Math. Proc. Camb. Phil. Soc. (1999), **126**, 17

Printed in the United Kingdom © 1999 *Cambridge Philosophical Society*

The average number of divisors of an irreducible quadratic polynomial†

By JAMES McKEE
Pembroke College, Oxford OX1 1DW

(*Received* 18 *August* 1997; *revised* 12 *December* 1997)

1. *Introduction*

For a non-zero integer n, let $d(n)$ denote the number of positive divisors of n. Let a, b and c be integers with $a > 0$, and set $\Delta = b^2 - 4ac$. If the quadratic polynomial ax^2+bx+c is irreducible over the rational numbers $\mathbf{Q}$ (that is, if Δ is not the square of an integer), then one has

$$\sum_{n \leqslant X} d(an^2+bn+c) \sim \lambda X \log X, \tag{1}$$

as $X \to \infty$, for some λ depending on a, b and c (see [**7**]). In this paper we discuss the way in which λ depends on a, b and c, giving a precise, compact expression in terms of class numbers. This extends previous work for the case $a = 1$, $\Delta < 0$ (see [**4**]).

For the case $a = 1$, $b = 0$, a much better description of the error is given in [**2**], with the following expression for λ:

$$\lambda = (8/\pi^2) \sum_{\alpha=0}^{\infty} \rho(2^\alpha)/2^\alpha \sum_{\substack{d^2 \mid c \\ d \text{ odd}}} 1/d \sum_{\substack{l=1 \\ l \text{ odd}}}^{\infty} \left(\frac{-c/d^2}{l}\right) \Big/ l. \tag{2}$$

Here ρ is a multiplicative function, defined below, and $(\frac{p}{q})$ is the Legendre/Jacobi symbol.

As well as looking for improvements to the error term, one can also seek a nice expression for λ (clearly a subjective matter). Comparison of (2) with Dirichlet's analytic class number formula (section 10·3 of [**6**]) indicates a close connection with class numbers. Indeed a connection with class numbers was pointed out by Hooley in [**1**] and [**3**]. For the case $a = 1$, $b^2 - 4c < 0$, a more compact expression for λ is given in [**4**], namely

$$\lambda = 12H^*(\Delta)/\pi \sqrt{|\Delta|}.$$

Here $H^*(\Delta)$ is the Kronecker/Hurwitz class number, which counts all classes of binary quadratic forms with discriminant Δ (both primitive and imprimitive), counting the class of $Ax^2+Bxy+Cy^2$ with weight inversely proportional to the size of its automorphism group.

Kronecker's class number, $H^*(\Delta)$, makes sense only for $\Delta < 0$, since for $\Delta > 0$ all the relevant automorphism groups are infinite. In this paper we give an extension of $H^*(\Delta)$ to $\Delta > 0$, giving each class a weighting which is, with the benefit of hindsight, a natural extension of Kronecker's. We then prove:

† This work was done whilst the author was at the Department of Mathematics and Statistics, University of Edinburgh, Edinburgh EH9 3JZ.

THEOREM. *Let b and c be integers with $\Delta = b^2-4c$ not a square. Then*

$$\sum_{n \leqslant X} d(n^2+bn+c) = \lambda X \log X + O(X),$$

where the implied constant in the $O(.)$ depends on b and c, and λ is defined by

$$\lambda = \begin{cases} 12H^*(\Delta)/\pi\sqrt{|\Delta|} & \text{if } \Delta < 0, \\ 12H^*(\Delta)\log\delta(\Delta)/\pi^2\sqrt{\Delta} & \text{if } \Delta > 0, \end{cases} \tag{3}$$

where $H^*(\Delta)$ is a weighted class number, and (for $\Delta > 0$) $\delta(\Delta)$ is a fundamental unit. For $\Delta < 0$, $H^*(\Delta)$ is defined below by (6); for $\Delta > 0$, $H^*(\Delta)$ and $\delta(\Delta)$ are defined below by (9) and (10).

To complete the picture, we may ask what happens to λ in (1) if a is greater than 1. A method for tackling this case is sketched in the introduction to [**5**]. The slightly tedious details are omitted. If $a > 1$, then the expression for λ in (3) should be multiplied by

$$\prod_{p|a} (1+\rho(p)/p+\rho(p^2)/p^2+\cdots)/(1+\tilde{\rho}(p)/p+\tilde{\rho}(p^2)/p^2+\cdots), \tag{4}$$

where the product is over prime divisors of a, $\rho(d)$ is the number of solutions to the quadratic congruence

$$an^2+bn+c \equiv 0 \pmod{d}, \quad 0 \leqslant n < d, \tag{5}$$

and $\tilde{\rho}(d)$ is the number of solutions to the quadratic congruence

$$n^2+bn+ac \equiv 0 \pmod{d}, \quad 0 \leqslant n < d.$$

Note that if $\gcd(a,b) = 1$, then (4) simplifies to

$$\prod_{p|a} p/(p+1).$$

The case $\Delta < 0$ in the Theorem is proved in [**4**]. Here we prove the case $\Delta > 0$, having defined a suitable extension of the Kronecker/Hurwitz class number to cover positive discriminants. It is tempting just to define $H^*(\Delta)$ for $\Delta > 0$ such that (3) holds (with the classical definition of $\delta(\Delta)$), but this would be unedifying. Instead we show how to assign a weighting to classes of forms such that if $H^*(\Delta)$ counts classes with these prescribed weights then (3) holds.

For $\Delta > 0$, binary quadratic forms with discriminant Δ have infinite automorphism groups. To define $H^*(\Delta)$ for $\Delta > 0$, we consider the index of a possibly smaller subgroup within the automorphism group, and count with weight inversely proportional to this index. This is seen to agree with Kronecker's definition for $\Delta < 0$ (with a small caveat), and gives just the right weighting for (3) to hold. Primitive classes are counted with weight 1. Imprimitive classes are counted with weight at most 1, but sometimes strictly less. For a given Δ, distinct classes may or may not be given different weights.

The next section of this paper is devoted to defining $H^*(\Delta)$. Then we prove the Theorem. The classical attack is to estimate the sum $\sum_{n \leqslant x} \rho(n)/n$, which leads

directly to an expression for λ, much as in (2). As in [**4**], however, we proceed indirectly, via an estimate of $\sum_{n \leqslant x} \rho(n)$, in order to reveal the precise connection with the weighted class number.

2. *A weighted class number*

For integers A, B and C with B^2-4AC not a square, let (A, B, C) denote the binary quadratic form $Ax^2+Bxy+Cy^2$. The group $SL_2(\mathbf{Z})$ acts on the set of all such forms via

$$(A,B,C)\begin{pmatrix} p & q \\ r & s \end{pmatrix} = (A',B',C'),$$

where

$$\begin{pmatrix} A' & B'/2 \\ B'/2 & C' \end{pmatrix} = \begin{pmatrix} p & r \\ q & s \end{pmatrix}\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

Forms in the same orbit under this action are called equivalent. The discriminant of (A,B,C) is B^2-4AC, and this is invariant under equivalence. The number of equivalence classes of forms with discriminant Δ is finite, and is denoted $H(\Delta)$. Note that there is no requirement that $\gcd(A, B, C) = 1$.

The stabilizer of (A, B, C) under the action of $SL_2(\mathbf{Z})$ is called the automorphism group of (A, B, C), denoted $\mathrm{Aut}(A, B, C)$. Equivalent forms have isomorphic automorphism groups.

Let $S(\Delta)$ be a set of representatives of the equivalence classes of forms with discriminant Δ. For $\Delta < 0$, the Kronecker/Hurwitz weighted class number, $H^*(\Delta)$, is defined by counting each class of forms with weight twice the reciprocal of the size of the automorphism group of forms in that class. Thus

$$H^*(\Delta) = \sum_{(A,B,C)\in S(\Delta)} 2/|\mathrm{Aut}(A,B,C)|, \tag{6}$$

where $|.|$ denotes the cardinality of a set.

This is the appropriate class number for our purpose when $\Delta < 0$ (see [**4**]), but the definition makes sense only for $\Delta < 0$, since $\mathrm{Aut}(A, B, C)$ is infinite when $\Delta > 0$. Indeed if $\Delta > 0$ then $\mathrm{Aut}(A, B, C)$ is isomorphic to $\mathbf{Z}\times\mathbf{Z}_2$, and can be described concretely. Let $f = \gcd(A, B, C)$, and let v, w be positive integers giving the fundamental solution to

$$v^2-\Delta w^2/f^2 = 4. \tag{7}$$

Then the automorphisms of (A, B, C) are precisely $\pm T^n$ $(n\in\mathbf{Z})$, where

$$T = \begin{pmatrix} v/2-Bw/2f & -Cw/f \\ Aw/f & v/2+Bw/2f \end{pmatrix}. \tag{8}$$

The map

$$\pm T^n \mapsto \pm(v/2+w\sqrt{\Delta}/2f)^n$$

embeds $\mathrm{Aut}(A, B, C)$ as a subgroup of the group of units of the ring of integers of the quadratic field $\mathbf{Q}(\sqrt{\Delta})$. So far this is all standard: see, for example [**6**] (this treats only the case $f = 1$, but the extension to any f is straightforward).

Let P_Δ be the principal form with discriminant Δ (that is, either $P_\Delta = (1, 0, -\Delta/4)$ or $P_\Delta = (1, 1, (1-\Delta)/4)$, according as $\Delta \equiv 0 \pmod 4$ or $\Delta \equiv 1 \pmod 4$). Then if (A, B, C) has discriminant $\Delta > 0$, $\mathrm{Aut}(P_\Delta)$ embeds in $\mathrm{Aut}(A, B, C)$ via the identity map:

$$x/2 + y\sqrt{\Delta}/2 \mapsto x/2 + fy\sqrt{\Delta}/2f.$$

For $\Delta > 0$, define $H^*(\Delta)$ by

$$H^*(\Delta) = \sum_{(A,B,C)\in S(\Delta)} 1/[\mathrm{Aut}(A,B,C) : \mathrm{Aut}(P_\Delta)]. \tag{9}$$

In other words, we count the class containing (A, B, C) with weight given by the reciprocal of the index of $\mathrm{Aut}(P_\Delta)$ in $\mathrm{Aut}(A, B, C)$. Note that this definition makes sense for $\Delta < 0$ also, and agrees with the former definition of $H^*(\Delta)$ unless $\Delta = -3$ or $\Delta = -4$. In particular, if $\Delta = -3n^2$ or $\Delta = -4n^2$ (the only non-trivial cases), then our definition agrees with Kronecker's unless $n = 1$. When $n = 1$ it is the principal form itself which has unusually many automorphisms, so it is not surprising that this index formula for the weight breaks down.

Another formula for $H^*(\Delta)$ will be used in the proof of the Theorem. For $D > 0$, D not a square, define

$$\delta(D) = (v + w\sqrt{D})/2, \tag{10}$$

where v and w give the fundamental solution to the Pellian equation

$$v^2 - Dw^2 = 4.$$

Then, from (7) and (8),

$$\delta(\Delta) = \delta(\Delta/f^2)^{[\mathrm{Aut}(A,B,C) : \mathrm{Aut}(P_\Delta)]},$$

hence (9) gives

$$H^*(\Delta) = \sum_{(A,B,C)\in S(\Delta)} \log \delta(\Delta/f^2)/\log \delta(\Delta), \tag{11}$$

where, as before, $f = f(A, B, C) = \gcd(A, B, C)$.

These definitions of H^* and δ are used in the statement of the Theorem. Note that if Δ is fundamental, then this weighted class number is none other than the classical class number. If Δ is not fundamental, then the weighted class number may be different, and note also that different classes may be given different weights.

Examples. If $\Delta = 5$, we can take $S(\Delta) = \{(1, 1, -1)\}$, and $H(5) = H^*(5) = 1$. Also note that $\delta(5) = (3 + \sqrt{5})/2$.

If $\Delta = 20$, we can take $S(\Delta) = \{(1, 0, -5), (2, 2, -2)\}$, and $H(20) = 2$. To compute H^*, note that $\delta(20) = (18 + 4\sqrt{20})/2 = \delta(5)^3$, so we count $(2, 2, -2)$ with weight $1/3$, and $H^*(20) = 4/3$. Here we see a simple example where different classes are counted with different weights.

3. *Proof of Theorem*

As remarked in the introduction, the case $\Delta < 0$ is proved in [**4**], so we may suppose that $\Delta > 0$.

As before, $S(\Delta)$ denotes a set of representatives of the equivalence classes of forms (A, B, C) with discriminant Δ (allowing $\gcd(A, B, C) > 1$), but now we choose representatives such that $A > 0$ whenever $(A, B, C) \in S(\Delta)$.

Suppose that d is a positive integer, and for some $(A, B, C) \in S(\Delta)$ we have

$$Ap^2+Bpq+Cq^2 = d, \quad \gcd(p,q) = 1. \tag{12}$$

Such a representation of d is called a proper representation. Then there exist r_0, $s_0 \in \mathbf{Z}$ with $ps_0 - qr_0 = 1$, and the general solution to $ps-qr=1$ is $s = s_0+tq$, $r = r_0+tp$ $(t \in \mathbf{Z})$. If

$$(A,B,C)\begin{pmatrix} p & q \\ r_0 & s_0 \end{pmatrix} = (d, m_0, l_0),$$

then

$$(A,B,C)\begin{pmatrix} p & q \\ r & s \end{pmatrix} = (d, m, l)$$

with $m = m_0+2td$. Hence, for any given integer k, our proper representation of d, (12), leads to a unique $m = m_0+2td$ with $k \leqslant m < k+2d$. We choose $k = b$, with b as in the statement of the Theorem. Moreover, $m^2 \equiv \Delta \pmod{4d}$, since (d, m, l) has discriminant Δ, so (12) leads to a unique m satisfying

$$m^2 \equiv \Delta \pmod{4d}, \quad b \leqslant m < b+2d. \tag{13}$$

Conversely, a solution to (13), $m^2-4dl = \Delta$, implies that (d, m, l) is a form with discriminant Δ, which properly represents d. Now (d, m, l) must be equivalent to a unique element of $S(\Delta)$, say (A, B, C). Then

$$(A,B,C) = (d,m,l)\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

for some $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL_2(\mathbf{Z})$, and (A, B, C) properly represents d, with the representation determined by (d, m, l) and $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$. Now $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ is unique up to an automorphism of (A, B, C), and all such are given by (plus or minus) powers of the fundamental automorphism (8). The fundamental automorphism transforms the line $y = 0$ in the (x, y)-plane into the line

$$(v-Bw/f)\,y = 2(Aw/f)x,$$

and we conclude that a solution to (13) leads to a unique proper representation of d by some $(A, B, C) \in S(\Delta)$, $Ax^2+Bxy+Cy^2 = d$, with $x, y \geqslant 0$, $\gcd(x, y) = 1$ and

$$0 \leqslant y/x < 2Aw/(fv-Bw).$$

If we let $\rho(d)$ be the number of solutions to (5), with $a = 1$, then completing the square and setting $m = 2n+b$ we see that $\rho(d)$ equals the number of solutions to (13). From the above argument it follows that

$$\rho(d) = \sum_{(A,B,C)\in S(\Delta)} \sum_{\substack{Ap^2+Bpq+Cq^2=d,\ \gcd(p,q)=1,\\ 0\leqslant q/p<2Aw/(fv-Bw)}} 1, \tag{14}$$

where v and w, defined by (7), depend on (A, B, C) in as much as they depend on $f = \gcd(A, B, C)$. Here the (p, q) sum is over pairs of positive integers satisfying the various conditions (except that we could have $q = 0$ if $d = A$).

Examples. For example, if our polynomial is n^2-5, then $\Delta = 20$ and we may take $S = \{(1, 0, -5), (2, 2, -2)\}$.

If $d = 4$, then $\rho(d) = \rho(4)$ is the number of solutions to (5) (with $a = 1$, $b = 0$,

$c=-5$, $d=4$), hence $\rho(d)=2$. There are two proper representations of 4 as x^2-5y^2 with $x,\ y\geqslant 0$ and $0\leqslant y/x<2{\cdot}1{\cdot}4/(1{\cdot}18-0{\cdot}4)=4/9$, namely $4=3^2-5{\cdot}1^2$ and $4=7^2-5{\cdot}3^2$.

Or with $d=10$, we have $\rho(d)=1$, and there is just one proper representation of 10 as $2x^2+2xy-2y^2$ with $x,\ y\geqslant 0$ and $0\leqslant y/x<2{\cdot}1{\cdot}1/(2{\cdot}3-0{\cdot}1)=1/2$, namely $10=2{\cdot}2^2+2{\cdot}2{\cdot}1-2{\cdot}1^2$.

We can use (14) to estimate $\Sigma_{d\leqslant X}\rho(d)$. Note that the estimate for the number of positive integers p and q satisfying the two conditions $1\leqslant Ap^2+Bpq+Cq^2\leqslant X/e^2$ and $0\leqslant q/p<2Aw/(fv-Bw)$, generalizes lemma 3·5($b$) in chapter 10 of [**6**]. Throughout, p and q are non-negative integers, μ is the Möbius function, and ν depends on $(A,\ B,\ C)$. Implied constants in $O(.)$ expressions may depend on $S(\Delta)$.

$$\begin{aligned}\sum_{d\leqslant X}\rho(d)&=\sum_{(A,B,C)\in S(\Delta)}\ \sum_{\substack{1\leqslant Ap^2+Bpq+Cq^2\leqslant X,\ \gcd(p,q)=1,\\ 0\leqslant q/p<2Aw/(fv-Bw)}}1\\ &=\sum_{(A,B,C)\in S(\Delta)}\ \sum_{e\leqslant\nu\sqrt{X}}\mu(e)\sum_{\substack{1\leqslant Ap^2+Bpq+Cq^2\leqslant X/e^2,\\ 0\leqslant q/p<2Aw/(fv-Bw)}}1\\ &=(6X/\pi^2\sqrt{\Delta})\sum_{(A,B,C)\in S(\Delta)}\log\delta(\Delta/f^2)+O(\sqrt{X}\log X).\end{aligned}$$

Thus, using (11), we get

$$\sum_{d\leqslant X}\rho(d)=6H^*(\Delta)\log\delta(\Delta)\,X/\pi^2\sqrt{\Delta}+O(\sqrt{X}\log X). \tag{15}$$

We have the classical estimate

$$\sum_{n\leqslant X}d(n^2+bn+c)=2X\sum_{d\leqslant X}\rho(d)/d+O\Big(\sum_{d\leqslant X}\rho(d)\Big)+O(X) \tag{16}$$

(see, e.g. [**4**]). Our estimate for $\Sigma_{d\leqslant X}\rho(d)$, (15), fed into (16), and using partial summation, gives

$$\sum_{n\leqslant X}d(n^2+bn+c)=12H^*(\Delta)\log\delta(\Delta)\,X\log X/\pi^2\sqrt{\Delta}+O(X),$$

as desired.

REFERENCES

[**1**] C. HOOLEY. On the representation of a number as the sum of a square and a product. *Math. Z.* **69** (1958), 211–227.

[**2**] C. HOOLEY. On the number of divisors of quadratic polynomials. *Acta Math.* **110** (1963), 97–114.

[**3**] C. HOOLEY. *Applications of sieve methods to the theory of numbers*. Cambridge Tracts in Mathematics 70 (Cambridge University Press, 1976).

[**4**] J. F. MCKEE. On the average number of divisors of quadratic polynomials. *Math. Proc. Camb. Phil. Soc.* **117** (1995), 389–392.

[**5**] J. F. MCKEE. A note on the number of divisors of quadratic polynomials; in *Sieve methods, exponential sums, and their application in number theory*, London Mathematical Society Lecture Note Series **237** (Cambridge University Press, 1997), pp. 275–281.

[**6**] H. E. ROSE. *A course in number theory* (Oxford University Press, 1988).

[**7**] E. J. SCOURFIELD. The divisors of a quadratic polynomial. *Trans. Glasgow Math. Assoc.* **5** (1961), 8–20.