JOURNAL OF NUMBER THEORY 45, 61–67 (1993)

# Representation of Primes in Arithmetic Progression by Binary Quadratic Forms

PIERRE KAPLAN

*Département de Mathématiques, Université de Nancy 1, B.P. 239, 54506 Vandoeuvre Cedex, France*

AND

KENNETH S. WILLIAMS*

*Centre for Research in Algebra and Number Theory, Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario K1S 5B6, Canada*

*Communicated by A. C. Woods*

Received October 11, 1991

## 1. INTRODUCTION

We denote the strict class group of primitive integral binary quadratic forms of fixed nonsquare discriminant $D$ under composition by $H(D)$. A genus $G$ of $H(D)$ is a subset which consists of all the classes giving the same values to the generic characters of $H(D)$. Composition induces a group structure on the set of genera of $H(D)$. The reader will find the basic properties of the genera of binary quadratic forms in [1, Chap. 4].

Let $A$ and $B$ be coprime integers. We are interested in the representability of the odd primes of an arithmetic progression $\{An + B : n \in Z\}$ by the genera and classes of $H(D)$. We prove

THEOREM 1. *Let $A$ and $B$ be coprime integers. Suppose that $G$ is a genus of classes in $H(D)$ having the property*

$$\text{Each prime } p \equiv B \pmod{A} \text{ with } p \nmid 2D \text{ is represented by a class from the genus } G. \tag{1.1}$$

* Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.



0022-314X/93 $5.00

*Let $k$ be an integer coprime with $2D$ which is represented by a class from the genus $G'$ of $H(D)$. Then each prime $q \equiv kB \pmod{A}$ is represented by a class from the genus $GG'$.*

THEOREM 2. *Let $A$ and $B$ be coprime integers. Suppose that $C$ is a class of $H(D)$ having the property*

$$\text{Each prime } p \equiv B \pmod{A} \text{ with } p \nmid 2D \text{ is represented by the class } C. \tag{1.2}$$

*Then each genus of $H(D)$ contains exactly one class if $C = C^{-1}$ and exactly two classes if $C \neq C^{-1}$. Moreover*

$$H(D) \approx \begin{cases} Z_2 \times Z_2 \times \cdots \times Z_2, & \text{if } C = C^{-1}, \\ Z_4 \times Z_2 \times \cdots \times Z_2, & \text{if } C \neq C^{-1}. \end{cases} \tag{1.3}$$

*Further, if $k$ is an integer coprime with $2D$ which is represented by the class $K$ of $H(D)$, then each prime $q \equiv kB \pmod{A}$ is represented by*

| | |
|---|---|
| *the class $CK$,* | *if $C = C^{-1}$,* |
| *both the classes $CK$ and $C^{-1}K$,* | *if $C \neq C^{-1}$, $K = K^{-1}$,* |
| *exactly one of the classes $CK$ and $C^{-1}K$,* | *if $C \neq C^{-1}$, $K \neq K^{-1}$.* |

The theorem of Kusaba [3, Théorème], proved using class field theory, is essentially the first part of Theorem 2 when $D$ is a fundamental discriminant.

An immediate corollary of Theorem 2 is the following generalization of the theorem of Ramanujan first proved by Williams in [5], and its generalization proved by Halter-Koch in [2] using class field theory.

COROLLARY. *Let $C$ be a class of $H(D)$ having the property* (1.2). *Let $k$ be an integer coprime with $2D$ which is represented by an ambiguous ($\equiv$ self-inverse) class of $H(D)$. Then each prime $q \equiv kB \pmod{A}$ is represented by the class $CK$.*

In the proofs of Theorem 1 and Theorem 2, we suppose that $A$ is even and $B$ is odd. There is no loss of generality in doing this as, for odd primes $p$, we have

$$p \equiv B \pmod{A} \Leftrightarrow \begin{cases} p \equiv B \pmod{2A}, & \text{if } A \text{ odd, } B \text{ odd,} \\ p \equiv A + B \pmod{2A}, & \text{if } A \text{ odd, } B \text{ even.} \end{cases}$$

We conclude this introduction with a simple example.

EXAMPLE. The form class group $H(-768)$ comprises 8 classes

$$I,\ A,\ A^2,\ A^3,\ B,\ AB,\ A^2B,\ A^3B,$$

TABLE I

| Genera | Generic characters | | |
|---|---|---|---|
| | $\left(\frac{k}{3}\right)$ | $\left(\frac{-1}{k}\right)$ | $\left(\frac{2}{k}\right)$ |
| $I$, $A^2$ | + | + | + |
| $A$, $A^3$ | + | + | − |
| $B$, $A^2B$ | + | − | − |
| $AB$, $A^3B$ | + | − | + |

which are the classes of the forms

$$X^2+192Y^2,\ 13X^2+8XY+16Y^2,\ 4X^2+4XY+49Y^2,\ 13X^2-8XY+16Y^2,$$
$$12X^2+12XY+19Y^2,\ 7X^2-4XY+28Y^2,\ 3X^2+64Y^2,\ 7X^2+4XY+28Y^2,$$

respectively. These classes fall into 4 genera as shown in Table I.

Each prime $p\equiv 13 \pmod{24}$ satisfies $(p/3)=(-1/p)=1$, $(2/p)=-1$ so that $p$ is represented by the class $A$. The integer 31 is represented by the class $AB$, so that by Theorem 2 each prime $p\equiv(13)(31)\equiv 19 \pmod{24}$ is represented by exactly one of the classes $A(AB)=A^2B$ and $A^{-1}(AB)=B$. Table II indicates which of $A^2B$ and $B$ represents $p$ for $p$ (prime) $\equiv 19 \pmod{24}$, $p<1000$.

Numerical data suggest that for primes $p\equiv 19 \pmod{24}$ we have

$$p=3x^2+64y^2, \qquad \text{if} \quad V_{(p+1)/4}\equiv 2 \pmod{p},$$
$$p=12x^2+12xy+19y^2, \qquad \text{if} \quad V_{(p+1)/4}\equiv -2 \pmod{p},$$

TABLE II

| | $A^2B$ | | $B$ |
|---|---|---|---|
| $p\equiv 19 \pmod{24}$ | $p=3x^2+64y^2$ | $p\equiv 19 \pmod{24}$ | $p=12x^2+12xy+19y^2$ |
| 67 | 1,1 | 19 | 0,1 |
| 139 | 5,1 | 43 | 1,1 |
| 211 | 7,1 | 163 | 3,1 |
| 283 | 3,2 | 379 | 5,1 |
| 307 | 9,1 | 523 | 6,1 |
| 331 | 5,2 | 547 | 1,5 |
| 499 | 9,2 | 643 | 2,5 |
| 571 | 13,1 | 691 | 7,1 |
| 619 | 11,2 | 787 | −3,7 |
| 739 | 15,1 | 811 | −2,7 |
| | | 859 | −1,7 |
| | | 883 | 8,1 |
| | | 907 | 4,5 |

where

$$V_{n+2} = -4V_{n+1} - V_n \qquad (n = 0, 1, 2, \ldots)$$
$$V_0 = 2, \qquad V_1 = -4.$$

In addition to the basic theory of binary quadratic forms, our proof of Theorem 1 uses Dirichlet's theorem on primes in an arithmetic progression, and our proof of Theorem 2 uses Meyer's theorem [4] which asserts that a primitive integral binary quadratic form represents infinitely many primes in any arithmetic progression consistent with the generic characters of the form.

## 2. A Property of Legendre Symbols

The following lemma is a consequence of Dirichlet's theorem on primes in an arithmetic progression and will be used in the proof of Theorem 1.

LEMMA. *Let $\varepsilon = \pm 1$ and let $A$ and $B$ be coprime integers. Let $S$ be a given finite set of primes.*

(i) *Let $r$ be an odd prime. If the Legendre symbol $((An+B)/r)$ has the value $\varepsilon$ for all $n \in Z$ for which $An+B$ is a prime $\neq r$ and not belonging to $S$ then $r \mid A$.*

(ii) *Suppose $A$ is even and $B$ is odd. If $(-1/(An+B)) = \varepsilon$ (resp. $(2/(An+B)) = \varepsilon$, $(-2/(An+B)) = \varepsilon$) for all $n \in Z$ for which $An+B$ is an odd prime not belonging to $S$ then $4 \mid A$ (resp. $8 \mid A$, $8 \mid A$).*

*Proof.* (i) Suppose $r \nmid A$. Let $k$ be an integer such that $(k/r) = -\varepsilon$. Then by Dirichlet's theorem there is a prime $q \notin S$ such that

$$q \equiv B \pmod{A},$$
$$q \equiv k \pmod{r}.$$

Then we have

$$\varepsilon = \left(\frac{q}{r}\right) \qquad (\text{as } q \equiv B \pmod{A})$$
$$= \left(\frac{k}{r}\right) \qquad (\text{as } q \equiv k \pmod{r})$$
$$= -\varepsilon \qquad (\text{choice of } k),$$

which is a contradiction, and so $r$ divides $A$.

(ii) We just treat the case $(2/(An+B))=\varepsilon$ as the other two cases are similar. Suppose $8 \nmid A$. As $A$ is even we have (a) $A \equiv 2 \pmod 4$ or (b) $A \equiv 4 \pmod 8$.

(a) By Dirichlet's theorem there is a prime $q \notin S$ such that

$$q \equiv B \pmod{A/2},$$

$$\left(\frac{2}{q}\right) = -\varepsilon.$$

As $q$, $A/2$, and $B$ are odd, we see that $q \equiv B \pmod A$ so that $(2/q)=\varepsilon$, which is a contradiction.

(b) By Dirichlet's theorem there is a prime $q \notin S$ such that

$$q \equiv B \pmod{A/4} \tag{2.1}$$

and

$$q \equiv \begin{cases} 1 \pmod 8, & \text{if } B \equiv 1 \pmod 4,\ \varepsilon = -1, \\ 3 \pmod 8, & \text{if } B \equiv 3 \pmod 4,\ \varepsilon = 1, \\ 5 \pmod 8, & \text{if } B \equiv 1 \pmod 4,\ \varepsilon = 1, \\ 7 \pmod 8, & \text{if } B \equiv 3 \pmod 4,\ \varepsilon = -1. \end{cases} \tag{2.2}$$

Then, by (2.1) and (2.2), we have $q \equiv B \pmod A$, so that $(2/q)=\varepsilon$. But from (2.2) we see that $(2/q)=-\varepsilon$, which is a contradiction. ∎

## 3. Proof of Theorem 1

Associated with the discriminant $D$ is the fundamental discriminant $D_0$ defined by $D = D_0 f^2$, where $f^2$ is the largest square dividing $D$ such that $D_0 \equiv 0$ or $1 \pmod 4$. We also let $D^*$ denote the product of the distinct odd primes dividing $D$, and we set

$$M = \begin{cases} 2D^*, & \text{if } D \equiv 1 \pmod 4 \text{ or } D \equiv 4 \pmod{16}, \\ 4D^*, & \text{if } D \equiv 12 \pmod{16} \text{ or } D \equiv 16 \pmod{32}, \\ 8D^*, & \text{if } D \equiv 0,\ 8, \text{ or } 24 \pmod{32}, \end{cases}$$

and observe that $D_0 \mid M$.

Now let $r$ be an odd prime divisor of $D$, so that the Legendre symbol $(\ /r)$ is a generic character for the discriminant $D$ [1, p. 52]. From (1.1) we see that $(p/r)$ has a fixed value for all primes $p \equiv B \pmod A$ with $p \nmid 2D$, so that, by Lemma 1(i), $r \mid A$. In addition each supplementary generic

character [1, p. 52] has a fixed value for all primes $p \equiv B \pmod{A}$ with $p \nmid 2D$ so, by Lemma 1(ii), as $A$ is assumed even and $B$ odd, we have

$$4 \mid A, \quad \text{if } D \equiv 12 \pmod{16} \text{ or } D \equiv 16 \pmod{32},$$

$$8 \mid A, \quad \text{if } D \equiv 0, 8, \text{ or } 24 \pmod{32}.$$

Hence $M \mid A$. As a consequence of this we see that any prime $p \equiv B \pmod{A}$ does not divide $2D$.

Let $p$ be a prime $\equiv B \pmod{A}$. Thus $p$ is represented by some class of the genus $G$ and so $(D/p) = 1$. Similarly we have $(D/k) = 1$. Now, as $D_0 \mid M \mid A$, we have for any prime $q \equiv kB \pmod{A}$

$$q \equiv kB \equiv kp \pmod{D_0},$$

so that as $D = D_0 f^2$ we have

$$\left(\frac{D}{q}\right) = \left(\frac{D_0}{q}\right) = \left(\frac{D_0}{kp}\right) = \left(\frac{D_0}{k}\right)\left(\frac{D_0}{p}\right) = \left(\frac{D}{k}\right)\left(\frac{D}{p}\right) = 1,$$

and thus $q$ is represented by some class $K$ of $H(D)$. We now determine the genus to which the class $K$ belongs.

Let $\chi$ denote any one of the generic characters for the discriminant $D$. Then, for any prime $p \equiv B \pmod{A}$ and any prime $q \equiv kB \pmod{A}$, we have

$$\begin{aligned} \chi(q) &= \chi(kB) \qquad (\text{as } q \equiv kB \pmod{M}) \\ &= \chi(k)\,\chi(B) \\ &= \chi(k)\,\chi(p) \qquad (\text{as } p \equiv B \pmod{M}) \end{aligned}$$

so that the genus of $K$ is $GG'$.

We observe that in the example in Section 1 we have

$$D = -768, \qquad D_0 = -3, \qquad f = 16, \qquad D^* = 3,$$
$$M = 24, \qquad A = 24, \qquad B = 13.$$

## 4. Proof of Theorem 2

Suppose the genus $G$ of the class $C$ contains a class $J \neq C, C^{-1}$. In view of the property (1.2) we have $M \mid A$, as in the proof of Theorem 1, and so the arithmetic progression $\{An + B : n \in Z\}$ is consistent with the generic characters of $K$. Hence, by Meyer's theorem [4], $J$ represents infinitely many primes $q \equiv B \pmod{A}$. But each such prime $q$ with $q \nmid 2D$ is represented by $C$, and thus only by $C$ and $C^{-1}$, which is a contradiction.

This proves that each genus contains exactly one class if $C = C^{-1}$ and exactly two classes if $C \neq C^{-1}$. In particular the subgroup $H(D)^2$ of $H(D)$ (which is the principal genus of $H(D)$) contains exactly one class if $C = C^{-1}$ and exactly two classes if $C \neq C^{-1}$. This proves (1.3).

Finally, if $k$ is an integer coprime with $2D$ which is represented by the class $K$, and $q$ is a prime $\equiv kB \pmod{A}$, then by Theorem 1, $q$ is represented by a class in the genus of $CK$. This genus contains the four classes $CK$, $C^{-1}K$, $CK^{-1}$, and $C^{-1}K^{-1}$. If $C = C^{-1}$ these four classes coincide and $q$ is represented by $CK$. If $C \neq C^{-1}$ and $K = K^{-1}$ the genus of $CK$ contains the two distinct inverse classes $CK(=CK^{-1})$ and $C^{-1}K\ (=C^{-1}K^{-1})$, and $q$ is represented by both classes. If $C \neq C^{-1}$ and $K \neq K^{-1}$ the genus of $CK$ contains the two distinct non-inverse classes $CK\ (=C^{-1}K^{-1})$ and $C^{-1}K$ $(=CK^{-1})$, and $q$ is represented by exactly one of these two classes.

## REFERENCES

1. D. A. BUELL, "Binary Quadratic Forms," Springer-Verlag, New York/Berlin/Heidelberg, (1989).
2. F. HALTER-KOCH, A theorem of Ramanujan concerning binary quadratic forms, preprint, 1991.
3. T. KUSABA, Remarque sur la distribution des nombres premiers, *C.R. Acad. Sci. Paris Sér. A* **265** (1967), 405–407.
4. A. MEYER, Über einen Satz von Dirichlet, *J. Reine Angew. Math.* **103** (1888), 98–117.
5. K. S. WILLIAMS, On an assertion of Ramanujan concerning binary quadratic forms, *J. Number Theory* **38** (1991), 118–133.