Math. Proc. Camb. Phil. Soc. (1982), **92**, 29
Printed in Great Britain

Indefinite binary forms representing the same numbers

BY LI DELANG
Sichuan University, Chengdu, China

(*Received* 5 *March* 1982)

It is an old problem whether two binary quadratic forms representing the same numbers are equivalent. Legendre asserted without proof that two positive definite forms representing the same numbers are equivalent. In 1895, Bauer(1) proved Legendre's assertion for primitive forms with the same discriminant. In 1938 Delone(2) proved that two positive definite binary forms with real coefficients are equivalent if they represent the same numbers, with the sole exception of the pair equivalent to

$$x^2+xy+y^2$$
$$x^2+3y^2,$$

and their scalings. Watson(3) rediscovered this result in 1979 and asked the same question for indefinite binary forms.

In this paper we find all pairs of indefinite binary forms with rational coefficients which represent the same numbers but are not equivalent. The main results are

THEOREM 1. *Let* $f(x,y)=ax^2+bxy+cy^2$ *be a primitive binary form (i.e.* $a,b,c\in\mathbb{Z}$ *and* $(a,b,c)=1$*) with discriminant* $D=b^2-4ac$*. If* $D\equiv 5 \pmod 8$ *and the equation* $t^2-Du^2=4$ *has an integer solution with odd* u*, then* $f(x,y)$ *and* $g(x,y)=f(x,2y)$ *represent the same numbers.*

THEOREM 2. *By scaling such* $f(x,y)$ *and* $g(x,y)$*, we obtain all pairs of indefinite binary forms with rational coefficients which represent the same numbers but are not equivalent.*

Proof of Theorem 1. We have to show that for any given integers x_0, y_0, the equation $g(x,y)=f(x_0,y_0)$ has integer solutions. This is trivial if y_0 is even, so suppose that y_0 is odd. Let t,u be odd integers such that $t^2-Du^2=4$. By the theory of automorphs of binary forms, we have $f(x_0,y_0)=f(x_1,y_1)$, where

$$(x_1,y_1)=(x_0,y_0)\begin{pmatrix}(t-bu)/2 & au\\ -cu & (t+bu)/2\end{pmatrix}.$$

Since t and y_0 are both odd, we can choose the sign of t so that

$$y_1=aux_0+(t+bu)y_0/2\equiv 0 \pmod 2.$$

Hence $f(x_0,y_0)=f(x_1,y_1)=g(x_1,y_1/2)$, as required.

To prove Theorem 2, we need some lemmas.

LEMMA 1. *Let* $f(x,y)$ *and* $g(x,y)$ *be two integral forms. If* f *and* g *represent the same numbers over* $\mathbb{Z}$*, then they do so over* $\mathbb{Z}_p$ *for all primes* p*.*

As usual we denote the ring of p-adic integers by $\mathbb{Z}_p$.

https://doi.org/10.1017/S030500410005965X Published online by Cambridge University Press

Proof. Since $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ with respect to the p-adic topology and f is continuous, $f(\mathbb{Z}_p, \mathbb{Z}_p)$ is the closure of $f(\mathbb{Z}, \mathbb{Z})$. Here for example

$$f(\mathbb{Z}, \mathbb{Z}) = \{n : n = f(x, y),\ x, y \in \mathbb{Z}\}.$$

If $f(\mathbb{Z}, \mathbb{Z})$ and $g(\mathbb{Z}, \mathbb{Z})$ are the same, then so are their closures $f(\mathbb{Z}_p, \mathbb{Z}_p)$ and $g(\mathbb{Z}_p, \mathbb{Z}_p)$.

We now consider the corresponding p-adic problem, dealing first with p odd.

LEMMA 2. *Let p be an odd prime, and f and g be two p-adic integral forms. If f and g represent the same numbers over $\mathbb{Z}_p$, then the discriminants D_f and D_g satisfy $\nu_p(D_f) = \nu_p(D_g)$, where $\nu_p(\,.\,)$ denotes the p-adic exponential valuation.*

Proof. Without loss of generality, we may suppose that

$$f = ax^2 + by^2,$$
$$g = ax^2 + b_1 y^2.$$

By scaling we may assume that $a = 1$, and $b, b_1 \in \mathbb{Z}_p$. Assume that $\nu_p(b) > \nu_p(b_1)$. If $\nu_p(b_1)$ is odd, then g represents b_1, but f does not. If $\nu_p(b_1)$ is even, then g represents a number $m = m_1 p^{\nu_p(b_1)}$ with m_1 a non-unit in $\mathbb{Z}_p$, while f does not.

LEMMA 3. *If f and g are forms defined over $\mathbb{Z}_2$, which represent the same numbers over $\mathbb{Z}_2$, then*

$$\nu_2(D_f) \equiv \nu_2(D_g) \pmod 2.$$

Proof. Without loss of generality we may suppose that f and g represent 1. Assume that $\nu_2(D_f)$ is even and $\nu_2(D_g)$ is odd. Then g is equivalent to $x^2 + 2^r by^2$ with r and b odd and f is equivalent to one of the following:

$$f_1 = ax^2 + 2^{2s} b_1 y^2, \quad a, b_1 \text{ odd}$$
$$f_2 = xy$$
$$f_3 = c(x^2 + xy + y^2), \quad c \text{ odd}.$$

Case 1. $f \sim f_1 = ax^2 + 2^{2s} b_1 y^2$.

In this case, g represents both $2^{2s} b_1$ and $2^{2s}(b_1 + 4a)$. Therefore

$$(b_1, -2b)_2 = (b_1 + 4a, -2b)_2 = 1, \tag{1}$$

where $(x, y)_2$ is the Hilbert norm residue symbol with respect to 2. But (1) is impossible for odd a, b and b_1 since $b_1 + 4a \equiv 5b \pmod 8$ and $(5, -2b)_2 = -1$ for all odd b.

Case 2. $f \sim f_2 = xy$.

In this case f represents every number in $\mathbb{Z}_2$ while g does not represent any number $m \equiv 5 \pmod 8$.

Case 3. $f \sim f_3 = c(x^2 + xy + y^2)$.

Now $\nu_2(f(x, y))$ is always even, but g represents $2^r b$ with odd r and b.

LEMMA 4. *Let f and g be primitive forms over $\mathbb{Z}_2$ with $\nu_2(D_f) < \nu_2(D_g)$ which represent the same numbers. Then*

$$f \sim c(x^2 + xy + y^2),$$
$$g \sim c(x^2 + 3y^2),$$

where c is a unit in $\mathbb{Z}_2$. Hence $D_f \equiv 5 \pmod 8$ and $D_g = 4D_f$.

https://doi.org/10.1017/S030500410005965X Published online by Cambridge University Press

Proof. If both $\nu_2(D_f)$ and $\nu_2(D_g)$ are odd, then

$$f \sim ax^2 + b2^{2r+1}y^2,$$
$$g \sim a_1x^2 + b_1 2^{2s+1}y^2,$$

where $s > r$ and a, b, a_1, b_1 are all odd. Hence g does not represent $b2^{2r+1}$. We may thus suppose that $\nu_2(D_f)$ and $\nu_2(D_g)$ are both even.

If

$$f \sim ax^2 + 2^{2r}by^2,$$
$$g \sim a_1x^2 + 2^{2s}b_1y^2,$$

where $s > r$ and a, b, a_1, b_1 are odd, we have

$$a_1 \equiv a \equiv b \pmod 4,$$

since g represents $2^{2r}b$ and a and $s > r$. But then f represents $2^{2r}(a+b) \equiv 2^{r+1} \pmod{2^{2r+2}}$ and g does not.

It is easy to see that f cannot be cxy, which is universal over $\mathbb{Z}_2$.

Therefore we have

$$f \sim c(x^2 + xy + y^2), \quad c \text{ odd},$$
$$g \sim ax^2 + b2^{2r}y^2, \quad a, b \text{ odd}.$$

If $r \geqslant 1$, then g represents at most one of c and $3c$ while f represents both. Hence $r = 0$. Since g represents c, we can write

$$g \sim cx^2 + by^2, \quad b \text{ odd}.$$

We must have $b \equiv 3c \pmod 8$ for $\nu_2(f(x,y))$ is always even and so g does not represent $2c$, $6c$, or $8c$.

We can now summarize the result of Lemmas 1–4 as follows:

LEMMA 5. *Let f, g be primitive forms defined over $\mathbb{Z}$ which represent the same numbers. Suppose that $D_f \leqslant D_g$. Then either*

$$(1) \quad D_f = D_g$$

or

$$(2) \quad D_g = 4D_f \quad \text{and} \quad D_f \equiv 5 \pmod 8.$$

Proof. D_f and D_g have the same sign because f, g are either both definite or both indefinite. By Lemmas 1, 2 we have $\nu_2(D_f) = \nu_2(D_g)$ for all odd primes. The rest follows from Lemmas 1, 3 and 4.

LEMMA 6. *Let f, g be two forms over $\mathbb{Z}$ with $D_f = D_g$. If both f and g represent an odd prime p, then f and g are equivalent, possibly improperly.*

Proof. We may assume that

$$f(x,y) \sim px^2 + b_1xy + c_1y^2, \quad |b_1| < p/2,$$
$$g(x,y) \sim px^2 + b_2xy + c_2y^2, \quad |b_2| < p/2.$$

From $D_f = D_g$, it follows that

$$b_2^2 \equiv b_2^2 \pmod p,$$

and therefore $b_1 = \pm b_2$, $c_1 = c_2$.

https://doi.org/10.1017/S030500410005965X Published online by Cambridge University Press

LEMMA 7. *Let f be a primitive binary form. Then f represents infinitely many primes.*

Proof. See Weber (4).

Remark. We can prove that the Dirichlet density of the set of primes represented by f is

$$\Delta = \begin{cases} 1/h & f \text{ is not ambiguous,} \\ 1/2h & f \text{ is ambiguous,} \end{cases}$$

where h is the class number of binary forms with discriminant D, in the narrow sense. This can be used to give another proof of Theorem 2.

Proof of Theorem 2. Suppose that f, g are two forms with rational coefficients representing the same numbers. By scaling, we may assume that both f and g are primitive. If f and g have the same discriminant, then f is equivalent to g by Lemmas 6 and 7. Therefore by Lemma 5 we may assume that $D_g = 4D_f$ and $D_f \equiv 5 \pmod 8$. By taking an equivalent form for f if necessary we may suppose that $f = ax^2 + bxy + cy^2$ with $(a, 2D) = 1$. The form $h(x, y) = f(x, 2y)$ has discriminant $D_h = 4D_f = D_g$ and h is primitive. The form $h(x, y)$ represents a prime by Lemma 7 which is represented by $f(x, y)$ and hence by $g(x, y)$. Therefore $g(x, y) \sim h(x, y)$ by Lemma 6.

To prove that $t^2 - Du^2 = 4$ has a solution with odd u, we note first that there are primes p_1, p_2 such that $p_1 = f(x_1, y_1)$ with x_1 and y_1 odd and $p_2 = f(x_2, y_2)$ with x_2 even, y_2 odd. In fact the forms $f_1(x, y) = f(2x + y, y)$ and $f_2(x, y) = f(2x, y)$ are both primitive. Therefore $f(2x + y, y) = p_1$ and $f(2x, y) = p_2$ have solutions for suitable odd primes p_1 and p_2. It is clear that y must be odd.

Now suppose that

$$f(x, y) = p \quad y \text{ odd},$$

$$h(x_0, y_0) = f(x_0, 2y_0) = p,$$

where p is an odd prime. By the theory of automorphs, there exists an automorph (possibly improper) of f which sends $(x_0, 2y_0)$ to (x, y).

If the equation $t^2 - Du^2 = 4$ has no solutions with odd t, u, then every proper automorph has matrix

$$T = \begin{pmatrix} (t - bu)/2 & au \\ -cu & (t + bu)/2 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2$$

Therefore it is impossible that

$$(x, y) = (x_0, 2y_0)\, T$$

for odd y.

If

$$S = \begin{pmatrix} l & m \\ n & k \end{pmatrix},$$

is the matrix of an improper automorph, every improper automorph has matrix ST for proper T, and so it is congruent to $S \pmod 2$. Hence

$$(x, y) \equiv (x_0, 2y_0)\, S \equiv (lx_0 + 2ny_0, mx_0 + 2ky_0) \pmod 2,$$

https://doi.org/10.1017/S030500410005965X Published online by Cambridge University Press

which implies that

$$x \equiv lx_0 \pmod 2.$$

This contradicts the fact that both

$$f(2z+1, y) = p$$

and

$$f(2z, y) = p$$

are possible.

Acknowledgement. The author has pleasure in thanking Professor Cassels for helpful suggestions which resulted in simplifications of the proof. The results were obtained whilst the author was visiting Cambridge University.

REFERENCES

(1) Bauer, M. B. *Math. és Termès Ertesitö* **13** (1895), 316–322.
(2) Delone, B. N. Geometry of positive quadratic forms addendum. *Uspehi Mat. Nauk* **4** (1938).
(3) Watson, G. L. Determination of a binary quadratic form by its values at integer points. *Mathematika* **26** (1979), 72–75, and **27** (1980), 188.
(4) Weber, H. Über Zahlen gruppen in algebraischen Zahlkorpern. *Mathematische Annalen* I, **48** (1897), 433–473; II, **49** (1897), 83–100; III, **50** (1898), 1–26.

https://doi.org/10.1017/S030500410005965X Published online by Cambridge University Press