QUADRATIC FIELDS WITH CYCLIC 2-CLASS GROUPS

CARLOS DOMINGUEZ, STEVEN J. MILLER, AND SIMAN WONG

ABSTRACT. For any integer $k \geq 1$, we show that there are infinitely many complex quadratic fields whose 2-class groups are cyclic of order 2^k. The proof combines the circle method with an algebraic criterion for a complex quadratic ideal class to be a square.

In memory of David Hayes.

1. INTRODUCTION

The genus theory of Gauss completely determines the elementary 2-subgroup of the class group of a complex quadratic field. In particular, we can construct complex quadratic class groups with prescribed elementary 2-subgroups. Using class field theory, Rédei [10] gave the first algorithm for determining the complete structure of the Sylow 2-subgroup of a quadratic class group. Now, genus theory readily yields an explicit criterion for a divisor class in a quadratic class group to be a square, cf. section 2 below. This leads to a new, simplified recursive algorithm (Shanks [12] used the language of quadratic forms; others ([2], [3], [14], [5]) worked with ideals). Unlike genus theory, however, neither the Rédei algorithm nor the recursive one imply the existence of quadratic fields with prescribed 2-class groups. For example, Hajir points out that we do not know if there are quadratic fields with arbitrarily large *cyclic* 2-class groups. Such number fields are interesting because in general, if the p-class group of a number field K is cyclic then p does not divide the class number of the Hilbert class field of K; in particular, the p-class field tower of K is finite [6, lemma 7]. In this paper we give an affirmative answer to Hajir's question.

Theorem 1.1. *For any integer $k \geq 1$, there exist infinitely many complex quadratic fields for which the Sylow 2-subgroups of their class groups are cyclic of order 2^k.*

By modifying a standard argument, we can construct complex quadratic fields with arbitrarily large cyclic 2-class group by finding distinct odd primes p_1, p_2 whose sum is four times an even integer power, cf. corollary 2.2. The existence of such prime pairs is guaranteed by a theorem of Perelli, which says that the binary

Goldbach problem for values of polynomials is true on average [8]. To pin down the exact size of the cyclic 2-class groups so produced, we apply the aforementioned criterion for deciding if an ideal class is a square to these prime pairs and turn it into congruence conditions on the prime pairs. Mimicing Perelli's circle method argument with these additional congruence conditions and the theorem follows. We give the class group arguments in §2. The proof of Theorem 1.1 is completed by generalizing some circle method results of Perelli, which we do in §3.

Remark. We do not have an analogous result for *real* quadratic fields, and there remains the question of constructing infinitely many quadratic class groups, real or complex, with prescribed, non-cyclic (narrow or full) 2-class groups.

2. PRESCRIBED CYCLIC 2-CLASS GROUPS

Lemma 2.1. *Fix an integer $m > 1$, and set $d = 4w^{2m} - x^2 > 0$ with $w, x \in \mathbf{Z}$ and positive. If w is even, $(x, w) = 1$, and $0 < x \leq 2w^m - 2$, then the class group of $\mathbf{Q}(\sqrt{-d})$ contains an element of order $2m$.*

Proof. This is classical, see for instance [1], except we do not require w to be prime and we need d to be odd. For completeness we give the argument.

Since x is odd and $-d \equiv 1 \, (\mathrm{mod} \, 4)$, both $\frac{x \pm \sqrt{-d}}{2}$ are algebraic integers in the ring of integers $\mathcal{O}_{-d}$ of $\mathbf{Q}(\sqrt{-d})$. We claim that the principal ideals $(\frac{x \pm \sqrt{-d}}{2})$ are coprime; otherwise some prime ideal $\mathfrak{p}$ of $\mathcal{O}_{-d}$ divides $(\frac{x^2 + d}{4}) = (w^{2m})$ as well as the *element* $\frac{x + \sqrt{-d}}{2} + \frac{x - \sqrt{-d}}{2} = x$, whence $\mathfrak{p}$ divides $(w, x) = 1$, a contradiction. Thus $(\frac{x \pm \sqrt{-d}}{2})$ are coprime ideals, whence the equality $4w^{2m} = d + x^2$ implies that $(\frac{x + \sqrt{-d}}{2}) = J^{2m}$ for some ideal J of $\mathcal{O}_{-d}$ with $J \neq J' :=$ the conjugate of J. Moreover, $\mathrm{Norm}(J) = w$ since $w > 0$.

Suppose the ideal class of J has order $< 2m$, and hence a proper divisor of $2m$. Then J^n is a principal ideal $(u + v\sqrt{-d})$ for some $0 < n \leq m$ with $u, v \in \frac{1}{2}\mathbf{Z}$. If $v \neq 0$, then

$$d/4 \; \leq \; u^2 + dv^2 \; = \; \mathrm{Norm}_{k/\mathbf{Q}}(J^n).$$

Since $n \leq m$, we have $\mathrm{Norm}_{k/\mathbf{Q}}(J^n) = w^n \leq w^m$, so $d \leq 4w^m$. But $0 < d = 4w^{2m} - x^2$, so $4w^{2m} - 4w^m \leq x^2$, whence $(2w^m - 1)^2 \leq x^2 + 1 < (x + 1)^2$, contradicting our hypothesis on x. Thus $v = 0$, whence $J^n = (u) = (J')^n$ as ideals, and hence $J = J'$, a contradiction. So the ideal class of J has order exactly $2m$, and the lemma follows. $\qquad\square$

Corollary 2.2. *Fix an integer $k \geq 1$, and suppose that there exists an even integer w such that $4w^{2^{k-1}}$ is the sum of two distinct primes $p_1, p_2 \geq 3$. Then the 2-class group of $\mathbf{Q}(\sqrt{-p_1 p_2})$ is cyclic of order divisible by 2^k.*

Proof. Since w is even, necessarily $p_1 p_2 \equiv 3 \, (\mathrm{mod} \, 4)$. Then genus theory implies that the 2-class group of $\mathbf{Q}(\sqrt{-p_1 p_2})$ is cyclic. We can write the two primes as $2w^{2^{k-1}} \pm x$ with $0 < x \leq 2w^{2^{k-1}} - 2$, so $p_1 p_2 = 4w^{2^k} - x^2 = 4w^{2 \cdot 2^{k-1}} - x^2$; the

condition $0 < x \leq 2w^m - 2$ now becomes $p_i \geq 3$. Apply Lemma 2.1 and we get the second part of the corollary. $\qquad\square$

For the rest of this paper, we take

$p_1 p_2 = 4w^{2^k} - x^2$ with $k \geq 1$, w even and positive, and $p_1, p_2 \geq 3$ distinct primes.

The condition that w is even implies that $p_1 p_2 \equiv 3 \,(\mathrm{mod}\ 4)$; from now on we stipulate that

$$p_1 \equiv 1 \,(\mathrm{mod}\ 4) \quad \text{and} \quad p_2 \equiv 3 \,(\mathrm{mod}\ 4).$$

Lemma 2.1 then furnishes an ideal J in $\mathcal{O}_{-d}$ of norm w whose ideal class has exact order 2^k. We now determine whether or not this ideal class of J is not the square of another ideal class. Since the 2-class group of $\mathcal{O}_{-d}$ is cyclic, this is equivalent to asking if the 2-class group has exact order 2^k.

Lemma 2.3. *With the notation as above, the 2-class group of $\mathbf{Q}(\sqrt{-p_1 p_2})$ is cyclic of exact order 2^k if and only if the quadratic symbol $(p_1/w) = -1$.*

Proof. For any negative fundamental discriminant $-D$ and for any ideal $\mathfrak{a} \subset \mathcal{O}_{-D}$, the 'fundamental criterion' in [5, p. 345] says that the ideal class of $\mathfrak{a}$ is a square if and only the Hilbert symbols

$$\left(\frac{\mathrm{Norm}(\mathfrak{a}), -D}{p}\right) = 1 \qquad \text{for every prime } p | D.$$

Moreover, by [5, (1.8) on p. 345],

(1) $$\prod_{p|D}\left(\frac{\mathrm{Norm}(\mathfrak{a}), -D}{p}\right) = 1.$$

We now apply this to the ideal class J of order divisible by 2^k furnished by Lemma 2.1. We have $\mathrm{Norm}(J) = w$, and since the fundamental discriminant $-p_1 p_2$ has exactly two prime divisors, (1) implies that

$$\left(\frac{w, -p_1 p_2}{p_1}\right) = \left(\frac{w, -p_1 p_2}{p_2}\right).$$

In particular,

the ideal class of J is *not* a square $\Longleftrightarrow \left(\dfrac{w, -p_1 p_2}{p_1}\right) = -1 \Longleftrightarrow \left(\dfrac{w, -p_1 p_2}{p_2}\right) = -1.$

Since $4w^{2^{k-1}} = p_1 + p_2$, we have $p_1 \nmid w$. Expressing the Hilbert symbol in terms of Legendre symbols [11, Thm. 1 on p. 20] and recalling that $p_1 \equiv 1 \,(\mathrm{mod}\ 4)$ and $p_2 \equiv 3 \,(\mathrm{mod}\ 4)$, we see that

(2) the ideal class of J is *not* a square $\Longleftrightarrow \left(\dfrac{p_1}{w}\right) = -1 \Longleftrightarrow \left(\dfrac{p_2}{w}\right) = \left(\dfrac{-1}{w}\right).$

As the 2-class group of $\mathbf{Q}(\sqrt{-p_1 p_2})$ is cyclic, we are done. $\qquad\square$

3. Circle Method

Thanks to Lemma 2.3, to prove Theorem 1.1 for a given $k \geq 1$ we need to find infinitely many pairs of distinct odd primes $p_1, p_2 \geq 3$ such that

(i) $p_1 + p_2 = 4w^{2^{k-1}}$ with w even, and

(ii) $p_1 \equiv 1 \pmod{4}$, and

(iii) $(p_1/w) = -1$.

The first condition is the binary Goldbach problem for polynomials, which Perelli [8] has already shown to be true on average. Denote by $\Lambda(d)$ the von Mangoldt function, and define

$$R(d) = \sum_{d_1 + d_2 = d, \, d_i > 0} \Lambda(d_1)\Lambda(d_2).$$

Let $F \in \mathbf{Z}[x]$ be a non-constant polynomial. For any integer $d > 0$, define

$$\rho_F(d) = \#\{m \pmod{d} : F(m) \equiv 0 \pmod{d}\}.$$

Denote by $a(F)$ the leading coefficient of F. Define

$$C(F) = a(F)\rho_F(2) \prod_{p > 2} \left(1 + \frac{\rho_F(p)}{p(p-2)}\right)\left(1 - \frac{1}{(p-1)^2}\right).$$

Suppose $a(F)$ is *positive*. For $N > 0$, set $N_F = N^{1/(2 \deg F)}$. A special case of a theorem of Perelli [8, Thm. 2] says that for any $A > 0$,

$$(3) \qquad \sum_{N_F^2 \leq n \leq N_F^2 + N_F} R(F(n)) = C(F)N_F^{1 + 2 \deg F} + O_{A,F}(N^{1 + 2 \deg F} \log^{-A} N_F).$$

If d is not the sum of two primes then

$$R(d) \leq \sum_{p^n \leq d, \, n \geq 2} \log(p) \log(\sqrt{d - p^n}) \ll d^{1/2} \log^2 d,$$

so the contribution to the left side of (3) from those $F(n)$ that are not the sum of two primes is $O_F(N_F^{1 + \deg F} \log^2 N_F)$. Similarly, the contribution to the left side of (3) from those n for which $F(n) = p_1 + p_2$ with one of the $p_i < 5$ is $O(N_F)$. Since F is non-constant, $C(F) \neq 0$ if and only if $\rho_F(2) \neq 0$, which in turn is equivalent to F taking on even values. So Perelli's theorem implies that if $F \in \mathbf{Z}[x]$ is non-constant and takes on even values, then infinitely many of its values can be written as the sum of two primes ≥ 3. Applying this to $F(x) = 2(2x)^{2^{k-1}}$, we see that for any fixed $k > 1$, Perelli's theorem implies that condition (i) holds for infinitely many pairs of primes $p_1, p_2 \geq 3$.

Perelli's theorem is proved using the circle method, for which we can readily introduce congruence conditions such as (ii). We now explain how to handle condition (iii). Suppose the even integer w is of the form $w = 2M^2$ for some integer M. Note that w is coprime to the p_i, so

$$\left(\frac{p_1}{w}\right) = \left(\frac{p_1}{2}\right)\left(\frac{p_1}{M}\right)^2 = \left(\frac{p_1}{2}\right) = \begin{cases} 1 & \text{if } p_1 \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p_1 \equiv \pm 3 \pmod{8}. \end{cases}$$

Combine everything and we see that to prove Theorem 1.1 it suffices to prove the following result.

Theorem 3.1. *Given any $k \geq 1$, there exist infinitely many pairs of primes $p_1, p_2 \geq 3$ and integers $w = 2M^2$ such that*
- (1) $p_1 + p_2 = 4(2M^2)^{2^{k-1}} = 2^{1+2^{k-1}} M^{2^k}$ *for some integer M, and*
- (2) $p_1 \equiv 5 \pmod 8$ *and* $p_2 \equiv 3 \pmod 8$.

There are several different approaches we could take to prove Theorem 3.1. We chose to modify Perelli's paper by changing the generating function and mirroring the calculations. Another approach would be to introduce products of characters to restrict to given equivalence classes (in the spirit of (37) below) earlier. Such an attack would quickly give us the factor of $1/4$ for the main term, but would require a new analysis of bounds on exponential sums twisted by a character. Further, it would still require us to mirror Perelli's arguments. As both approaches require us to follow Perelli's paper, to aid the reader who may not be as familiar with these techniques as with the earlier algebraic arguments, we take the first approach.

3.1. **Preliminaries.** Let N be a large integer, and $F \in \mathbb{Z}[x]$ with $\deg F = k \geq 1$. Define

$$(4) \qquad f_2(\alpha; N) = \sum_{p \leq c_1 N} (\log p) e(\alpha p)$$

where p ranges over primes congruent to $\pm 3 \pmod 8$, c_1 is a suitable coefficient depending on F, and as always

$$(5) \qquad\qquad e(x) \;=\; e^{2\pi i x}.$$

We choose this notation to mirror that of Vaughan [13, p. 27-37], where $f(\alpha)$ is the same sum, but without the restriction on p. We use the subscript of 2 in function definitions throughout to point out such similar parallels.

We briefly comment on the role c_1 plays. In our applications we will take n satisfying $N^{1/k} \leq n \leq N^{1/k} + H$ for some small $H \leq N^{1/k}$. Thus if $F(x) = cx^k + \cdots$ then $F(n)$ will be on the order of cN. If $c = 3$ then we cannot write $F(n) = p_1 + p_2$ if we restrict to primes at most N. This is why we must let the sums be a little longer; taking c_1 to be 3^k times the leading coefficient of F will clearly suffice for all large N.

Define $P = (\log N)^B$ where B is a positive constant, and for $1 \leq a \leq q \leq P$ with $(a, q) = 1$ define

$$(6) \qquad\qquad \mathfrak{M}(q, a) = \{\alpha : |\alpha - a/q| \leq PN^{-1}\}$$

as the major arc centered at a/q, and let $\mathfrak{M}$ denote the union of all the $\mathfrak{M}(q, a)$. Since N is large, the major arcs are all disjoint and lie in $(PN^{-1}, 1 + PN^{-1}]$. We define the minor arcs by

$$\mathfrak{m} = (PN^{-1}, 1 + PN^{-1}] \setminus \mathfrak{M}.$$

We have

$$(7) \qquad R_2(n) = \int_{\mathfrak{M}} f_2(\alpha; N)^2 e(-n\alpha) \, d\alpha + \int_{\mathfrak{m}} f_2(\alpha; N)^2 e(-n\alpha) \, d\alpha$$

where

$$(8) \qquad R_2(n) = \sum_{\substack{p_1,p_2 \le c_1 N \\ p_1+p_2=n}} \log p_1 \ \log p_2$$

with, again, the primes restricted mod 8 as with $f_2(\alpha; N)$. Note $R_2(n)$ is a weighted counting of the number of representations of n as a sum of two primes congruent to 3 or 5 modulo 8. Clearly if $R_2(n) > 0$ then there must be at least one representation of n having the desired properties. Further, from our choice of c_1 we see every representation of n is counted if n is of size $N + o(N)$; if n is much larger, we are only counting the representations with each prime factor at most $c_1 N$ and could therefore miss some.

While we are able to obtain good formulas for the integral over the major arc for a fixed n, there are no correspondingly nice estimates for the minor arc contribution. This should not be surprising, as if there were then we would essentially be solving the original Goldbach problem! Rather, we lower our expectations and obtain a good upper bound for the sum of the contributions of the minor arcs for all n in a small interval. The advantage of this approach is that we can now exploit cancellation from the n-sum; without this cancellation we have no chance of proving our claim.

We first state some needed arithmetic input in §3.2. We then analyze the major arcs in §3.3. In §3.4 we prove Theorem 3.1, in the course of which we bound the contribution from the minor arcs.

3.2. **Arithmetic Input.** The following function is used throughout our analysis of the major and minor arcs.

Definition 3.2. *Let μ_2 be an arithmetic function defined by $\mu_2(q) = \mu(q)/2$ whenever $8 \nmid q$, $\mu_2(8) = -\sqrt{2}$ and*

$$(9) \qquad \mu_2(8q) = \sum_{\substack{r=1 \\ (r,8q)=1}}^{8q} e(r/8q)$$

where $r \equiv \pm 3 \ (8)$.

Note that without the latter restriction the sum is just $\mu(8q) = 0$ by a well-known theorem. Hence if μ_3 is the same sum but instead with the restriction that $r \equiv \pm 1 \ (8)$, then $\mu_2(8q) = -\mu_3(8q)$. The next lemma is useful in finding a simple expression for $\mu_2(8q)$, which we will do in Lemma 3.4.

Lemma 3.3. *Let $k \ge 3$ be an integer and q be an odd positive integer. Define $\phi_2(2^k q)$ to be the number of positive integers $r < 2^k q$ with $(r, 2^k q) = 1$ and $r \equiv \pm 3$ (8). Define $\phi_3(2^k q)$ similarly except with $r \equiv \pm 1$ (8). Then*

$$\phi_2(2^k q) = \phi_3(2^k q) = 2^{k-2}\phi(q).$$

Proof. Clearly if $(r, 2^k q) = 1$, then either $r \equiv \pm 3$ (8) or $r \equiv \pm 1$ (8), so we have $\phi_2(2^k q) + \phi_3(2^k q) = \phi(2^k q) = 2^{k-1}\phi(q)$. So we need only show $\phi_2(2^k q) = \phi_3(2^k q)$.

Let a and b be any integers congruent to 3 mod 8 with $(a, 2^k q) = 1 = (b, 2^k q)$. Then letting c and d be the smallest positive integers congruent to $a + 4q$ and

$b + 4q$, respectively, we quickly have $(c, 2^k q) = 1 = (d, 2^k q)$, $c \equiv d \equiv 7$ (8), and $c = d \implies a = b$. Using a similar argument to map integers 5 mod 8 to those 1 mod 8, we have that $\phi_2(2^k q) \leq \phi_3(2^k q)$. By a near-identical argument, we have that $\phi_3(2^k q) \leq \phi_2(2^k q)$. Hence $\phi_2(2^k q) = \phi_3(2^k q)$, and the lemma follows. $\square$

We now give a simple formula for $\mu_2(8q)$, which will be useful in evaluating certain exponential sums.

Lemma 3.4. *We have*

(10) $$\mu_2(8q) = \left(\frac{q}{2}\right) |\mu(q)| \sqrt{2}$$

for all $q > 1$, where $\left(\frac{q}{2}\right)$ is the Kronecker symbol

$$\left(\frac{q}{2}\right) = \begin{cases} 0 & \text{if } q \text{ is even,} \\ 1 & \text{if } q \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } q \equiv \pm 3 \pmod{8}. \end{cases}$$

Proof. First note that

$$\begin{aligned} \mu_2(8) &= e(3/8) + e(5/8) \\ &= 2\cos(3\pi/4) \\ &= -\sqrt{2}. \end{aligned}$$

It happens that for all $k > 3$, $\mu_2(2^k) = 0$. To see this, first note that for $r \equiv \pm 3$ (8), $(r, 2^k) = 1$. So

$$\mu_2(2^k) = \sum_{n=1}^{2^{k-3}} e\left(\frac{8n - 5}{2^k}\right) + \sum_{n=1}^{2^{k-3}} e\left(\frac{8n - 3}{2^k}\right).$$

As each of these sums is geometric with common ratio $e(8/2^k) = e(1/2^{k-3})$, we have

$$\begin{aligned} \mu_2(2^k) &= \frac{e\left(\frac{2^k+3}{2^k}\right) - e\left(\frac{3}{2^k}\right)}{e(1/2^{k-3}) - 1} + \frac{e\left(\frac{2^k+5}{2^k}\right) - e\left(\frac{5}{2^k}\right)}{e(1/2^{k-3}) - 1} \\ &= 0. \end{aligned}$$

We now show that, for odd q and any $k \geq 3$, $|\mu_2(2^k q)| = |\mu_2(2^k)\mu(q)|$. We have from Lemma 3.3 that $\mu_2(2^k q)$ (resp. $\mu_3(2^k q)$) consists of a sum of $2^{k-2}\phi(q)$ terms ranging over all $r \equiv \pm 3$ (8) (resp. $r \equiv \pm 1$ (8)) such that $(r, 2^k q) = 1$. Using the fact that

$$\mu(q) = \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e(r/q),$$

a sum with $\phi(q)$ terms, we note that a sum expansion of $\mu_2(2^k)\mu(q)$ would contain $2^{k-2}\phi(q)$ terms. Each term would be of the form $e(s/2^k)e(t/q) = e\left(\frac{sq + 2^k t}{2^k q}\right)$ with $s \equiv \pm 3$ (8) and $(t, q) = 1$. Clearly this fraction is always in lowest terms, since $2 \nmid sq$ and $(2^k t, q) = 1$. Depending on whether $q \equiv \pm 1$ (8) or ± 3 (8), $sq + 2^k t$

is always either ± 3 (8) or ± 1 (8), respectively. Also, if $s_0 q + 2^k t_0 \equiv s_1 q + 2^k t_1$ (mod $2^k q$), then $(s_0 - s_1)q + (t_0 - t_1)2^k \equiv 0$ (mod $2^k q$) and so $s_0 = s_1$ and $t_0 = t_1$ since $s_0, s_1 < 2^k$ and $t_0, t_1 < q$. Therefore the expansion of $\mu_2(2^k)\mu(q)$ contains exactly $2^{k-2}\phi(q)$ different terms, and either $\mu_2(2^k)\mu(q) = \mu_2(2^k q)$ or $\mu_2(2^k)\mu(q) = \mu_3(2^k q)$. Since $|\mu_2| = |\mu_3|$, we can say that $|\mu_2(2^k)\mu(q)| = |\mu_2(2^k q)|$.

From here it's not hard to check that $\mu_2(2^k q) = -\sqrt{2}$ if $q > 1$ is squarefree and $\pm 3 \mod 8$ and $\mu_2(2^k q) = \sqrt{2}$ if $q > 1$ is squarefree and $\pm 1 \mod 8$. $\square$

We end with the promised relation between an exponential sum and μ_2, which is used in finding a good approximating function to f_2 on the major arcs.

Lemma 3.5. *With the usual restrictions on r and $(a, 8q) = 1$, we have*

$$(11) \qquad \sum_{\substack{r=1 \\ (r,8q)=1}}^{8q} e(ar/8q) = \left(\frac{a}{2}\right)\mu_2(8q).$$

Proof. This follows immediately from the arguments above, as $\mu_2(r)$ if $a \equiv \pm 1 \mod 8$ and and $\mu_3(r) = -\mu_2(r)$ if $a \equiv \pm 3 \mod 8$. $\square$

3.3. **Contribution from the Major Arcs.** The following analogue of Vaughan's Lemma 3.1 [13, p. 30] allows us to approximate our generating function f_2 on the major arcs with a well-behaved function, up to a small error.

Lemma 3.6. *Let*

$$(12) \qquad v(\beta) = \sum_{m=1}^{c_1 N} e(\beta m).$$

Then there is a positive constant C such that whenever $1 \le a \le q \le P$, $(a, q) = 1$ and $\alpha \in \mathfrak{M}(q, a)$ one has

$$(13) \qquad f_2(\alpha; N) = \frac{\mu_2(q)}{\phi(q)} v(\alpha - a/q) + O(N \exp(-C(\log n)^{1/2}))$$

whenever $8 \nmid q$ and

$$(14) \qquad f_2(\alpha; N) = \frac{\left(\frac{a}{2}\right)\mu_2(q)}{\phi(q)} v(\alpha - a/q) + O(N \exp(-C(\log n)^{1/2}))$$

otherwise.

Proof. Following Vaughan [13], we define our generating function to be

$$(15) \qquad f_2(\alpha; N) = \sum_{\substack{p \le c_1 N \\ p \equiv \pm 3 \, (8)}} (\log p)e(\alpha p).$$

We note that the corresponding generating function for Perelli [8] is (in his notation)

$$(16) \qquad S(\alpha) = \sum_{n \le c_1 N} \Lambda(n)e(n\alpha).$$

There is no harm in replacing $\Lambda(n)$ (which restricts the sum to prime powers) with $\lambda(n)$ (which restricts the sum to primes), as the difference between these two sums is $O(N^{1/2})$, which can easily be absorbed by the error terms. In fact, for our purposes it is better to restrict to prime sums as this way we know that the representation will be as a sum of two primes and not potentially a prime power.

We first consider the special case $\alpha = a/q$, and then as is standard pass to all α in the major arc $\mathfrak{M}(q, a)$. We have

$$(17) \qquad f_2(a/q; N) \;=\; \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e(ar/q)\vartheta_2(c_1 N, q, r) + O((\log N)(\log q))$$

with

$$(18) \qquad \vartheta_2(x, q, r) \;=\; \sum_{\substack{p \leq x \\ p \equiv r \,(q)}} \log p$$

where the primes p, in addition to satisfying $p \equiv r \bmod q$, must also satisfy $p \equiv \pm 3 \bmod 8$. We must now break into cases depending on q.

If $q = 2^k q_0$ with $k \leq 1$ and q_0 odd, then $p \equiv r \bmod q$ and $p \equiv \pm 3 \bmod 8$ imply that there exist r_1 and r_2 such that

$$\vartheta_2(c_1 N, q, r) \;=\; \sum_{\substack{p \leq c_1 N \\ p \equiv r_1 \,(8q_0)}} \log p + \sum_{\substack{p \leq c_1 N \\ p \equiv r_2 \,(8q_0)}} \log p$$

$$= \frac{2c_1 N}{\phi(8q_0)} + O(N \exp(-C_1(\log N)^{1/2}))$$

$$(19) \qquad = \frac{c_1 N}{2\phi(q)} + O(N \exp(-C_1(\log N)^{1/2}))$$

by the Siegel-Walfisz theorem[1] and the fact that, if $q = 2q_0$, $\phi(q) = \phi(q_0)$.

If $q = 4q_0$ with q_0 odd, then $p \equiv r \bmod q$ and $p \equiv \pm 3 \bmod 8$ implies that either all the p are 3 mod 8 or 5 mod 8 (depending on $r \bmod 4$), so there exists r_1 such that

$$\vartheta_2(c_1 N, q, r) \;=\; \sum_{\substack{p \leq c_1 N \\ p \equiv r_1 \,(8q_0)}} \log p$$

$$= \frac{c_1 N}{\phi(8q_0)} + O(N \exp(-C_2(\log N)^{1/2}))$$

$$(20) \qquad = \frac{c_1 N}{2\phi(q)} + O(N \exp(-C_2(\log N)^{1/2})).$$

---

[1]The Siegel-Walfisz theorem states that for $C, B > 0$ and a and q relatively prime, then $\sum_{\substack{p \leq x \\ p \equiv a(q)}} \log p = \frac{x}{\phi(q)} + O(x/\log^C x)$ for $q \leq \log^B x$, and the big-Oh constant depends only on C and B. See for example [4, 7].

Hence, if $8 \nmid q$,

$$(21) \qquad f_2(a/q; N) = \frac{c_1 N}{2\phi(q)} \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e(ar/q) + O(N \exp(-C(\log N)^{1/2})).$$

The sum on the right hand side is well-known to equal $\mu(q)$. Therefore

$$f_2(a/q; N) = \frac{c_1 N \mu(q)}{2\phi(q)} + O(N \exp(-C(\log N)^{1/2}))$$

$$(22) \qquad\qquad = \frac{c_1 N \mu_2(q)}{\phi(q)} + O(N \exp(-C(\log N)^{1/2})).$$

When $8 \mid q$, we have that $\vartheta_2(c_1 N, q, r) = 0$ if $r \equiv \pm 1 \bmod 8$ and

$$(23) \qquad \vartheta_2(c_1 N, q, r) = \frac{c_1 N}{\phi(q)} + O(N \exp(-C_3(\log N)^{1/2}))$$

if $r \equiv \pm 3 \bmod 8$. Hence

$$(24) \qquad f_2(a/q; N) = \frac{c_1 N}{\phi(q)} \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e(ar/q) + O(N \exp(-C(\log N)^{1/2}))$$

where the sum only counts $r \equiv \pm 3 \bmod 8$. However, we know from Lemma 3.5 that this sum is just $\left(\frac{a}{2}\right) \mu_2(q)$. So when $8 \mid q$,

$$(25) \qquad f_2(a/q; N) = \frac{c_1 N \left(\frac{a}{2}\right) \mu_2(q)}{\phi(q)} + O(N \exp(-C(\log n)^{1/2})).$$

As $v(0) = c_1 N$, the lemma's claim is true when we take $\alpha = p/q$. The rest of the proof (namely, general α in the major arc $\mathfrak{M}(q, a)$) proceeds almost identically to the proof of the corresponding lemma in Vaughan [13, p. 31], with the only difference being 2-subscripts added in obvious places. $\qquad\square$

Consider a major arc $\mathfrak{M}(q, a)$ where $8 \mid q$. Since $(q, a) = 1$, we must have that a is odd, and hence $\left(\frac{a}{2}\right)^2 = 1$. Therefore, for $\alpha \in \mathfrak{M}(q, a)$, an arbitrary major arc, the lemma above gives

$$(26) \qquad f(\alpha)^2 - \frac{\mu_2(q)^2}{\phi(q)^2} v(\alpha - a/q)^2 \ll N^2 \exp(-C(\log N)^{1/2}).$$

The rest of the major arc treatment is the same as in Vaughan (p. 31-32), except for one non-trivial adjustment. The original singular series

$$(27) \qquad \mathfrak{S}_1(m) = \sum_{q=1}^{\infty} \frac{\mu(q)^2}{\phi(q)^2} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(-am/q)$$

needs to be replaced with

$$(28) \qquad \mathfrak{S}_2(m) = \sum_{q=1}^{\infty} \frac{\mu_2(q)^2}{\phi(q)^2} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(-am/q),$$

and we must show that $\mathfrak{S}_2(m)$ can also be bounded away from zero. We have that

$$\mathfrak{S}_2(m) \;=\; \frac{1}{4}\sum_{\substack{q=1\\8\nmid q}}^{\infty}\frac{\mu(q)^2}{\phi(q)^2}c_q(m)+\sum_{q=1}^{\infty}\frac{\mu_2(8q)^2}{\phi(8q)^2}c_{8q}(m)$$

$$(29)\qquad\qquad =\; \frac{\mathfrak{S}_1(m)}{4}+\frac{1}{8}c_8(m)\sum_{\substack{q=1\\q\ \mathrm{odd}}}^{\infty}\frac{\mu(q)^2}{\phi(q)^2}c_q(m)$$

where the $8\nmid q$ restriction in the first sum can be ignored since $\mu(8q)=0$ anyway, and $c_q(m)$ is Ramanujan's sum

$$(30)\qquad\qquad c_q(m) \;=\; \sum_{\substack{a=1\\(a,q)=1}}^{q} e(-am/q),$$

which is a multiplicative function of q, and is known to equal

$$(31)\qquad\qquad c_q(m) \;=\; \frac{\mu(q/(q,m))\phi(q)}{\phi(q/(q,m))}.$$

To calculate the sum in (29) over q odd, first write

$$(32)\qquad\qquad \mathfrak{S}_1(m) \;=\; \sum_{\substack{q=1\\q\ \mathrm{odd}}}^{\infty}\frac{\mu(q)^2}{\phi(q)^2}c_q(m)+\sum_{\substack{q=2\\q\ \mathrm{even}}}^{\infty}\frac{\mu(q)^2}{\phi(q)^2}c_q(m).$$

Since $\mu(q)=0$ whenever $4\mid q$, we can take the second sum just over $q=2q_0$, where q_0 is odd. Since μ,ϕ, and c_q are all multiplicative on q, we have

$$\mathfrak{S}_1(m) \;=\; \sum_{\substack{q=1\\q\ \mathrm{odd}}}^{\infty}\frac{\mu(q)^2}{\phi(q)^2}c_q(m)+\frac{\mu(2)^2}{\phi(2)^2}c_2(m)\sum_{\substack{q=1\\q\ \mathrm{odd}}}^{\infty}\frac{\mu(q)^2}{\phi(q)^2}c_q(m)$$

$$(33)\qquad\qquad =\; 2\sum_{\substack{q=1\\q\ \mathrm{odd}}}^{\infty}\frac{\mu(q)^2}{\phi(q)^2}c_q(m).$$

Therefore

$$(34)\qquad\qquad \mathfrak{S}_2(m) \;=\; \frac{\mathfrak{S}_1(m)}{4}\left(1+\frac{c_8(m)}{4}\right).$$

Note that $\mathfrak{S}_2(m)=0$ when m is odd or $m\equiv 4 \mod 8$, which is what one would expect, since the only numbers which can be written as the sum of primes 3 and/or 5 mod 8 are those 0, 2, and 6 mod 8, and in those cases it is clear that $\mathfrak{S}_2(m)\gg 1$ since $\mathfrak{S}_1(m)\gg 1$.

3.4. **Proof of Theorem 3.1.** We are now ready to prove the following result, which we then show immediately yields Theorem 3.1.

Theorem 3.7. *Let $F \in \mathbf{Z}[x]$ be a polynomial of degree $k > 0$ that is not always odd, $L = \log N$, $A, \varepsilon \geq 0$, and assume H satisfies $N^{1/(3k)+\varepsilon} \leq H \leq N^{1/k-\epsilon}$. Then*

$$(35) \qquad \sum_{N^{1/k} \leq n \leq N^{1/k}+H} |R_2(F(n)) - F(n)\mathfrak{S}_2(F(n))|^2 \ll HN^2 L^{-A}.$$

Proof. Taking $H = N^{1/(3k)+\varepsilon}$, $\varepsilon > 0$ sufficiently small, we may write

$$\sum_{N^{1/k} \leq n \leq N^{1/k}+H} |R_2(F(n)) - F(n)\mathfrak{S}_2(F(n))|^2$$

$$= \sum_{N^{1/k} \leq n \leq N^{1/k}+H} \left| \int_{\mathfrak{M}} f_2(\alpha; N)^2 e(-F(n)\alpha) \, d\alpha \right.$$

$$\left. + \int_{\mathfrak{m}} f_2(\alpha; N)^2 e(-F(n)\alpha) \, d\alpha - F(n)\mathfrak{S}_2(F(n)) \right|^2$$

$$\leq \sum_{N^{1/k} \leq n \leq N^{1/k}+H} \left| \int_{\mathfrak{M}} f_2(\alpha; N)^2 e(-F(n)\alpha) \, d\alpha - F(n)\mathfrak{S}_2(F(n)) \right|^2$$

$$+ \sum_{N^{1/k} \leq n \leq N^{1/k}+H} \left| \int_{\mathfrak{m}} f_2(\alpha; N)^2 e(-F(n)\alpha) \, d\alpha \right|^2$$

$$= \sum_{\mathfrak{M}} + \sum_{\mathfrak{m}}.$$

We apply our estimation for $f_2(\alpha; N)$ from Lemma 3.6 and our new singular series $\mathfrak{S}_2$ (and its bounds) to integrate it over the major arcs, and then argue as in equations (2) to (4) of Perelli [8] to bound its difference from $F(n)\mathfrak{S}_2(F(n))$. We find

$$(36) \qquad \sum_{\mathfrak{M}} \ll HN^2 L^{-2B+c_2} + HN^2 L^{-A}$$

where c_2 is a suitable constant based on F and $L = \log N$.

We are left with bounding $\sum_{\mathfrak{m}}$. As this minor arc calculation is almost identical to that in [8], we simply highlight below the harmless modifications needed in adopting Perelli's framework to our problem. His minor arc calculation begins with equation (5) at the bottom of [8, p. 481]. With the exception of the final reference in the last bullet point, *all* equation numbers and expressions in the bullet points below refer to items in [8].

- Equation (5) follows from algebraic manipulation of S, and does not depend greatly on the actual definition of S. We find a similar estimate for

our quantity, defined in (15):

$$f_2(\alpha; N) \;=\; \sum_{\substack{p \le c_1 N \\ p \equiv \pm 3\,(8)}} (\log p) e(\alpha p),$$

which differs from the sum in [8] in two minor ways: we have $\lambda(n)$ instead of $\Lambda(n)$, and our n is restricted to be $\pm 3 \bmod 8$.

- Equations (6) through (8) prove a variant of Weyl's inequality, which is also true for our variant of S.

- Equations (9) to (14) manipulate the arcs themselves and do not depend on S, and are therefore true in our case as well.

- Equation (15) directly involves S, and therefore changes slightly in our case. Remember that we want to restrict S to only count primes restricted to those congruent to 3 and 5 mod 8. Hence we replace μ with μ_2 as defined in the major arc section, and we change W to sum only over our restricted set of primes. The change from μ to μ_2 has absolutely no effect on the argument, since all that matters is that μ_2^2 is bounded by a small constant (specifically, 2), which gets absorbed in the constant induced by the $\ll$. T does not depend on primes, and is thus unchanged.

- Equation (16) is a simple rearrangement, and follows for our problem as well. Equations (17) to (23) are L-function arguments that do not change, and Equation (24) is just Parseval.

- To get from Equation (24) to (25) requires an estimate for W, and therefore requires updating since we have changed the definition of W. The estimation is based on the formula

$$\sum_{n \le x} \Lambda(n)\chi(n) - \delta_\chi x \;=\; \sum_\rho \frac{x^\rho}{\rho} + O(L^2),$$

where the sum on the right is over the non-trivial zeroes of $L(s, \chi)$ and δ_χ is 1 if $\chi = \chi_0$ and 0 otherwise. We want to restrict this sum to $n \equiv \pm 3 \bmod 8$. We can do this by writing

$$\sum_{n \le x} \Lambda(n)\chi(n)\frac{1 - \left(\frac{n}{2}\right)}{2} - \delta_\chi x \;=\; \sum_{n \le x} \Lambda(n)\chi(n) - \delta_\chi x - \frac{1}{2}\sum_{n \le x} \Lambda(n)\chi(n)\left(\frac{n}{2}\right).$$

Since $\chi(n)\left(\frac{n}{2}\right)$ is itself a non-principal character, we can simply apply (37) to the second sum, and we see that the restricted sum is of the same order of magnitude as the original; hence we can conclude the same estimation of the minor arcs. The result follows directly from Perelli's calculations. He cites work by himself and Pintz, [9]. In that paper, we see the only change is in Equation (22), and that change is just the character manipulation which we've already described above.

$\square$

We can now complete the proof of our main result.

Proof of Theorem 3.1. By Theorem 3.7, we have

$$(37) \qquad \sum_{N^{1/k} \leq n \leq N^{1/k}+H} |R_2(F(n)) - F(n)\mathfrak{S}_2(F(n))|^2 \ \ll \ \frac{HN^2}{\log^A N}$$

with $N^{1/(3k)+\varepsilon} \leq H \leq N^{1/k-\epsilon}$. Trivial estimation gives $F(n)\mathfrak{S}_2(F(n)) \gg N$; here we are using $F(n) \gg N$ and $\mathfrak{S}_2(F(n)) \gg 1$. Imagine that none of the $F(n)$ (for n in the range specified) can be represented as the sum of two primes satisfying our conditions. Then $R_2(F(n)) = 0$ for all these n, and the n-sum equals

$$(38) \qquad \sum_{N^{1/k} \leq n \leq N^{1/k}+H} |F(n)\mathfrak{S}_2(F(n))|^2 \ \gg \ \sum_{N^{1/k} \leq n \leq N^{1/k}+H} N^2 \ = \ HN^2.$$

For N sufficiently large, however, this contradicts Theorem 3.7, which says the n-sum is at most $HN^2/\log^A N$. Thus there must be at least one n in the given range that has the desired representation.

To obtain infinitely many n, we repeat these arguments on disjoint intervals; for example, if N is sufficiently large we may take $N_\ell = N^\ell$, so for the ℓth interval we have the range $N^{\ell/k} \leq n \leq N^{\ell/k} + H_\ell$. $\qquad \square$

Remark. In the interest of keeping the exposition as elementary as possible, we do not optimize the proof of Theorem 3.4. With a little more work, arguing along the lines of [8] we could obtain some estimates on the number of n in the studied intervals that have the desired representation. This would make our results on the infinitude of complex quadratic fields for which the Sylow 2-subgroups of their class groups are cyclic of order 2^k explicit, giving a lower bound on the number of such fields. As this would be at the cost of keeping the exposition clear, and the resulting bounds would be too small for applications, we do not pursue this here.

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] H. Bauer, Die 2-Klassenzahlen spezieller quadratischer Zahlkörper. *J. Reine Angew. Math.* **252** (1972) 79-81.

[3] H. Bauer, Zur Berechnung der 2-Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern. *J. Reine Angew. Math.* **248** (1971) 42-46.

[4] H. Davenport, Multiplicative Number Theory, 2nd edition (revised by H. Montgomery). Graduate Texts in Mathematics, Vol. 74, Springer-Verlag, New York, 1980.

[5] H. Hasse, An algorithm for determining the structure of the 2-Sylow-subgroups of the divisor class group of a quadratic number field, in: *Symposia Mathematica, Vol. XV*, p. 341–352. Academic Press, 1975.

[6] F. Hajir, On the class numbers of Hilbert class fields. *Pacific J. Math.* **181** (1997) 177-187.

[7] H. Iwaniec and E. Kowalski, Analytic Number Theory. AMS Colloquium Publications, Vol. 53, AMS, Providence, RI, 2004.

[8] A. Perelli, Goldbach numbers represented by polynomials. *Rev. Mat. Iberoamericana* **12** (1996) 477-490.

[9] A. Perelli and J. Pintz, On the exceptional set for Goldbach's problem in short intervals. *J. London Math. Soc* **47** (1993), 41–49.

[10] L. Rédei, Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung. Acta Math. Acad. Sci. Hungar. **4** (1953) 31-87.

[11] J. P. Serre, *A course in arithmetic.* Springer-Verlag, 1973.

[12] D. Shanks, Gauss's ternary form reduction and the 2-Sylow subgroup. *Math. Comp.* **25** (1971) 837-853. Corrigenda, *Math. Comp.* **32** (1978) 1328-1329.

[13] R. C. Vaughan, The Hardy-Littlewood Method (second edition). Cambridge Tracts in Mathematics, 1997

[14] W. C. Waterhouse, Pieces of eight in class groups of quadratic fields. *J. Number Theory* **5** (1973) 95-97.

DEPARTMENT OF MATHEMATICS & STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA 01267
E-mail address: Carlos.R.Dominguez@williams.edu

DEPARTMENT OF MATHEMATICS & STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA 01267
E-mail address: Steven.J.Miller@williams.edu

DEPARTMENT OF MATHEMATICS & STATISTICS, UNIVERSITY OF MASSACHUSETTS. AMHERST, MA 01003-9305 USA
E-mail address: siman@math.umass.edu