http://dx.doi.org/10.1090/conm/210/02785

Contemporary Mathematics
Volume 210, 1998

THE ABC CONJECTURE AND EXPONENTS OF CLASS GROUPS OF QUADRATIC FIELDS

M. Ram Murty[1]

1. Introduction.

Jayadeva, in a commentary of the 11th century, describes a method he calls *cakravāla* (from the Sanskrit word *cakra* which means 'wheel') to determine all solutions of the equation

$$x^2 - dy^2 = m \tag{1}$$

with $d > 0$. (He however does not prove that he has all of the solutions.) This equation, usually called Pell's equation, had been studied much earlier by several Indian mathematicians. In the work of Brahmagupta, dating back to the 7th century, we find a whole section devoted to such equations. His 'bhavana' (meaning production in Sanskrit) rules gave an algorithm for producing many solutions. Later in the 12th century, Bhaskara had given an algorithm for finding all solutions and it was believed, until the work of Jayadeva, that Bhaskara's work was the oldest detailed treatment of such equations. See Weil [W, p. 17-24] for an illuminating discussion on this matter.

Not to upset tradition, we will continue to refer to (1) as Pell's equation. We shall use the 'bhavana' and 'cakravala' methods to study exponents of ideal class groups of real quadratic fields. The corresponding results for imaginary quadratic fields are also established and are much stronger.

To be precise, the problem we wish to investigate in this paper concerns quadratic extensions of the rational number field. Given a natural number g, we wish to count the number of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ with $0 < d < x$ whose order of the class group is divisible by g. We investigate the identical question for real quadratic fields.

There have been many papers written showing that the number of such fields is infinite. First, if g is a power of 2, then genus theory gives a very precise answer. The number of such fields with absolute value of the discriminant less than x is asymptotic to cx for some constant c which of course depends on the power of 2.

When $g = 3$, Davenport and Heilbronn [DH] have obtained precise results. If $r_3(d)$ denotes the rank of the 3-part of the ideal class group of $\mathbb{Q}(\sqrt{-d})$, they proved

$$\sum_{d<x} 3^{r_3(d)} \sim 2x.$$

If $R_3(d)$ is the 3-rank of the class group of $\mathbb{Q}(\sqrt{d})$ they showed

$$\sum_{d<x} 3^{R_3(d)} \sim \frac{4}{3}x.$$

[1] *Research partially supported by NSERC, FCAR and CICMA.*

© 1998 American Mathematical Society

Licensed to Queen's Univ. Prepared on Wed Nov 30 14:41:16 EST 2016for download from IP 130.15.100.65.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/publications/ebooks/terms

It is not clear if one can deduce that a positive proportion of such fields have class number divisible by 3.

It is however, possible to deduce some quantitative estimate from a related result of Davenport and Heilbronn [DH]. Indeed, they show that the number of cubic fields of positive discriminant less than x is asymptotically $1/12\zeta(3)$. By class field theory, the class number of $\mathbb{Q}(\sqrt{d})$ is divisible by 3 if and only if there exists a cubic field of discriminant d. It is now immediate that the number of real quadratic fields whose discriminant is $< x$ and whose class number is divisible by 3 is $\gg x^{1/3-\epsilon}$. An identical result can be deduced in the imaginary quadratic case.

Many authors, such as Nagell [Na], Humbert [Hu], Ankeny and Chowla [AC] and Kuroda [K], have shown that for a given number g, there are infinitely many imaginary quadratic fields whose class number is divisible by g. For real quadratic fields, infinitude has been shown by Yamamoto [Y] and Weinberger [We] independently.

In either the imaginary quadratic or the real quadratic case, nothing quantitative is known, for $g \geq 5$. Cohen and Lenstra [CL] formulated the following conjecture when $g = p$ is a prime. In the imaginary quadratic case, they conjecture that the probability p divides the class number is

$$1 - \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^i}\right).$$

In the real quadratic case, they conjecture

$$1 - \prod_{i=2}^{\infty} \left(1 - \frac{1}{p^i}\right)$$

as the probability that p divides the class number.

Assuming the ABC conjecture, we will prove that the number of imaginary quadratic fields whose disriminant is $< x$ with exponent of the class group divisible by g is $\gg x^{\frac{1}{g}-\epsilon}$. In the real quadratic case, we obtain $\gg x^{\frac{1}{2g}-\epsilon}$. These we state as:

Theorem 13. *Let $g \geq 3$ be odd and assume the ABC conjecture. The number of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ with $0 < d < x$ and whose class group has exponent divisible by g is $\gg x^{\frac{1}{g}-\epsilon}$ for any $\epsilon > 0$. (Here the implied constant will depend on ϵ.)*

Theorem 14. *Let $g \geq 3$ be odd and assume the ABC conjecture. The number of real quadratic fields $\mathbb{Q}(\sqrt{d})$ with $0 < d < x$ and whose class group has exponent divisible by g is $\gg x^{1/2g-\epsilon}$ for any $\epsilon > 0$.*

We also deduce in the last section an interesting result about exponents of the class group of certain real quadratic fields.

2. The imaginary quadratic case.

We begin with the following theorem.

Licensed to Queen's Univ. Prepared on Wed Nov 30 14:41:16 EST 2016for download from IP 130.15.100.65.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/publications/ebooks/terms

Theorem 1. *Suppose that $n^g - 1 = d$ is squarefree with n odd and ≥ 5. Then the class group of $\mathbb{Q}(\sqrt{-d})$ has an element of order g.*

Proof. We have the ideal factorization in $\mathbb{Q}(\sqrt{-d})$:

$$(n)^g = (1+\sqrt{-d})(1-\sqrt{-d}).$$

Since n is odd, the ideals $(1+\sqrt{-d})$ and $(1-\sqrt{-d})$ are coprime. Thus, they must each be the g-th power of an ideal. Therefore,

$$\mathfrak{A}^g = (1+\sqrt{-d}) \quad \text{and} \quad (\mathfrak{A}')^g = (1-\sqrt{-d})$$

where $\mathfrak{A}$ and $\mathfrak{A}'$ are coprime and $\mathbb{N}\mathfrak{A} = n$. If for some $m \leq g-1$, we have that $\mathfrak{A}^m$ is principal, then for some $u, v \in \mathbb{Z}$,

$$\mathfrak{A}^m = (u+v\sqrt{-d}) \quad \text{or} \quad (\frac{u+v\sqrt{-d}}{2})$$

depending on whether $-d \equiv 2,3 \pmod 4$ or $-d \equiv 1 (\bmod 4)$ respectively. We must have $v \neq 0$ for otherwise $\mathfrak{A}$ and $\mathfrak{A}'$ would have a common factor. Thus, taking norms of the above equation, we find in case $-d \equiv 2,3 (\bmod 4)$:

$$n^{g-1} \geq n^m = u^2 + dv^2 \geq d = n^g - 1$$

so that $1 \geq n^{g-1}(n-1) \geq 4 \cdot 5^{g-1}$, a contradiction. In the case $-d \equiv 1 (\bmod 4)$, we find:

$$n^{g-1} \geq n^m \geq \frac{u^2+dv^2}{4} \geq \frac{d}{4} = \frac{n^g-1}{4}$$

so that $1 \geq n^{g-1}(n-4) \geq 5^{g-1}$, a contradiction. This completes the proof of the theorem.

Theorem 2. *Let $g > 2$. Suppose that $n^g - 1 = p^2 d$, with d squarefree, n odd and ≥ 5. If $p < n^{g/4}/2\sqrt{2}$, then the class group of $\mathbb{Q}(\sqrt{-d})$ has an element of order g.*

Proof. We proceed as before:

$$(n)^g = (1+p\sqrt{-d})(1-p\sqrt{-d}).$$

Since n is odd, $(1+p\sqrt{-d})$ and $(1-p\sqrt{-d})$ are coprime. Thus, they must each be the g-th power of an ideal. Therefore,

$$\mathfrak{A}^g = (1+p\sqrt{-d}) \quad \text{and} \quad (\mathfrak{A}')^g = (1-p\sqrt{-d})$$

where $\mathfrak{A}$ and $\mathfrak{A}'$ are coprime with $\mathbb{N}\mathfrak{A} = \mathbb{N}\mathfrak{A}' = n$. Thus, the order of the ideal class of $\mathfrak{A}$ divides g. Suppose $\mathfrak{A}^m$ is principal for some $m \leq g/2$. Then, as before

$$\mathfrak{A}^m = (u+v\sqrt{-d}) \quad \text{or} \quad (\frac{u+v\sqrt{-d}}{2})$$

Licensed to Queen's Univ. Prepared on Wed Nov 30 14:41:16 EST 2016for download from IP 130.15.100.65.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/publications/ebooks/terms

according as the residue class d belongs to mod 4. Thus, as before,

$$n^{g/2} \geq n^m = \frac{u^2 + dv^2}{4} \geq \frac{d}{4} = \frac{n^g - 1}{4p^2} \geq \frac{n^g}{8p^2}$$

so that $p \geq n^{g/4}/2\sqrt{2}$ contrary to hypothesis. This completes the proof.

3. The real quadratic case.

We begin by reviewing some classical material about continued fractions.

Lemma 3. *If N and d are integers with $d > 0$ and $|N| < \sqrt{d}$ and d is not a square, then all positive solutions of the Pell's equation*

$$x^2 - dy^2 = N$$

are such that x/y is a convergent of $\sqrt{d}$.

Proof. See LeVeque [L, p. 181, Theorem 9-8].

We apply this as follows:

Lemma 4. *The continued fraction of $\sqrt{d}$ with $d = a^2 + 1$ is*

$$[a, 2a, 2a, \ldots].$$

Moreover, if $|u^2 - dv^2| \neq 0$ or 1, then

$$|u^2 - dv^2| > \sqrt{d}.$$

Proof. We find from the continued fraction algorithm that the convergents p_k/q_k always satisfy

$$p_k^2 - dq_k^2 = \pm 1$$

so that the result easily follows from Lemma 3.

Theorem 5. *Suppose that n is odd, $n \geq 5$ and $n^{2g} + 1 = d$ is squarefree. Then the class group of $\mathbb{Q}(\sqrt{d})$ has an element of order g.*

Remark. This theorem is essentially due to Ankeny and Chowla [AC]. Since they did not supply a complete proof, we do so here. This will have its use since we will also need to modify their result later on.

Proof. As before,

$$(n)^{2g} = (-1 + \sqrt{d})(1 + \sqrt{d}).$$

Since n is odd, each of the ideals $(-1 + \sqrt{d})$ and $(1 + \sqrt{d})$ must be coprime. Hence

$$\mathfrak{A}^{2g} = (-1 + \sqrt{d}) \quad \text{and} \quad (\mathfrak{A}')^{2g} = (1 + \sqrt{d}).$$

Licensed to Queen's Univ. Prepared on Wed Nov 30 14:41:16 EST 2016for download from IP 130.15.100.65.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/publications/ebooks/terms

If $\mathfrak{A}^m = (u + v\sqrt{d})$ or $(\frac{u+v\sqrt{d}}{2})$ according as $d \equiv 2, 3 \pmod 4$ or $d \equiv 1 \pmod 4$, then

$$n^m = |u^2 - dv^2| \quad \text{or} \quad |\frac{u^2 - dv^2}{4}|.$$

In either case, we deduce from Lemma 4 that

$$n^m \geq |\frac{u^2 - dv^2}{4}| \geq \frac{n^g}{4}.$$

If $m \leq g - 1$, we deduce $n \leq 4$, a contradiction. Therefore, $\mathfrak{A}$ has order $\geq g$. Since $\mathfrak{A}^{2g}$ is principal, $\mathfrak{A}$ has order g or $2g$. In either case, the class group has an element of order divisible by g.

We modify Theorem 5 in the following way:

Theorem 6. *Let g be odd and ≥ 5. Suppose that n is odd, $n \geq 5$ and $n^{2g} + 1 = p^2 d$ with $1 < d$ squarefree, p satisfying $p < n^{3/2}/2$. Then the class group of $\mathbb{Q}(\sqrt{d})$ has an element of order g.*

Proof. We proceed as before to find that $(-1 + p\sqrt{d})$ and $(1 + p\sqrt{d})$ must be $2g$-th powers of coprime ideals (since n is odd). Thus,

$$\mathfrak{A}^{2g} = (-1 + p\sqrt{d})$$

and if

$$\mathfrak{A}^m = (u + v\sqrt{d}) \quad \text{or} \quad (\frac{u + v\sqrt{d}}{2})$$

with $m \leq g - 3$ we find by Lemma 4 that

$$n^{g-3} \geq n^m \geq |\frac{u^2 - dv^2}{4}| > |\frac{(pu)^2 - p^2 dv^2}{4p^2}| > \frac{n^g}{4p^2}$$

so that $2p > n^{3/2}$, contrary to hypothesis. Thus, if $\mathfrak{A}^m$ is principal, then $m \geq g - 1$ and must divide $2g$, since g is odd. Thus, $m = g$ or $2g$ and in either case, we are done.

4. Application of the ABC conjecture.

One can use the ABC conjecture to determine if any large prime factors divide $n^g - 1$. Recall that the ABC conjecture states that if

$$A + B = C$$

and A, B, C are three integers mutually coprime, then

$$\max(|A|, |B|, |C|) \ll \prod_{p|ABC} p^{1+\epsilon}$$

for any $\epsilon > 0$ and the implied constant depends on ϵ. Now let $0 < \delta < g$. Thus, if $p^2 | n^g - 1$ and $p > n^{1+\delta}$, then considering the ABC equation $1 + (n^g - 1) = n^g$, the ABC conjecture implies

$$n^g \ll n^{(1+\epsilon)(g-\delta)}.$$

Licensed to Queen's Univ. Prepared on Wed Nov 30 14:41:16 EST 2016for download from IP 130.15.100.65.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/publications/ebooks/terms

If we choose $\epsilon = \delta/(g-\delta)$, this is a contradiction for n sufficiently large. We conclude that if $p^2|n^g - 1$ then $p < n^{1+\delta}$. This we state as:

Proposition 7. *Let $0 < \delta < g$ and assume the ABC conjecture. If p is prime and $p^2|n^g - 1$, then $p < n^{1+\delta}$ for all n sufficiently large.*

We can state a similar result for $n^{2g} + 1$. Assuming the ABC conjecture, Granville [G] has recently established that for any polynomial f, the number of $n < x$ such that a given polynomial $f(n)$ is squarefree is asymptotically $c_f x$ for some constant c_f. In out context, we need such a result for the polynomial $f(n) = n^g - 1$ and n odd. One can modify the method of Granville to yield such a result and from it deduce Theorems 13, with exponent $1/g$ and Theorem 14 with exponent $1/2g$. Granville's application of the ABC invokes the deep theorem of Belyi. For the sake of independent interest, we will adopt here a slightly different route. We begin by stating the analog of Proposition 7 tailored to be applied in the real quadratic case.

Proposition 8. *Let $0 < \delta < 2g$ and assume the ABC conjecture. If p is prime and $p^2|n^{2g} + 1$, then $p < n^{1+\delta}$.*

We record, for later calculation, the following corollaries:

Corollary 9. *Let $0 < \delta < g$ and assume the ABC conjecture. Then the number of $n \leq x$ such that there is a prime $p > n^{1+\delta}$ and $p^2|(n^g - 1)$ is bounded.*

Corollary 10. *Let $0 < \delta < 2g$ and assume the ABC conjecture. Then, the number of $n \leq x$ such that there is a prime $p > n^{1+\delta}$ and $p^2|(n^{2g} + 1)$ is bounded.*

5. The simple asymptotic sieve.

We now proceed as in Hooley [H]. We use the identity

$$\sum_{d^2|n} \mu(d) = \begin{cases} 1 & \text{if } n \text{ is squarefree} \\ 0 & \text{otherwise.} \end{cases}$$

Let $0 < \delta < g$. We will write $n \sim x$ to mean that there exist positive constants a and b so that $ax < n < bx$. Let $N(x)$ be the number of $n \sim x$ such that $f(n) = n^g - 1$ is squarefree or has a prime divisor p satisfying $n < p < n^{1+\delta}$. Let P_z be the product of the primes $\leq z$. Clearly, if $z = c \log x$ for sufficiently small c, then

$$N(x) \leq N(x, z)$$

where

$$N(x,z) = \sum_{n \sim x} \sum_{d^2|(f(n), P_z^2)} \mu(d).$$

By Corollary 9, the number of $n \leq x$ such that there is a prime $p > n^{1+\delta}$ and $p^2|(n^g - 1)$ is bounded. Hence,

$$N(x) \geq N(x,z) - \sum_{z<p<x^{1+\delta}} N_p(x) + O(1)$$

Licensed to Queen's Univ. Prepared on Wed Nov 30 14:41:16 EST 2016for download from IP 130.15.100.65.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/publications/ebooks/terms

where $N_p(x)$ is the number of $n \sim x$ such that $p^2|f(n)$. We will choose z sufficiently small so that the error terms are controlled. Indeed,

$$N(x,z) = \sum_{d|P_z} \mu(d) N_d(x)$$

where $N_d(x)$ is the number of $n \sim x$ such that $d^2|f(n)$. Letting $\rho(p^2)$ be the number of solutions of the congruence $f(m) \equiv 0(\bmod p^2)$, we find that choosing $z = \frac{1}{2\log 2g}\log x$ gives

$$N(x,z) = x\prod_{p<z}\left(1-\frac{\rho(p^2)}{p^2}\right) + O(x^{1/2}).$$

Now,

$$\sum_{z<p<x} N_p(x) \ll \frac{x}{\log x}$$

since $\rho(p^2) \le g$ for p coprime to g by a simple calculation via Hensel's lemma. This leads to:

Theorem 11. *Let g be odd, $0 < \delta < g$ and assume the ABC conjecture. Let $\tilde{N}(x)$ be the number of odd $n \sim x$ such that $f(n) = n^g - 1$ is either squarefree or has a prime divisor p satisfying $p^2|(n^g-1)$ with $n < p < n^{1+\delta}$. Then*

$$\tilde{N}(x) = \frac{x}{4}\prod_{p>2}\left(1-\frac{\rho(p^2)}{p^2}\right) + O\left(\frac{x(\log\log x)^{g-1}}{\log x}\right).$$

Proof. We begin by observing that by an argument similar to the above, the number of *even* $n \sim x$ such that $n^g - 1$ has no squared prime factor $p < x$ is

$$= \frac{x}{2}\prod_{2<p<z}\left(1-\frac{\rho(p^2)}{p^2}\right) + O\left(\frac{x}{\log x}\right).$$

Since g is odd, $\rho(4) = 1$ so that

$$N(x) = \frac{3}{4}x\prod_{2<p<z}\left(1-\frac{\rho(p^2)}{p^2}\right) + O\left(\frac{x}{\log x}\right).$$

Thus,

$$\tilde{N}(x) = \frac{1}{4}x\prod_{2<p<z}\left(1-\frac{\rho(p^2)}{p^2}\right) + O\left(\frac{x}{\log x}\right).$$

In the above calculation, it remains to estimate

$$\prod_{p}\left(1-\frac{\rho(p^2)}{p^2}\right) - \prod_{p<z}\left(1-\frac{\rho(p^2)}{p^2}\right) \ll \sum_{d>z}\frac{g^{\nu}(d)}{d^2},$$

Licensed to Queen's Univ. Prepared on Wed Nov 30 14:41:16 EST 2016for download from IP 130.15.100.65.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/publications/ebooks/terms

where $\nu(d)$ denotes the number of distinct prime factors of d. Since

$$\sum_{n\leq x} g^{\nu(d)} \ll x(\log x)^{g-1}$$

we have by partial summation

$$\sum_{d>z} \frac{g^{\nu(d)}}{d^2} \ll \int_z^\infty \frac{(\log t)^{g-1}dt}{t^2} \ll \frac{(\log z)^{g-1}}{z}$$

which completes the proof since $z = \frac{1}{2\log 2g}\log x$.

In an identical manner, we prove

Theorem 12. *Let $0 < \delta < 2g$. Assume the ABC conjecture. Let $N_1(x)$ be the number of $n \sim x$ such that $f(n) = n^{2g} + 1$ is either squarefree or has $p^2|(n^{2g}+1)$ with $n < p < n^{1+\delta}$. Then,*

$$N_1(x) = x\prod_p \Big(1 - \frac{\rho(p^2)}{p^2}\Big) + O(\frac{x(\log\log x)^{2g-1}}{\log x})$$

where $\rho(p^2)$ is the number of solutions of the congruence $n^{2g} + 1 \equiv 0(\bmod p^2)$.

6. The main theorems.

We can now prove:

Theorem 13. *Let $g \geq 3$ be odd and assume the ABC conjecture. The number of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ with $0 < d < x$ whose class group has an element of order g is $\gg x^{1/g-\epsilon}$ for any $\epsilon > 0$.*

Proof. Let $x^{1/g}/2 \leq n \leq x^{1/g}$ and $0 < \delta < g$. The number of n in this range, for which $n^g - 1$ is either squarefree or has a prime divisor satisfying $p^2|n^g - 1$ and $n < p < n^{1+\delta}$ is by Theorem 11 equal to

$$c_1 x^{1/g} + O(\frac{x^{1/g}(\log\log x)^{g-1}}{\log x})$$

where

$$c_1 = \prod_p \Big(1 - \frac{\rho(p^2)}{p^2}\Big).$$

Observe that if p is coprime to g, then $\rho(p^2) \leq g$ (by a simple application of Hensel's lemma) so that each factor in the above product for $p > \sqrt{g}$ is non-zero. However the congruence $n^g \equiv 1(\bmod p)$ has $(g, p-1)$ solutions and these lift to $(g, p-1)$ solutions mod p^2 if p is coprime to g. If $p|g$ the number of solutions is $(g, p(p-1))$ which is clearly less than p^2 and hence $c_1 \neq 0$. We now assert that for each n enumerated by $\tilde{N}(x^{1/g})$ in Theorem 11, either $n^g - 1$ is squarefree or $n^g - 1 = p^2 d$ where d is squarefree and p is a prime satisfying $n < p < n^{1+\delta}$. Indeed, if $n^g - 1$

Licensed to Queen's Univ. Prepared on Wed Nov 30 14:41:16 EST 2016for download from IP 130.15.100.65.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/publications/ebooks/terms

has two prime factors p_1 and p_2 satisfying $n < p_1 < n^{1+\delta}$, $n < p_2 < n^{1+\delta}$ and $p_1^2 p_2^2 | n^g - 1$, then by the ABC conjecture,

$$n^g \ll \left(\frac{n^{g+1}}{p_1 p_2}\right)^{1+\epsilon}$$

which implies

$$n^{2+2\epsilon} < (p_1 p_2)^{1+\epsilon} \ll n^{1+\epsilon(g+1)}.$$

Thus, the number of such n's is bounded. Therefore, the n's enumerated by $\tilde{N}(x^{1/g})$ can be put into one of two sets S_1 or S_2 (say) according as $n^g - 1$ is squarefree or $n^g - 1 = p^2 d$ with d squarefree and p a prime satisfying $n < p < n^{1+\delta}$. Since $\tilde{N}(x^{1/g}) \gg x^{1/g}$, the size of at least one of these sets is $\gg x^{1/g}$. If S_1 has size $\gg x^{1/g}$ then we are done by Theorem 1. If S_2 has size $\gg x^{1/g}$, then for each $n \in S_2$, $n^g - 1 = p^2 d$. We enumerate the number of distinct d's that can arise. Since $(n-1)|(n^g - 1)$ and $p > n$, we deduce $(n-1)|d$. Hence any given d can be repeated at most $O(d^\epsilon)$ times. Thus, the number of distinct quadratic fields arising from S_2 is $\gg x^{1/g-\epsilon}$. The result now follows from Theorems 1 and 2.

In an identical fashion, we derive:

Theorem 14. *Let $g \geq 3$ be odd and assume the ABC conjecture. The number of real quadratic fields $\mathbb{Q}(\sqrt{d})$ $0 < d < x$ whose class group has an element of order g is $\gg x^{1/2g-\epsilon}$ for any $\epsilon > 0$.*

Proof. We proceed as in the proof of Theorem 13 with $x > (4g)^g$. The corresponding set S_1 enumerting $n^{2g} + 1$ squarefree presents no problem. We must deal with S_2. Since g is odd, $(n^2+1)|(n^{2g}+1)$. For $n \in S_2$, $n^{2g}+1 = p^2 d$ with d squarefree. If $p|(n^2+1)$ and $p|(\frac{n^{2g}+1}{n^2+1})$, then p divides the discriminant of $n^{2g}+1$. This means $p|2g$, which is a contradiction since $p > n > 2g$. Therefore, either $p^2|(n^2+1)$ or $p^2|(\frac{n^{2g}+1}{n^2+1})$. The former case leads to $p \leq n$, which is a contradiction. Thus, $(n^2+1)|d$. Now the argument continues as before. Any given d can be repeated at most $O(d^\epsilon)$ times in the enumeration of S_2. This completes the proof.

7. Exponents of class groups of certain real quadratic fields.

Lemma 4 allows us to derive a result on exponents of class groups of quadratic fields. In the imaginary quadratic case, Boyd and Kisilevsky [BK] proved assuming the generalised Riemann hypothesis (GRH) that the exponent of the class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$, $d > 0$ satisfies

$$\gg \frac{\log d}{\log \log d}.$$

One cannot, of course, expect such a result to hold in the real quadratic case since extensive numerical calculations suggest that there are infinitely many real quadratic fields of class number 1. However, the real quadratic fields $\mathbb{Q}(\sqrt{a^2+1})$ have large class groups and the identical analogue of the theorem of [BK] seems to be:

Licensed to Queen's Univ. Prepared on Wed Nov 30 14:41:16 EST 2016for download from IP 130.15.100.65.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/publications/ebooks/terms

Theorem 15. *Suppose a^2+1 is squarefree and let $e(a)$ be the exponent of the class group of $\mathbb{Q}(\sqrt{a^2+1})$. Then, assuming GRH,*

$$e(a) \gg \frac{\log a}{\log\log a}.$$

Proof. Let d be the discriminant of $k = \mathbb{Q}(\sqrt{a^2+1})$. By the Chebotarev density theorem and the GRH (see [MMS]) we know there is always a prime ideal $\mathfrak{p}$ satisfying

$$N_{k/\mathbb{Q}}(\mathfrak{p}) \leq (\log d)^2$$

in any given ideal class. Let $\mathfrak{p}$ be non-principal with exponent $e(a)$. Then $\mathfrak{p}^{e(a)}$ is principal:

$$\mathfrak{p}^{e(a)} = (u + v\sqrt{d})$$

(say). Then, taking norms, and applying Lemma 4, we deduce

$$e(a)\log\log d \gg \log d.$$

Since $d = a^2+1$ or $4(a^2+1)$, the result is now immediate.

REFERENCES

[AC] N. Ankeny and S. Chowla, On the divisibility of the class number of quadratic fields, Pacific Journal of Math., 5 (1955) p. 321 - 324.

[BK] D. Boyd and H. Kisilevsky, On the exponent of the ideal class groups of complex quadratic fields, Proc. Amer. Math. Soc., 31 (1972) 433 - 436.

[CL] H. Cohen and H.W. Lenstra Jr., Heuristics on class groups of number fields, Springer Lecture Notes, 1068, in Number Theory Noordwijkerhout 1983 Proceedings.

[DH] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, Proc. Royal Soc. , A 322 (1971) p. 405 - 420.

[G] A. Granville, ABC allows us to count squarefrees, preprint.

[H] C. Hooley, Applications of sieve methods, Cambridge Tracts in Mathematics, 1976.

[Hu] P. Humbert, Sur les nombres de classes de certains corps quadratiques, *Comment. Math. Helv.* **12** (1939/40) 233-245; also **13** (1940/41) 67.

[K] S. Kuroda, On the class number of imaginary quadratic fields, *Proc. Japan Acad.*, **40** (1964) 365-367.

[L] W. LeVeque, Topics in Number Theory, Vol. 1, Addison-Wesley, Reading. Mass., 1956.

[Na] T. Nagell, Uber die klassenzahl imaginar-quadratischer Zahlkorper, *Abh. Math. Sem. Univ. Hamburg* **1** (1922) 140 - 150.

[MMS] M. Ram Murty, V. Kumar Murty and N. Saradha, Modular forms and the Chebotarev density theorem, *American Journal of Mathematics*, **110** (1988) 253-281.

Licensed to Queen's Univ. Prepared on Wed Nov 30 14:41:16 EST 2016for download from IP 130.15.100.65.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/publications/ebooks/terms

[Y] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.*, **7** (1970) 57-76.

[W] A. Weil, Number Theory, An approach through history, From Hammurapi to Legendre, Birkhäuser, Boston, Basel, Stuttgart, 1984.

[We] P. Weinberger, Real Quadratic Fields with Class Number Divisible by n, *Journal of Number Theory*, **5** (1973) 237-241.

Department of Mathematics,
Queen's University,
Kingston, Ontario
K7L 3N6, Canada
murty@mast.queensu.ca

Licensed to Queen's Univ. Prepared on Wed Nov 30 14:41:16 EST 2016for download from IP 130.15.100.65.
License or copyright restrictions may apply to redistribution; see http://www.ams.org/publications/ebooks/terms