Functiones et Approximatio
XXXVII.1 (2007), 203–211

QUADRATIC CLASS NUMBERS DIVISIBLE BY 3

D. Roger Heath-Brown

Dedicated to Jean-Marc Deshouillers
in celebration of his Sixtieth Birthday

Abstract: Let $N_+(X)$ denote the number of distinct real quadratic fields $\mathbb{Q}(\sqrt{d})$ with $d \leqslant X$ for which $3|h(\mathbb{Q}(\sqrt{d}))$. Define $N_-(X)$ similarly for $\mathbb{Q}(\sqrt{-d})$. It is shown that $N_+(X), N_-(X) \gg X^{9/10-\varepsilon}$ for any $\varepsilon > 0$. This improves results of Byeon and Koh [2] and of Soundararajan [7], which had exponent $7/8 - \varepsilon$.
Keywords: class number, quadratic field, divisible, density.

Let d be a square-free integer, which may be positive or negative, and let $h(-d)$ be the class number of $\mathbb{Q}(\sqrt{-d})$. In this paper we investigate the frequency of values of d for which $3|h(-d)$. It follows from conjectures of Cohen and Lenstra [3], that asymptotically a constant proportion of values of d have this property. The conjectured proportion is different for positive and negative d, being

$$1 - \prod_{j=1}^{\infty}(1 - 3^{-j})$$

in the case of imaginary quadratics, for example. It follows from the work of Davenport and Heilbronn [5] that a positive proportion of d have $3 \nmid h(-d)$, both in the case of d positive and d negative. However it remains an open problem whether or not the same is true for values with $3|h(-d)$.

Write $N_-(X)$ for the number of positive square-free $d \leqslant X$ for which $3|h(-d)$, and similarly let $N_+(X)$ be the number of positive square-free $d \leqslant X$ for which $3|h(d)$. It was shown by Ankeny and Chowla [1] that $N_-(X)$ tends to infinity with X, and in fact their method yields $N_-(X) \gg X^{1/2}$. The best known result in this direction is that due to Soundararajan [7], who shows that

$$N_-(X) \gg_\varepsilon X^{7/8-\varepsilon},$$

2000 Mathematics Subject Classification: primary: 11R29; secondary: 11R11, 11R47.

for any positive ε. In the case of real quadratic fields it was shown by Byeon and Koh [2] how Soundararajan's analysis can be adapted to prove

$$N_+(X) \gg_\varepsilon X^{7/8-\varepsilon}.$$

The purpose of this note is to present a small improvement on these results, as follows.

Theorem. *For large X we have*

$$N_-(X) \gg_\varepsilon X^{9/10-\varepsilon}$$

and

$$N_+(X) \gg_\varepsilon X^{9/10-\varepsilon},$$

for any positive ε.

We should remark that Soundararajan considers more generally imaginary quadratic fields whose class group contains an element of given order g, say, and establishes lower bounds for the corresponding counting function. However the method we describe only appears to improve on his analysis in the case $g = 3$.

For the proof we begin by considering $N_-(X)$, following the argument used by Soundararajan, but improving on it at one key point. As in [7] we will examine

$$N(X) := \#\{d \leqslant X : \mu^2(d) = 1,\, 3|d,\, 3|h(-d)\}$$

and show that $N(X) \gg_\varepsilon X^{9/10-\varepsilon}$. This will immediately yield

$$N_-(X) \gg_\varepsilon X^{9/10-\varepsilon}.$$

Our result for $N_+(X)$ will then be a consequence of that for $N_-(X)$, since the theorem of Scholz [6] yields $3|h(k)$ for any positive integer for which $3|h(-3k)$.

As in [7], let $T \leqslant X^{1/2}/64$ be a parameter to be chosen later, and set $M = T^{2/3}X^{1/3}/2$ and $N = TX^{1/2}/8$. For $d \leqslant X$ let $R(d) = 0$ if d is not square-free, and for square-free d let $R(d)$ be the number of solutions m, n, t of the equation $m^3 = n^2 + t^2 d$, subject to the conditions

$$t \nmid m, \quad M < m \leqslant 2M, \quad N < n \leqslant 2N, \quad T < t \leqslant 2T, \tag{1}$$

$$m \equiv 1 \bmod 18, \quad n \equiv 2 \bmod 18, \quad t \text{ prime}. \tag{2}$$

These conditions are slightly different from those used by Soundararajan. However we note that if T is large enough, then any solution $m^3 = n^2 + t^2 d$ counted by $R(d)$ will have $(m, n) = 1$ and $(t, 6) = 1$, as required by Soundararajan. The second of these conditions is trivial, since t is prime. For the first, we note that if $p|(m, n)$ then $p^2|t^2 d$. Since d is square-free and t is prime, this can only happen if $p = t$, contradicting the assumption that $t \nmid m$. Clearly our conditions imply that $3|d$ whenever $R(d) > 0$, and Soundararajan demonstrates that we also have

$3|h(-d)$ for such d. For the proof of our theorem it will therefore suffice to show that

$$\#\{d : R(d) \neq 0\} \gg_\varepsilon X^{9/10-\varepsilon} \tag{3}$$

for suitable choice of T. In order to establish this we use Cauchy's inequality in the form

$$\Big(\sum_d R(d)\Big)^2 \leqslant \Big(\#\{d : R(d) \neq 0\}\Big)\Big(\sum_d R(d)^2\Big).$$

This yields

$$\#\{d : R(d) \neq 0\} \geqslant \frac{\Big(\sum_d R(d)\Big)^2}{\sum_d R(d)^2}$$

and hence

$$\#\{d : R(d) \neq 0\} \gg \min\{S_1\,,\, S_1^2/S_2\} \tag{4}$$

with

$$S_1 = \sum_d R(d)$$

and

$$S_2 = \sum_d R(d)(R(d)-1).$$

We begin by considering S_1. We have

$$S_1 = \#\{(m,n,t) : t^2|m^3-n^2,\ (m^3-n^2)/t^2 \text{ square-free}\},$$

with m, n, t subject to (1) and (2). A trivial modification of the argument given by Soundararajan [7, §3] shows that the number of triples (m,n,t) satisfying (1) and (2), for which $t^2|m^3-n^2$ and such that $(m^3-n^2)/t^2$ is divisible by p^2 for a prime $p > (\log X)^2$, is $o(MN/(T\log X)) + o(MX^{1/3}T^{2/3})$. For this it suffices to replace the conditions on t in (1) and (2) by the weaker constraint $(t, 6m) = 1$, as used by Soundararajan, and to replace his range $\log X < p \leqslant Z$ in the definition of N_2 by $(\log X)^2 < p \leqslant Z$. If we define

$$S(m,t) = \#\{n : t^2|m^3-n^2\} - \sum_{p \leqslant (\log X)^2} \#\{n : p^2t^2|m^3-n^2\}$$

it follows that

$$S_1 \geqslant \sum_{m,t} S(m,t) + o(MN/(T\log X)), \tag{5}$$

providing that $T \leqslant X^{1/4-\varepsilon}$ for some fixed $\varepsilon > 0$. Here it is understood that m, t, n still satisfy the constraints (1) and (2).

We proceed to estimate $S(m,t)$. Unless m is a quadratic residue of t there will be no corresponding values of n. However if m is a quadratic residue of t the admissible values for n fall into 2 congruence classes modulo $18t^2$. There are

$N/18t^2 + O(1)$ values of $n \in (N, 2N]$ in each such congruence class. We now observe that if $p \leqslant (\log X)^2$ and $(\log X)^2 \leqslant T < t \leqslant 2T$, then $p \neq t$. Moreover (2) shows that if $p^2 | m^3 - n^2$ then $p \geqslant 5$. Thus the solutions n of $p^2t^2 | m^3 - n^2$ lie in at most 4 congruence classes modulo $18p^2t^2$, whence

$$\#\{n : p^2t^2 | m^3 - n^2\} \leqslant \frac{2N}{9p^2t^2} + O(1).$$

It then follows that

$$\begin{aligned} S(m,t) &\geqslant \frac{N}{18t^2} + O(1) - \sum_{5 \leqslant p \leqslant (\log X)^2} \Big(\frac{2N}{9p^2t^2} + O(1) \Big) \\ &\geqslant \frac{N}{18t^2} \Big(1 - 4 \sum_{p \geqslant 5} p^{-2} \Big) + O((\log X)^2) \\ &\gg NT^{-2} \end{aligned}$$

for $T \leqslant X^{1/4}$, since $\sum_{p \geqslant 5} p^{-2} < 1/4$. We insert this bound into (5) and note that t has $\gg M$ quadratic residues $m \in (M, 2M]$, since $M \gg T$. This leads to the bound

$$S_1 \gg \frac{MN}{T \log X} \gg T^{2/3} X^{5/6} (\log X)^{-1}, \tag{6}$$

providing that $T \leqslant X^{1/4-\varepsilon}$ for some fixed $\varepsilon > 0$.

The key to our improvement over the work of Soundararajan is an alternative treatment of S_2. This is at most the number of solutions $(m_1, n_1, t_1) \neq (m_2, n_2, t_2)$ to

$$t_2^2(m_1^3 - n_1^2) = t_1^2(m_2^3 - n_2^2), \quad t_i^2 | m_i^3 - n_i^2, \quad (i = 1, 2), \tag{7}$$

subject to (1) and (2). If $t_1 = t_2$ then

$$n_1^2 - n_2^2 = m_1^3 - m_2^3 \neq 0.$$

Thus each pair m_1, m_2 determines $O_\varepsilon(M^\varepsilon)$ pairs n_1, n_2, for any $\varepsilon > 0$. Since $t_1 = t_2 | m_1^3 - n_1^2$ these values then determine $O_\varepsilon(M^\varepsilon)$ values for t_1, t_2. The contribution to S_2 arising from solutions with $t_1 = t_2$ is therefore

$$\ll_\varepsilon M^{2+2\varepsilon} \ll_\varepsilon T^{4/3} X^{2/3+2\varepsilon}. \tag{8}$$

Henceforth we will confine our attention to the case in which $t_1 \neq t_2$.

We shall count solutions according to the values of t_1, t_2 and $k = t_2 n_1 + t_1 n_2$. It follows from (7) that

$$t_2^2 m_1^3 \equiv k^2 \bmod t_1, \quad t_1^2 m_2^3 \equiv k^2 \bmod t_2,$$

and

$$t_2^2 m_1^3 \equiv t_1^2 m_2^3 \bmod k.$$

Since t_1 and t_2 are distinct primes, the first congruence is equivalent to one of at most 3 conditions

$$m_1 \equiv m_{10} \bmod t_1, \tag{9}$$

say. Similarly the second congruence produces at most 3 conditions

$$m_2 \equiv m_{20} \bmod t_2. \tag{10}$$

To handle the third congruence we work modulo the maximal square-free factor of k, given by

$$v = v(k) = \prod_{p|k} p.$$

We note that $t_1|k$ would imply $t_1|n_1$, since t_1 and t_2 are distinct primes. This would entail $t_1|m_1$ on account of the condition $t_1^2|m_1^3 - n_1^2$. However (1) requires that $t \nmid m$, and we therefore conclude that

$$(t_1, k) = 1, \quad \text{and} \quad (t_2, k) = 1, \tag{11}$$

the second condition being established in a precisely analogous way. Hence if $p|k$ and $p \equiv 2 \bmod 3$, the congruence

$$t_2^2 m_1^3 \equiv t_1^2 m_2^3 \bmod p \tag{12}$$

is equivalent to a linear condition $m_1 \equiv c m_2 \bmod p$, say. On the other hand, if $p \equiv 1 \bmod 3$, then either we must have $p|m_1, m_2$, or (12) is equivalent to 3 linear congruences of the form $m_1 \equiv c m_2 \bmod p$. On combining these conditions for the various primes $p|k$ we see that there is a collection of at most $3^{\omega(v)}$ lattices $\Lambda_i^{(0)} \subseteq \mathbb{Z}^2$ such that any pair m_1, m_2 must satisfy

$$(m_1, m_2) \in \Lambda_i^{(0)} \tag{13}$$

for some i. Moreover we will have $\det(\Lambda_i^{(0)}) = v v_0$, where v_0 is the product of those primes p for which (12) implies $p|m_1, m_2$.

Since t_1, t_2 and v are coprime in pairs, by (11), we may combine the conditions (9), (10) and (13), to deduce that (m_1, m_2) must lie in one of at most $3^{2+\omega(v)}$ lattice cosets of the form $(a_1, a_2) + \Lambda$, where $\det(\Lambda) = t_1 t_2 v v_0$. Here we may choose the coset representative to satisfy $M < a_1, a_2 \leqslant 2M$, for otherwise there can be no relevant pairs (m_1, m_2) satisfying (1). If we now write $(u_1, u_2) = (m_1, m_2) - (a_1, a_2)$ it follows that

$$(u_1, u_2) \in \Lambda, \quad |u_1|, |u_2| \leqslant M.$$

We are now ready to count the number of available pairs (u_1, u_2). For this we use Lemma 1 of Davenport [4], which shows that if an n-dimensional lattice Λ has

successive minima $\lambda_1, \dots, \lambda_n$ then the number of lattice points of norm at most x is

$$\ll \prod_{i=1}^{n} (1 + x/\lambda_i).$$

Moreover we have the standard Minkowski inequalities $\det(\Lambda) \ll \lambda_1 \dots \lambda_n \ll \det(\Lambda)$. Thus, in our case, we find that if the successive minima are $\lambda_1 \leqslant \lambda_2$ then

$$\lambda_1 \ll \sqrt{\det(\Lambda)} \ll \sqrt{t_1 t_2 v v_0} \ll T^2 N \ll T^3 X^{1/2} \ll X^2. \tag{14}$$

Moreover, there are

$$\begin{aligned} &\ll (1 + M/\lambda_1)(1 + M/\lambda_2) \\ &\ll 1 + M^2/\det(\Lambda) + M/\lambda_1 \\ &\ll 1 + M^2/t_1 t_2 v + M/\lambda_1 \end{aligned}$$

possible pairs (m_1, m_2) for each of at most $3^{2+\omega(v)}$ lattices Λ. Since $v \leqslant k \ll TN \ll T^2 X^{1/2} \ll X^2$, we have $3^{2+\omega(v)} \ll_\varepsilon X^\varepsilon$ for any positive ε. Taking into consideration the contribution (8), it therefore follows that

$$S_2 \ll_\varepsilon T^{4/3} X^{2/3+2\varepsilon} + X^\varepsilon \sum_{t_1, t_2, k} \Big(1 + \frac{M^2}{T^2 v} + \frac{M}{\lambda_1}\Big), \tag{15}$$

where for each triple t_1, t_2, k we take the smallest value of λ_1 from all the corresponding lattices Λ. The first term in the sum produces

$$\ll_\varepsilon X^\varepsilon T^3 N \ll_\varepsilon T^4 X^{1/2+\varepsilon}.$$

To handle the second term we use the following result, which will be proved at the end of the paper.

Lemma 1. *For any $k \in \mathbb{N}$ define $v(k) = \prod_{p|k} p$. Then for every $\varepsilon > 0$ we have*

$$\#\{k \leqslant K : v(k) = v\} \ll_\varepsilon K^\varepsilon$$

uniformly in v.

Thus the second term in the sum on the right of (15) contributes

$$\begin{aligned} &\ll_\varepsilon X^\varepsilon M^2 \sum_{v \leqslant 8TN} \frac{1}{v} \#\{k \leqslant 8TN : v(k) = v\} \\ &\ll_\varepsilon X^\varepsilon M^2 (TN)^\varepsilon \sum_{v \leqslant 8TN} \frac{1}{v} \\ &\ll_\varepsilon T^{4/3} X^{2/3+3\varepsilon}. \end{aligned}$$

Thus

$$S_2 \ll_\varepsilon T^{4/3}X^{2/3+3\varepsilon} + T^4X^{1/2+\varepsilon} + X^\varepsilon \sum_{t_1,t_2,k} \frac{M}{\lambda_1}. \tag{16}$$

It remains to handle the contribution from the term M/λ_1. Let (μ_1, μ_2) be the shortest non-zero vector in the lattice Λ, so that λ_1 is the length of (μ_1, μ_2). We shall consider the set of triples (t_1, t_2, k) for which a given vector (μ_1, μ_2) can arise. Thus the contribution to S_2 is

$$\ll_\varepsilon X^\varepsilon M \sum_{\mu_1,\mu_2} \frac{\#\{t_1, t_2, v\}}{\sqrt{|\mu_1|^2 + |\mu_2|^2}}.$$

In view of (14) we will have $\mu_1, \mu_2 \ll X^2$. Moreover, according to the construction of the lattice Λ we must have $v_0|\mu_1, \mu_2$, whence $v_0 \leqslant \text{h.c.f.}(\mu_1, \mu_2)$. The inequalities

$$\lambda_1 \ll \sqrt{\det(\Lambda)} \ll \sqrt{t_1t_2vv_0} \ll T^{3/2}N^{1/2}\sqrt{v_0} \ll T^2X^{1/4}\sqrt{v_0}$$

therefore imply that

$$\mu_1, \mu_2 \ll T^2X^{1/4}\sqrt{\text{h.c.f.}(\mu_1, \mu_2)}.$$

Since $(\mu_1, \mu_2) \in \Lambda$, we see from the way that the lattice Λ was constructed using (9), (10) and (12), that $t_1|\mu_1$, $t_2|\mu_2$ and $v|t_2^2\mu_1^3 - t_1^2\mu_2^3$. If μ_1 and μ_2 are both non-zero they determine $O_\varepsilon(X^\varepsilon)$ possible prime divisors t_1, t_2. Since t_1 and t_2 are distinct, the number $t_2^2\mu_1^3 - t_1^2\mu_2^3$ is non-zero and hence has $O_\varepsilon(X^\varepsilon)$ possible divisors v. This produces a contribution

$$\ll_\varepsilon X^{3\varepsilon} M \sum_{\mu_1,\mu_2} \frac{1}{\sqrt{|\mu_1|^2 + |\mu_2|^2}}$$

to S_2. We shall consider terms in the dyadic range

$$B < \sqrt{|\mu_1|^2 + |\mu_2|^2} \leqslant 2B,$$

for which we count pairs μ_1, μ_2 according to the value of $h = \text{h.c.f.}(\mu_1, \mu_2)$. Thus each dyadic range produces

$$\begin{aligned}
&\ll_\varepsilon X^{3\varepsilon}MB^{-1} \sum_{h\leqslant B} \#\{\mu_1, \mu_2 \ll \min(B\,, T^2X^{1/4}h^{1/2}) : h|\mu_1, \mu_2\} \\
&\ll_\varepsilon X^{3\varepsilon}MB^{-1} \sum_{h\leqslant B} \Big(\frac{\min(B\,, T^2X^{1/4}h^{1/2})}{h}\Big)^2 \\
&\ll_\varepsilon X^{3\varepsilon}MB^{-1} \min(B^2\,, T^4X^{1/2}\log 2B).
\end{aligned}$$

Summing for values of B running over powers of 2 yields a total

$$\ll_\varepsilon MT^2X^{1/4+4\varepsilon} \ll_\varepsilon T^{8/3}X^{7/12+4\varepsilon}.$$

On the other hand, if μ_1 vanishes, for example, there are $O(T)$ choices for t_1 and $O_\varepsilon(X^{2\varepsilon})$ possible values for t_2 and v. This leads to a contribution

$$\ll_\varepsilon X^{3\varepsilon}MT \sum_{\mu_2 \ll X^2} |\mu_2|^{-1} \ll_\varepsilon X^{4\varepsilon}MT \ll_\varepsilon T^{5/3}X^{1/3+4\varepsilon}.$$

On comparing these bounds with (16) we see that

$$S_2 \ll_\varepsilon T^{4/3}X^{2/3+3\varepsilon} + T^4X^{1/2+\varepsilon} + T^{8/3}X^{7/12+4\varepsilon} + T^{5/3}X^{1/3+4\varepsilon}.$$

Clearly the fourth term is redundant, being dominated by the third term.

Finally, inserting this last bound into (4), and using (6), we find that

$$\#\{d : R(d) \neq 0\} \gg X^{-5\varepsilon} \min\{T^{2/3}X^{5/6}\,,\, X\,,\, T^{-8/3}X^{7/6}\,,\, T^{-4/3}X^{13/12}\}.$$

The optimal choice for T is thus $T = X^{1/10}$, which matches the first and third terms in the minimum, and leads to the lower bound $X^{9/10-5\varepsilon}$. This establishes the required bound (3), on re-defining ε.

It remains to prove Lemma 1. Since $v(k) \leqslant v$ we can clearly suppose that $v \leqslant K$. Then, for any $\eta > 0$ we have

$$\#\{k \leqslant K : v(k) = v\} \leqslant \sum_{\substack{k=1 \\ v(k)=v}}^{\infty} (\frac{K}{k})^\eta \leqslant K^\eta \prod_{p|v} \Big(\sum_{e=0}^{\infty} p^{-e\eta} \Big).$$

However

$$\sum_{e=0}^{\infty} p^{-e\eta} \leqslant \sum_{e=0}^{\infty} 2^{-e\eta} = A(\eta),$$

say, whence

$$\#\{k \leqslant K : v(k) = v\} \leqslant K^\eta A(\eta)^{\omega(v)}.$$

Since $\omega(v) = O((\log 3v)/(\log\log 3v))$ and $v \leqslant K$ we deduce that

$$\#\{k \leqslant K : v(k) = v\} \ll_\eta K^{2\eta}$$

and the result follows, on taking $\eta = \varepsilon/2$.

References

[1] N.C. Ankeny and S. Chowla, On the divisibility of the class number of quadratic fields, *Pacific J. Math.,* 5 (1955), 321–324.

[2] D. Byeon and E. Koh, Real quadratic fields with class number divisible by 3, *Manuscripta Math.,* 111 (2003), 261–263.

[3] H. Cohen and H.W. Lenstra, Jr, Heuristics on class groups of number fields, *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983),* 33–62, (Lecture Notes in Math., 1068, Springer, Berlin, 1984).
[4] H. Davenport, Indefinite quadratic forms in many variables. II, *Proc. London Math. Soc. (3),* 8 (1958), 109–126.
[5] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields. II, *Proc. Roy. Soc. London Ser. A,* 322 (1971), 405–420.
[6] A. Scholz, Über die Beziehung der Klassenzahlen quadratischer Körper zueinander, *J. reine angew. Math.,* 166 (1932), 201–203.
[7] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, *J. London Math. Soc.,* 61 (2000), 681–690.

Address: Mathematical Institute, 24–29, St. Giles', Oxford, OX1 3LB, UK
E-mail: rhb@maths.ox.ac.uk
Received: 14 November 2006; **revised:** 9 January 2007