if and only if $n=f(a,b)$ for some quadratic form of discriminant d^2-4 and integers a,b with $(a,b)=1$.*

https://doi.org/10.4153/CMB-1994-030-1 Published online by Cambridge University Press

PROOF OF THEOREM 3. Given $d \neq 2$ let $T_{i,d}$, $i = 1, \ldots, h(d)$ be a complete set of trace class representatives in trace d. Suppose

$$T_{i,d} = \pm \begin{pmatrix} u_{i,d} & v_{i,d} \\ w_{i,d} & t_{i,d} \end{pmatrix} \text{ with } u_{i,d} + t_{i,d} = d \text{ and determinant one.}$$

Now consider a conjugate of $T_{i,d}$.

$$\begin{aligned} &\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u_{i,d} & v_{i,d} \\ w_{i,d} & t_{i,d} \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ (1) \qquad &= \pm \begin{pmatrix} \star & v_{i,d}a^2 + (t_{i,d} - u_{i,d})ab - w_{i,d}b^2 \\ \star & \star \end{pmatrix} \end{aligned}$$

The upper right hand corner of a general conjugate of $T_{i,d}$ then defines a quadratic form in two variables. For each $i = 1, 2, \ldots, h(d)$ let

$$f_{i,d}(x, y) = v_{i,d}x^2 + (t_{i,d} - u_{i,d})xy - w_{i,d}y^2.$$

A computation shows that the discriminant of each $f_{i,d}(x, y)$ as defined above is $d^2 - 4$. (The middle term $t_{i,d} - u_{i,d} = d - 2u_{i,d}$.)

Now suppose that the equation $x^2 + dx + 1 = 0$ is solvable modulo n so that $x^2 + dx + 1 = -nm$ or equivalently $-x(d + x) - nm = 1$. Therefore there exists a projective matrix

$$\pm \begin{pmatrix} -x & n \\ m & d + x \end{pmatrix} \in M \text{ which has trace } d.$$

This matrix must then be a conjugate of one of the standard representatives $T_{i,d}$. Therefore the upper right hand corner, n, of this matrix must have the form of a conjugate of $T_{i,d}$ and thus $n = f_{i,d}(a, b)$. Further $(a, b) = 1$ since $ad - bc = 1$ in (1).

Conversely suppose that $n = f_{i,d}(a, b)$ for some $f_{i,d}(x, y)$ with $(a, b) = 1$. Then there exists integers c, d such that $ad - bc =$ and thus there is a projective matrix

$$\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M.$$

Conjugating $T_{i,d}$ by this matrix gives

$$\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} T_{i,d} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \pm \begin{pmatrix} \star & n \\ \star & \star \end{pmatrix}$$

which has trace d. Therefore it must have the form

$$\pm \begin{pmatrix} -x & n \\ m & x + d \end{pmatrix}.$$

Further it has determinant one and so $-x(x + d) - nm = 1$ or $x^2 + dx + 1 = -nm$ and therefore $x^2 + dx + 1 = 0$ is solvable modulo n. This proves the main part of the theorem.

The constructive procedure for finding the $\{f_{i,d}(x, y)\}$ is as follows. Use the method of Theorem 2 to find a complete set $\{T_{i,d}\}$, $i = 1, \ldots, h(d)$ of representatives for trace

https://doi.org/10.4153/CMB-1994-030-1 Published online by Cambridge University Press

classes in trace d. Formally conjugate each of them as in (1) to get the corresponding $f_{i,d}(x,y)$.

Since $h(d)$ = number of trace classes in trace d this equals the class number of the field $\mathbb{Q}(\sqrt{d^2-4})$ by the Lattimer-MacDuffee Theorem [12].

To show the uniqueness part suppose $n = f(a,b)$ with $(a,b) = 1$ and the discriminant of $f(x,y)$ being d^2-4. Suppose $f(x,y) = vx^2 + txy + wy^2$. Let $w_1 = -w$ and $t = d - 2u$ so that $u = (d-t)/2$. Then since the discriminant is d^2-4 we have $u(d-u) - vw = 1$ so that the projective matrix

$$(2) \qquad V_f = \pm \begin{pmatrix} u & v \\ w_1 & d-u \end{pmatrix} \text{ is in } M.$$

Proceeding as in the proof of the first part this matrix has trace d and determinant one. Since (a,b) =1 there exists integers c,d such that $ad - bc = 1$ and so the projective matrix

$$T = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is also in } M.$$

Then conjugating V_f by T gives us

$$\pm \begin{pmatrix} x & n \\ \star & -x+d \end{pmatrix}.$$

Since this has determinant one, $x^2 + dx + 1 = 0$ modulo n and therefore $n = f_{i,d}(u,v)$ for some $(u,v) = 1$ from the first part. Associate to each quadratic form $f(x,y)$ of discriminant d^2-4 the matrix V_f as given in (2). Define f_1 to be equivalent to f_2 if V_{f_1} is conjugate to V_{f_2}. This is the mentioned equivalence relation.

We now give an example of the procedure. Using the table of representatives for traces up to 6 we determine a set of $\{f_{i,d}\}$.

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

https://doi.org/10.4153/CMB-1994-030-1 Published online by Cambridge University Press

The theorem then says for example that $x^2 + 5x + 1 = 0$ is solvable modulo n if and only if $n = a^2 - 3ab - 3b^2$ or $n = 3a^2 - 3ab - b^2$ for some integers a, b with $(a, b) = 1$. For p a prime this says that 21 is a square modulo p if and only if p is represented by one of those two forms.

4. **On the determination of $h(d)$.** The determination of $h(d)$ is known from the class number formulas [2], however the procedure outlined in Theorems 2 and 3 actually provides another recursive technique for finding this number. In this final section we present some facts about this technique.

Let $h(k, d)$ = number of super block reduced form words of block length k and trace d. Then from Lemma 3.

LEMMA 4. $h(d) = \sum_{k=2}^{d-1} h(k, d)$.

Therefore the recursive counting procedure lies in the determination of $h(k, d)$. Consider the function f: (super block reduced sequences) $\longrightarrow \mathbb{N}$ the natural numbers, given by

$$f(a_1, b_1, \ldots, a_k, b_k) = \text{trace}(xy)^{a_1}(xy^2)^{b_1} \cdots (xy)^{a_k}(xy^2)^{b_k}.$$

The function f is what is used to evaluate the trace of a super block reduced form word. We obtain a few straightforward facts about this function.

LEMMA 5. *Let f be the function defined above. Then:*

(1) $f(a, b) = ab + 2$

(2) $f(a_1, b_1, a_2, b_2) = 2 + a_1b_1 + a_1b_2 + b_2a_1 + b_2a_2 + a_1b_1a_2b_2$

(3) In general $f(a_1, b_1, \ldots, a_k, b_k) = 2 +$ *(collection of even products in* a_ib_i*)*

(4) $f(a_1, b_1, \ldots, a_k, b_k) = f(b_i, a_{i+1}, \ldots)$ *for any cyclic permutation of* $a_1, b_1, \ldots, a_k, b_k$

The proofs are computations on traces. As corollaries we obtain the following.

COROLLARY 2. $h(d - 1, d) = 2$.

PROOF. Again by computation the only super block reduced form words of block length $d - 1$ and trace d are $(xy)^{d-2}xy^2$ or $(xy)(xy^2)^{d-2}$. All others give traces greater than d.

Then from Lemma 5 part (1) we obtain.

COROLLARY 3. *The class number $h(d) \geq$ the number of divisors of $d - 2$. In particular $h(d)$ grows with d.*

Ken Williams in a private correspondence [14] has given the following alternative (more traditional) proof of Corollary 3. Let $\mu(n - 2)$ = number of positive divisors of $n - 2$. Let a be an arbitrary divisor of $n - 2$. Since a can be positive or negative there are $2\mu(n - 2)$ possibilities for a. Consider the $2\mu(n - 2)$ integral binary quadratic forms

$$f_a(x, y) = ax^2 + (n - 2)xy - \big((n - 2)/a\big)y^2.$$

https://doi.org/10.4153/CMB-1994-030-1 Published online by Cambridge University Press

Each $f_a(x,y)$ has discriminant d^2-4. Further it can be shown that each $f_a(x,y)$ is primitive and reduced. Further each $f_a(x,y)$ is ambiguous as a divides $n-2$. From Proposition 3.8 of [1] the $2\mu(n-2)$ ambiguous reduced forms f_a fall into at least $\mu(n-2)$ different cycles of reduced forms. Hence $h(d)$ = number of cycles of reduced forms of discriminant $d^2-4 \geq \mu(n-2)$.

Finally using Nielsen reduction [7], [11] on the super block reduced form words we get an easy proof of the following interesting result.

LEMMA 6. *Given positive integers $m,n \geq 2$ we can find A,B in M with* $\mathrm{tr}(A) = m$ *and* $\mathrm{tr}(B) = n$ *such that* $\langle A,B\rangle$ *is free of rank* 2.

PROOF. Let $A = (xy)^{m-2}(xy^2)$ and $B = (xy)(xy^2)^{n-2}$. Then $\mathrm{tr}(A) = m$, $\mathrm{tr}(B) = n$ and using Nielsen reduction A,B generate a free group of rank 2.

We close with a question. Consider the ideal classes in $\mathbb{Q}(\sqrt{d^2-4})$. We have seen that these are in one to one correspondence with the super block reduced sequences of integers of sum $d-1$ or less. What if anything do these sequences tell us about the structure of the ideal classes?

REFERENCES

1. D. A. Buell, *Binary Quadratic Forms*, Springer-Verlag, 1989.

2. H. Cohn, *A Second Course in Number Theory*, John Wiley, New York, 1962.

3. B. Fine, *The Algebraic Theory of the Bianchi Groups*, Marcel Dekker, 1990.

4. ———, *A Note on the Fermat Two-Square Theorem*, Canad. Math. Bull. (1) **20**(1977), 93–95.

5. ———, *Sum of Squares Rings*, Canad. J. Math. **XXIX**(1977), 155-161.

6. ———, *Cyclotomic Equations and Square Properties in Rings*, Internat. J. Math. (1) **9**(1986), 89–95.

7. ———, *Subgroup Presentations without Coset Representatives*. In: Combinatorial Group Theory, Proceedings of the Fall Foliage Conference, Springer-Verlag, 1990, 59–74.

8. C. F. Gauss, *Disquitiones Arithmeticae*.

9. G. Kern-Isbrenner and G. Rosenberger, *A note on Numbers of the Form* $n = x2 + Ny2$, Arch. Math.

10. R. Kulkarni, *private communication*.

11. W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory*, Wiley Interscience, New York, 1966.

12. M. Newman, *Integral Matrices*, Academic Press, New York, 1972.

13. M. Sheingorn, *private communication*.

14. K. Williams, *private communication*.

15. W. Magnus, *Non-Euclidean Tesselations and Their Groups*, Academic Press, 1974.

16. J. L. Brenner and R. Lyndon, *Non-parabolic Subgroups of the Modular Group*, J. Algebra (2) **77**(1982), 311–322.

Department of Mathematics
Fairfield University
Fairfield, Connecticut 06430
U.S.A

https://doi.org/10.4153/CMB-1994-030-1 Published online by Cambridge University Press