Far East J. Math. Sci. 5 (1)(1997), 153-157

ON A FORMULA OF DIRICHLET

PIERRE KAPLAN and KENNETH S. WILLIAMS

(Received October 30, 1996)

Submitted by K. K. Azad

Abstract

The range of validity of Dirichlet's formula for the number of primary representations of the positive integer n by a representative set of inequivalent, primitive, integral, binary quadratic forms of discriminant d is extended from gcd (n, d) = 1 to gcd (n, f) = 1, where f is the conductor of the discriminant d.

Let n be a positive integer and let d be a nonsquare integer with $d \equiv 0$ or 1 (mod 4). Let $\{f_i(x, y) = a_i x^2 + b_i xy + c_i y^2 \mid i = 1, 2, \ldots, h\}$ be a representative set of inequivalent, primitive, integral, binary quadratic forms of discriminant d. Only positive-definite forms are taken if $d < 0$. Let $N(n, d)$ denote the number of primary representations of n by the forms $f_i(x, y)$ ($i = 1, 2, \ldots, h$). For the necessary background on binary quadratic forms, the reader is referred to [2, § 11.4, § 12.1-12.4]. Dirichlet [1, p. 229] showed in 1840 that if gcd $(n, d) = 1$, then

$$N(n, d) = w(d) \sum_{e \mid n} \left(\frac{d}{e}\right) \tag{1}$$

where $w(d) = 1, 2, 4, 6$ according as $d > 0$, $d < -4$, $d = -4$, $d = -3$ respectively, e runs through the positive divisors on n, and $\left(\frac{d}{e}\right)$ is the Kronecker symbol. It is the purpose of this note to show that a simple argument extends the range of validity of

1991 Mathematics Subject Classification : 11E16.

Key words and phrases : binary quadratic forms, Dirichlet's formula, number of representations.

(1) from gcd $(n, d) = 1$ to gcd $(n, f) = 1$, where f is the conductor of d, that is, f is the largest positive integer such that $f^2 \mid d$ and $d/f^2 \equiv 0$ or 1 (mod 4). This fact seems to have been totally overlooked until recently. Our extension of Dirichlet's formula follows from (1) and the simple lemmas below.

Lemma 1. *Let p be a prime with $p \mid d$ and $p \nmid f$. Then each $f_i(x, y)$ $(i = 1, 2, \ldots, h)$ can be taken in the form*

$$f_i(x, y) = a_i x^2 + b_i xy + c_i p y^2,$$

where $p \nmid a_i c_i$ and $p \mid b_i$.

Proof. Replacing $f_i(x, y)$ by an equivalent form, we may suppose that $p \nmid a_i$. If $p \neq 2$ then as $p \mid d$ and $p \nmid f$, we have $p \parallel d$. We may choose an integer t such that $b_i' = 2a_i t + b_i \equiv 0 \pmod p$. Then $f_i(x, y)$ is equivalent to the form $a_i x^2 + b_i' xy + c_i' y^2$, where $c_i' = a_i t^2 + b_i t + c_i$, which is of the required type as $p \parallel c_i'$ since $c_i' = (b_i'^2 - d)/(4a_i)$, $p \parallel d$ and $p \mid b_i'$.

If $p = 2$ then, as $2 \mid d$ and $2 \nmid f$, we see that $2 \mid b_i$ and $d \equiv 8$ or $12 \pmod{16}$. If $c_i \equiv 2 \pmod 4$ then $f_i(x, y)$ is already of the required type. If $c_i \not\equiv 2 \pmod 4$, from $d = b_i^2 - 4a_i c_i$, we deduce that $c_i \equiv 1 \pmod 2$ and $a_i + b_i + c_i \equiv 2 \pmod 4$. Replacing f_i by the equivalent form $a_i x^2 + (2a_i + b_i) xy + (a_i + b_i + c_i) y^2$, we have f_i in the required form.

Lemma 2. *With the notation of Lemma 1,*

$$\{ a_i p x^2 + b_i xy + c_i y^2 \mid i = 1, 2, \ldots, h \}$$

is a representative system of inequivalent, primitive, integral binary quadratic forms of discriminant d.

Proof. We have only to check that $a_i p x^2 + b_i xy + c_i y^2$ and $a_j p x^2 + b_j xy + c_j y^2$ are inequivalent for $i \neq j$. Suppose not. Then there exist integers r, s, t, u with $ru - st = 1$ such that

$$a_i px^2 + b_i xy + c_i y^2 = a_j p (rx + sy)^2 + b_j (rx + sy)(tx + uy) + c_j (tx + uy)^2.$$

Hence

$$a_i p = a_j pr^2 + b_j rt + c_j t^2 ,$$

$$b_i = 2a_j prs + b_j (ru + st) + 2c_j tu ,$$

$$c_i = a_j ps^2 + b_j su + c_j u^2 .$$

As $p \nmid a_i c_i, p \mid b_i, p \nmid a_j c_j$, and $p \mid b_j$, we see that $p \nmid u$ and $p \mid t$. Set $t = pt'$ and $s' = ps$. Then $ru - s' t' = 1$ and

$$a_i = a_j r^2 + b_j r t' + c_j pt'^2 ,$$

$$b_i = 2a_j rs' + b_j (ru + s' t') + 2cjpt' u ,$$

$$pc_i = a_j s'^2 + b_j s'u + pc_j u^2 ,$$

so that

$$a_i x^2 + b_i xy + c_i py^2 = a_j (rx + s' y)^2 + b_j (rx + s'y) (t'x + uy) + c_j p (t' x + uy)^2 ,$$

contradicting that $a_i x^2 + b_i xy + c_i p y^2$ and $a_j x^2 + b_j xy + c_j p y^2$ are inequivalent for $i \neq j$.

From now on we suppose that n is prime to f and we set

$$n = n_1 n_2 , \quad n_1 = \prod_{p \mid d} p^{\nu_p(n)} , \quad n_2 = \prod_{p \nmid d} p^{\nu_p(n)} ,$$

so that gcd (n_2 , d) = 1. We have

Lemma 3.

$$N(n, d) = N(n_2, d) .$$

Proof. Let p be a prime with $p \mid n_1$. As $p \mid d$ and $p \nmid f$ we can choose each representative form f_i as in Lemma 1. For $i = 1, \ldots h$, let

$$S_i = \text{set of primary solutions } (x, y) \text{ of } a_i x^2 + b_i xy + c_i p y^2 = n$$

and

$$T_i = \text{set of primary solutions } (x, y) \text{ of } a_i p x^2 + b_i x y + c_i y^2 = n/p.$$

It is easy to check that $(x, y) \to (px, y)$ defines a bijection from T_i to S_i. Hence, by Lemma 2, we have

$$N(n, d) = \sum_{i=1}^{h} card(S_i) = \sum_{i=1}^{n} card(T_i) = N(n/p, d).$$

Applying this result to each prime p dividing n_1, we obtain the result of Lemma 3.

We can now complete the proof that Dirichlet's formula (1) holds for gcd $(n, f) = 1$. If e is a divisor of n such that $e \nmid n_2$ then gcd $(e, n_1) > 1$ so that $\left(\frac{d}{e}\right) = 0$ and thus

$$\begin{aligned} N(n, d) &= N(n_2, d) && \text{(by Lemma 3)} \\ &= w(d) \sum_{e \mid n_2} \left(\frac{d}{e}\right) && \text{(by (1) as gcd } (n_2, d) = 1) \\ &= w(d) \sum_{e \mid n} \left(\frac{d}{e}\right) && \text{(by the preceding remark).} \end{aligned}$$

We remark that Dirichlet's formula (1) may not hold if gcd $(n, f) > 1$. To see this take $d = -16$ and $n = 2$. Here $f = 2$, $w(-16) = 2$, and $h = 1$. We can take the single representative primitive, positive-definite, integral, binary quadratic form of discriminant -16 as $x^2 + 4y^2$. Clearly this form does not represent 2 so that $N(2, -16) = 0$. However

$$w(-16) \sum_{\mu \mid 2} \left(\frac{-16}{\mu}\right) = 2\left(\left(\frac{-16}{1}\right) + \left(\frac{-16}{2}\right)\right) = 2(1 + 0) = 2.$$

When $d < 0$ a formula for $N(n, d)$ valid for all positive integers n has been given by Huard, Kaplan and Williams [3].

References

[1] P. G. L. Dirichlet, Vorlesungen über Zahlentheorie, Chelsea Publishing Co., New York, 1968.

[2] L. - K. Hua, Introduction to Number Theory, Springer-Verlag (Berlin, Heidelberg, New York), 1982.

[3] J. G. Huard, P. Kaplan and K. S. Williams, The Chowla-Selberg formula for genera, Acta Arithmetica 73 (1995), 271-301.

Départment de Mathématiques
Université de Nancy 1,
B. P. 239, 54506 Vandoeuvre lés Nancy Cédex
France
E-mail address: kaplan@iecn.u-nancy.fr

Centre for Research in Algebra and Number Theory
Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario
Canada K1S 5B6
E-mail address: williams@math.carleton.ca