Proceedings of the Edinburgh Mathematical Society (1992) **36**, 145–150 ©

THE SQUAREROOT OF AN AMBIGUOUS FORM IN THE PRINCIPAL GENUS

by KENNETH HARDY* and KENNETH S. WILLIAMS†

(Received 8th May 1991)

A squareroot of an ambiguous form in the principal genus of primitive integral binary quadratic forms of fixed discriminant is given explicitly in terms of a solution of a certain Legendre equation.

1991 *Mathematics subject classification*: 11E16.

Let $D \equiv 0, 1 \pmod 4$ be a nonsquare integer. Let f be a primitive, integral binary quadratic form of discriminant D, which is positive-definite if $D<0$. If f belongs to the principal genus of classes of forms of discriminant D then Gauss' famous duplication theorem (see for example [**1**, Theorem 4.21]) asserts that there exists a primitive binary quadratic form g of discriminant D such that $f \sim g^2$. Moreover Gauss [**2**, §286] has given a method of computing g using the reduction of ternary quadratic forms. In [**3**] Shanks improves Gauss' method and provides an algorithm suitable for machine computation. In this note we show that when f is an *ambiguous* form in the principal genus, g can be described in a simple way in terms of the solution of a certain Legendre equation (eqn. (3) below).

Replacing f by an equivalent form we may suppose that f is of one of the following two types:

(I) $$f = Ax^2 + Cy^2 = (A, 0, C), \quad \mathrm{GCD}(A, C) = 1, \quad D = -4AC,$$

or

(II) $$f = Ax^2 + Axy + Cy^2 = (A, A, C), \quad \mathrm{GCD}(A, C) = 1, \quad D = A^2 - 4AC.$$

We set

$$\begin{cases} \alpha = 2, B = C \quad\quad\;\;, & \text{if } f \text{ is of type (I)}, \\ \alpha = 1, B = 4C - A, & \text{if } f \text{ is of type (II)}, \end{cases} \tag{1}$$

so that

$$D = -\alpha^2 AB, \tag{2}$$

*Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-8049.
†Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

and show that there exist integers X, Y, Z satisfying Legendre's equation

$$AX^2 + BY^2 = Z^2, \quad \mathrm{GCD}(X, Y) = 1, \tag{3}$$

with

$$\begin{cases} \mathrm{GCD}(Z, 2AB) = 1 & , \text{ if } f \text{ is of type (I)}, \\ \mathrm{GCD}(Z, 2AB) = 1 & \\ \qquad \text{or} & \\ X \equiv Y \equiv Z + 1 \equiv 1 \pmod 2, \mathrm{GCD}\left(\frac{Z}{2}, 2AB\right) = 1 & , \text{ if } f \text{ is of type (II)}. \end{cases} \tag{4}$$

To see this, recall that a form in the principal genus represents primitively a square coprime with any given integer. Thus, if f is of type (I), there exist integers X, Y, Z such that

$$AX^2 + CY^2 = Z^2, \quad \mathrm{GCD}(X, Y) = 1, \quad \mathrm{GCD}(Z, 2AC) = 1,$$

establishing (3) and (4) in this case. If f is of type (II) there exist integers R, S, T such that

$$AR^2 + ARS + CS^2 = T^2, \quad \mathrm{GCD}(R, S) = 1, \quad \mathrm{GCD}(T, 2A(4C - A)) = 1.$$

Set

$$X = R + \frac{S}{2}, \quad Y = \frac{S}{2}, \quad Z = T, \quad \text{if } S \text{ is even},$$

$$X = 2R + S, \quad Y = S, \quad Z = 2T, \quad \text{if } S \text{ is odd}.$$

The integers X and Y satisfy

$$AX^2 + (4C - A)Y^2 = Z^2, \quad \mathrm{GCD}(X, Y) = 1,$$

with

$$\mathrm{GCD}(Z, 2A(4C - A)) = 1, \quad \text{if } S \text{ is even},$$

or

$$X \equiv Y \equiv Z + 1 \equiv 1 \pmod 2, \ \mathrm{GCD}(Z/2, 2A(4C - A)) = 1, \quad \text{if } S \text{ is odd},$$

establishing (3) and (4) in this case. From (3) and (4) we easily deduce that

$$\mathrm{GCD}(A, Y) = \mathrm{GCD}(B, X) = \mathrm{GCD}(X, Z) = \mathrm{GCD}(Y, Z) = 1. \tag{5}$$

Let u, v be integers such that

$$Xv - Yu = 1. \tag{6}$$

When f is of type (II) and $Z \equiv 1 \pmod 2$, we can arrange that u and v are both odd by replacing (u, v) by $(u + X, v + Y)$, if necessary, as X and Y are of opposite parity.

We define a, b, c by

$$\left.\begin{array}{ll} a=Z,\ b=2(AXu+BYv),\ c=Au^2+Bv^2 & ,\ \text{if } f \text{ is of type (I)},\\ a=Z,\ b=AXu+BYv,\ c=(Au^2+Bv^2)/4 & ,\ \text{if } f \text{ is of type (II)},\\ & \text{and } Z\equiv 1 \pmod 2,\\ a=Z/2,\ b=AXu+BYv,\ c=Au^2+Bv^2 & ,\ \text{if } f \text{ is of type (II)},\\ & \text{and } Z\equiv 0 \pmod 2. \end{array}\right\} \quad (7)$$

Note that when f is of type (II) and $Z\equiv 1 \pmod 2$ we have

$$c=A\frac{(u^2-v^2)}{4}+Cv^2,$$

which is an integer as both u and v are odd in this case. Thus the quantities a, b, c in (7) are all integers.

We define the integral binary quadratic form g by

$$g=(a,b,ac), \quad (8)$$

and prove:

Theorem. $g^2 \sim f$.

Proof. We first show that $g=(a,b,ac)$ is a primitive form, that is

$$\mathrm{GCD}(a,b)=1. \quad (9)$$

We have

$$\begin{aligned} bY &= \alpha(AXu+BYv)Y && \text{(by (1), (7))}\\ &= \alpha(AXYu+(Z^2-AX^2)v) && \text{(by (3))}\\ &= \alpha(Z^2v-AX(Xv-Yu))\\ &= \alpha(Z^2v-AX) && \text{(by (6))} \end{aligned}$$

so that

$$\begin{aligned} \mathrm{GCD}(a,b) &= \mathrm{GCD}(a,bY) && \text{(by (5), (7))}\\ &= \mathrm{GCD}(a,\alpha(Z^2v-AX))\\ &= \mathrm{GCD}(a,Z^2v-AX) && \text{(by (1), (4), (7))}\\ &= \mathrm{GCD}(a,AX) && \text{(by (7))}\\ &= 1 && \text{(by (4), (5), (7))} \end{aligned}$$

as claimed.

Next we show that $g=(a,b,ac)$ has discriminant D. We have, appealing to (2), (3), (6) and (7),

$$\begin{aligned} b^2-4a^2c &= \alpha^2((AXu+BYv)^2-Z^2(Au^2+Bv^2)) \\ &= \alpha^2((AXu+BYv)^2-(AX^2+BY^2)(Au^2+Bv^2)) \\ &= -\alpha^2AB(Xv-Yu)^2 \\ &= -a^2AB \\ &= D. \end{aligned}$$

Finally we observe that the unimodular transformation with matrix

$$\begin{bmatrix} X & u \\ Y & v \end{bmatrix}, \quad \text{if } f \text{ is of type (I)}$$

$$\begin{bmatrix} X-Y & \frac{u-v}{2} \\ 2Y & v \end{bmatrix}, \quad \text{if } f \text{ is of type (II) and } Z\equiv 1 \pmod 2,$$

$$\begin{bmatrix} \frac{X-Y}{2} & u-v \\ Y & 2v \end{bmatrix}, \quad \text{if } f \text{ is of type (II) and } Z\equiv 0 \pmod 2,$$

transforms f into the form (a^2,b,c). Hence, in view of (9) (see [**1**, Corollary 4.13]), we have

$$f\sim(a^2,b,c)\sim(a,b,ac)^2=g^2$$

as asserted. □

Example 1. The ambiguous form $f=(401,0,419)$ has discriminant $D=-67276=-4\cdot 401\cdot 419\equiv 20 \pmod{32}$ so its generic characters are the Legendre symbols $(\frac{}{401})$ and $(\frac{}{419})$. The form f represents primitively the odd integer $401\cdot 2^2+419=2023$, which is coprime with D. As

$$\left(\frac{2023}{401}\right)=\left(\frac{18}{401}\right)=\left(\frac{2}{401}\right)=1$$

and

$$\left(\frac{2023}{419}\right)=\left(\frac{-72}{419}\right)=\left(\frac{-2}{419}\right)=1,$$

the form f lies in the principal genus of classes of primitive, positive-definite binary quadratic forms of discriminant D. The appropriate Legendre equation is

$$401X^2+419Y^2=Z^2,$$

which must have an integral solution $(X, Y, Z) \neq (0,0,0)$ satisfying (see [4])

$$0 \leqq X \leqq \sqrt{419} \doteq 20, \quad 0 \leqq Y \leqq \sqrt{401} \doteq 20.$$

A simple computer search quickly finds

$$X=11, \quad Y=4, \quad Z=235.$$

A solution of

$$11v-4u=1$$

is

$$u=-3, \quad v=-1,$$

so, by (7) and (8), a squareroot of $f=(401,0,419)$ is given by

$$g=(235,-29818,946580) \sim (235,-208,761).$$

Example 2. The ambiguous form $f=(5849,5849,2925)$ has discriminant $D=-34222499=-5849 \cdot 5851 \equiv 1 \pmod 4$ so its generic characters are $(\frac{\cdot}{5849})$ and $(\frac{\cdot}{5851})$. The form $f=(5849,5849,2925)$ represents primitively the odd integer 2925 which is coprime with the discriminant D. As $(\frac{2925}{5849})=(\frac{5849}{2925})=(\frac{-1}{2925})=1$ and $(\frac{2925}{5851})=(\frac{5851}{2925})=(\frac{1}{2925})=1$ the form f belongs to the principal genus. The appropriate Legendre equation is

$$5849X^2+5851Y^2=Z^2,$$

which has the solution

$$X=3, \quad Y=5, \quad Z=446.$$

A solution of

$$3v-5u=1$$

is

$$u=1, \quad v=2$$

so, by (7) and (8), a squareroot of f is given by

$$g=(223,76057,6523419) \sim (223,-209,38415).$$

https://doi.org/10.1017/S0013091500005952 Published online by Cambridge University Press

REFERENCES

1. Duncan A. Buell, *Binary Quadratic Forms* (Springer-Verlag, New York, 1989).

2. Carl Friedrich Gauss, *Disquisitiones Arithmeticae* (Yale University Press, 1966).

3. Daniel Shanks, Gauss's ternary form reduction and the 2-Sylow subgroup, *Math. Comp.* **25** (1971), 837–853. (Corrigendum, *Math. Comp.* **32** (1978), 1328–1329.)

4. Kenneth S. Williams, On the size of a solution of Legendre's equation, *Utilitas Math.* **34** (1988), 65–72.

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario
Canada K1S 5B6