Rational Representations of Primes by Binary Quadratic Forms

Ronald Evans
Department of Mathematics, 0112
University of California at San Diego
La Jolla, CA 92093-0112
revans@ucsd.edu

Mark Van Veen
Varasco LLC, 2138 Edinburg Avenue
Cardiff by the Sea, CA 92007
mvanveen@ucsd.edu

2000 Mathematics Subject Classification: 11E25

June 20, 2011

Abstract

Let q be a positive squarefree integer. A prime p is said to be q-admissible if the equation $p = u^2 + qv^2$ has rational solutions u, v. Equivalently, p is q-admissible if there is a positive integer k such that $pk^2 \in \mathcal{N}$, where $\mathcal{N}$ is the set of norms of algebraic integers in $\mathbb{Q}(\sqrt{-q})$. Let $k(q)$ denote the smallest positive integer k such that $pk^2 \in \mathcal{N}$ for all q-admissible primes p. It is shown that $k(q)$ has subexponential but suprapolynomial growth in q, as $q \to \infty$.

Keywords: binary quadratic forms, principal genus theorem, Brauer-Siegel theorem, 4-rank of class group, imaginary quadratic fields, Gauss bound.

1 Introduction

Fix a positive squarefree integer q. A prime p is called q-admissible (or simply admissible) if the equation

$$p = u^2 + qv^2 \tag{1.1}$$

has rational solutions u, v. (For a thorough investigation of the case where $u, v \in \mathbb{Z}$, see Cox [2].) As an example with $q = 89$, the primes 2, 5, and 17 are each 89-admissible, since

$$\begin{aligned} 2 &= (19/15)^2 + 89(1/15)^2, \quad 5 = (18/15)^2 + 89(3/15)^2, \\ 17 &= (40/15)^2 + 89(5/15)^2. \end{aligned} \tag{1.2}$$

There are no such representations for the three 89-admissible primes 2, 5, 17 that share a common denominator smaller than 15, although each of 2, 5, 17 can be represented individually with a smaller denominator, e.g., $2 = (3/7)^2 + 89(1/7)^2$. Roughly this paper addresses the question: For a large q, what is the size of the minimal common denominator shared by all q-admissible primes?

Clearly a prime p is q-admissible if and only if $p = N(\gamma)$ for some $\gamma \in \mathbb{Q}(\sqrt{-q})$, where N denotes the norm. Equivalently, p is q-admissible if and only if there is a positive integer k (depending on p) such that

$$pk^2 \in \mathcal{N} := \{N(\alpha) : \alpha \in \mathcal{O}\}, \tag{1.3}$$

where $\mathcal{O}$ is the ring of algebraic integers in $\mathbb{Q}(\sqrt{-q})$.

Let $k(q)$ denote the smallest positive integer k such that (1.3) holds for all of the (infinitely many) q-admissible primes p. It is not difficult to show that $k(q)$ exists; see the proof of Theorem 3.1. The example (1.2) suggests that perhaps $k(89) = 15$, and this turns out to be the case, as can be easily shown via the algorithm illustrated in Section 6.

The primary purpose of this paper is to estimate the growth of $k(q)$ as $q \to \infty$. Theorem 3.1 shows that $k(q)$ has subexponential growth in q, while Theorem 5.2 shows that $k(q)$ has suprapolynomial growth in q. The proof of Theorem 5.2 depends on Theorem 4.7, which gives an upper bound for the prime power factors of $k(q)$.

As preparation, we discuss conditions equivalent to admissibility in Section 2. The notion of admissibility is extended to squarefree positive integers

m in (2.7), and Theorem 2.1 gives a formula for the number of q-admissible divisors of m. As corollaries of Theorem 2.1, we elementarily derive the formulas (2.20), (2.21) given by Rédei [8] for the 4-rank of the class group H of $\mathbb{Q}(\sqrt{-q})$; these formulas are useful for computing numerical values of $k(q)$, as is discussed in Section 6.

Tables of values of $k(q)$ and $k(-q)$ for $q < 6000$ with q either prime or twice a prime are currently available at [www.math.ucsd.edu/~revans/table1]. We remark that for $q > 1$, the results of Section 2–4 remain valid when the parameter q is replaced throughout by $-q$, provided that the ideal classes in H are regarded in the narrow sense and the denominator in the Gauss bound G (defined in Theorem 3.1) is changed from 3 to 8. We cannot similarly extend the results of Section 5, as we have no counterpart of Siegel's result (5.5) for real quadratic fields $\mathbb{Q}(\sqrt{q})$.

2 Conditions equivalent to admissibility

We begin by demonstrating (2.3) and (2.4) below, which are known characterizations of admissibility of a prime p. For the history, see Lemmermeyer [6], but note that only unramified p is discussed in [6, Section 7].

Let d denote the discriminant of the quadratic field $\mathbb{Q}(\sqrt{-q})$. Thus

$$d = \begin{cases} -q, & \text{if } \ q \equiv 3 \pmod 4 \\ -4q, & \text{if } \ q \equiv 1 \ \text{ or } \ 2 \pmod 4). \end{cases}$$

Write

$$d = d_1 d_2 \cdots d_t, \tag{2.1}$$

where the d_i are the prime discriminants. For any prime p, define the functions $\psi_i(p)$, $1 \le i \le t$, by

$$\psi_i(p) = \begin{cases} (d_i/p), & \text{if } \ p \nmid d_i \\ \\ (dd_i^{-1}/p), & \text{if } \ p | d_i, \end{cases} \tag{2.2}$$

where the symbols in (2.2) are Kronecker symbols. For non-inert p, the $\psi_i(p)$ are values of genus characters; see [5, p. 52].

The equivalence

$$p \text{ is admissible } \Leftrightarrow \ \psi_1(p) = \cdots = \psi_t(p) = 1 \tag{2.3}$$

is elementary. It follows directly from Legendre's Theorem [5, Theorem 1.7], after lengthy but straightforward computations. For example, for $q = 89$ with $d_1 = -4,\ d_2 = 89,\ d = d_1 d_2$, we have

$$\psi_1(7) = (-4/7) = -1, \quad \psi_1(2) = \psi_2(2) = (89/2) = 1;$$

thus, by (2.3), $p = 7$ is not 89-admissible but $p = 2$ is.

If p is admissible and unramified in $\mathcal{O}$, then $(d/p) = 1$ by (2.1)–(2.3). Thus no inert prime is admissible, and every admissible prime p satisfies $p = N(P)$ for some prime ideal P dividing (p). It follows from (2.3) and genus theory [5, Theorem 2.17] that $p = N(P)$ is admissible if and only if the ideal class $[P]$ is a square in the class group H of $\mathbb{Q}(\sqrt{-q})$. In other words,

$$\text{(2.4)} \qquad p \text{ is admissible } \Leftrightarrow \ p = N(P) \text{ with } [P] \in H^2.$$

We can prove (2.4) without genus theory, as follows. If p is admissible, then by (1.3), $N(Pk/\alpha) = 1$ for some $\alpha \in \mathcal{O}$. The simple "Satz 90 for ideals" [5, Prop. 2.5] thus yields $Pk/\alpha = E/\overline{E}$ for some ideal $E \subset \mathcal{O}$. Since $E\overline{E} = (N(E))$ is principal, $[P] = [E]^2 \in H^2$. Conversely, if $[P] = [E]^2$ for some ideal $E \subset \mathcal{O}$, then $P\overline{E}^2$ is a principal integral ideal (α). Thus, by taking norms, we see that (1.3) holds for $k = N(E)$, so p is admissible.

Consider the example $q = 37$. In [1, Cor. 8.3.3], it is proved that for prime p with $p \equiv 1 \pmod 4$ and $(p/37) = 1$, we have

$$\text{(2.5)} \qquad p = x^2 + 37y^2 \quad \text{for some } x, y \in \mathbb{Z}.$$

This can also be seen from (2.3) - (2.4) as follows. Since $(-4/p) = (37/p) = 1$, p is 37-admissible by (2.3); hence by (2.4), $p = N(P)$ with $[P] \in H^2$. Since $|H| = 2$, we have $|H^2| = 1$, so P is principal, and (2.5) follows.

By a similar argument, when $q = 21$ and p is prime with $p \equiv 1$, 25, or 37 (mod 84), we have

$$\text{(2.6)} \qquad p = x^2 + 21y^2 \quad \text{for some } x, y \in \mathbb{Z}.$$

This is because $p = N(P)$ is 21-admissible with $[P] \in H^2$, which implies that P is principal since H is an elementary abelian group of order 4. As a final example, when $q = 105$ and p is prime with $p \equiv 1$, 109, 121, 169, 289, or 361 (mod 420), we have $p = x^2 + 105y^2$ since H is elementary abelian of order 8.

A positive squarefree integer m is called q-admissible if

$$mk^2 \in \mathcal{N} \tag{2.7}$$

for some positive integer k (depending on m). The smallest positive integer k for which (2.7) holds for all q-admissible squarefree m turns out to be $k(q)$; see Remark 4.3.

We proceed to prove (2.10) and (2.12) below, which characterize the admissibility of squarefree m. In the sequel, suppose that m has the factorization

$$m = m_1 m_2 \cdots m_n \tag{2.8}$$

for distinct primes m_j, $1 \le j \le n$. (Interpret $m = 1$ when $n = 0$.) If m is admissible, then by (2.7), $(d/m_j) = 1$ for each prime m_j which is unramified in $\mathcal{O}$. (This is not immediately obvious in the case $m_j = 2$, but it follows from the fact that $x^2 + qy^2 \equiv 4 \pmod 8$ when $q \equiv 3 \pmod 8$ and x, y are odd.) Thus if m is admissible, no m_j can be inert. We assume from now on that the primes m_j in (2.8) are all non-inert; thus there are prime ideals M_j for which $N(M_j) = m_j$ and

$$m = N(M), \qquad M := M_1 M_2 \cdots M_n. \tag{2.9}$$

We have the following extension of (2.4):

$$m \quad \text{is admissible} \;\Leftrightarrow\; [M] \in H^2. \tag{2.10}$$

The proof of (2.10) is just like our proof of (2.4) above, except with M in place of P.

The function ψ_i in (2.2) has been defined on primes, but we can extend the definition by multiplicativity:

$$\psi_i(m) := \prod_{j=1}^{n} \psi_i(m_j). \tag{2.11}$$

Then we have the following extension of (2.3):

$$m \quad \text{is admissible} \;\Leftrightarrow\; \psi_1(m) = \psi_2(m) = \cdots = \psi_t(m) = 1. \tag{2.12}$$

Like (2.3), the equivalence (2.12) is elementary; it follows directly from Legendre's Theorem [5, Theorem 1.7]. However, the many cases involved make the proof quite tedious. A quicker (but less elementary) proof is based on the genus characters χ_i defined in [5, p. 53]. By the Principal Genus Theorem [5, p. 53], $[M] \in H^2$ if and only if $\chi_i([M]) = 1$ for all genus characters χ_i, $1 \leq i \leq t$. Since

$$\psi_i(m) = \chi_i([M]), \quad 1 \leq i \leq t, \tag{2.13}$$

we see that (2.12) follows from (2.10).

It is useful to reformulate (2.12) in terms of the t by n matrix

$$S(m, d) := ((\ \psi_i(m_j)\ ))_{1 \leq i \leq t,\ 1 \leq j \leq n}\ . \tag{2.14}$$

By (2.11) - (2.12), m is admissible if and only if the product of the n entries in each of the t rows of $S(m, d)$ equals 1. (The product of the t entries in each of the n columns always equals 1, by the Product Formula for genus characters [5, p. 53].)

An "additive" version of the matrix $S(m, d)$ is the t by n matrix

$$R(m, d) := ((a_{ij}))_{1 \leq i \leq t,\ 1 \leq j \leq n} \tag{2.15}$$

over the field of two elements, where the a_{ij} are defined (mod 2) by

$$\psi_i(m_j) = (-1)^{a_{ij}}. \tag{2.16}$$

We see that m is admissible if and only if the sum of the n columns of $R(m, d)$ vanishes (mod 2). Similarly, a divisor $m_{j_1} \cdots m_{j_\nu}$ of m is admissible if and only if the sum of columns $j_1, \ldots, j_\nu$ vanishes. Thus there is a one to one correspondence between the admissible divisors of m and the column vectors in the null space of $R(m, d)$. Since there are 2^η elements in the null space, where η denotes the nullity, we have proved the following theorem.

Theorem 2.1 *Let m be the product of n distinct non-inert primes. Then there are 2^η admissible divisors of m, where $\eta = n - \operatorname{rank} R(m, d)$.*

An interesting special case of Theorem 2.1 arises when $n = t$ and the t prime factors of $m = m_1 \cdots m_t$ are the ramified primes. In this special case, write

$$S(d) := S(m, d), \quad R(d) := R(m, d)\ . \tag{2.17}$$

By genus theory, as the sets $\{j_1, \ldots, j_\nu\}$ run through the 2^t subsets of $\{1, \ldots, t\}$, the ideal classes $[M_{j_1} \cdots M_{j_\nu}]$ run twice through the 2^{t-1} elements of the group $\{z \in H : z^2 = 1\}$. Thus those classes $[M_{j_1} \cdots M_{j_\nu}]$ that lie in H^2 run twice through the elements of the group

$$A := \{z \in H^2 : z^2 = 1\}. \tag{2.18}$$

By (2.10), $[M_{j_1} \cdots M_{j_\nu}] \in H^2$ if and only if $m_{j_1} \cdots m_{j_\nu}$ is admissible. Therefore the number of admissible divisors of m is $2|A|$. It thus follows from Theorem 2.1 that

$$|A| = 2^{t-1-\text{rank } R(d)} \ . \tag{2.19}$$

On the other hand, clearly $|A| = 2^r$, where r is the 4-rank of H (i.e., r is the number of cyclic factors of order $\equiv 0 \pmod 4$ in the direct product decomposition of H into cyclic groups). Therefore by (2.19), the 4-rank r satisfies

$$r := t - 1 - \text{rank } R(d) \ . \tag{2.20}$$

The formula (2.20) for the 4-rank of H is essentially a result of Rédei [8]. We've given a new proof of his result by treating it as a special case of Theorem 2.1.

A formula for the 4-rank r will be needed for computing the quantity w in (6.4). An alternative method of computing r is based on the following result of Rédei-Reichardt (see [3], [8]). Let N_d be the number of factorizations $d = \Delta_1\Delta_2$, where the Δ_i are quadratic field discriminants or 1, such that $(\Delta_1/p) = 1$ for every prime p dividing Δ_2 and $(\Delta_2/p) = 1$ for every prime p dividing Δ_1; then

$$N_d = 2^{r+1}. \tag{2.21}$$

(Here $d = \Delta_1\Delta_2$ and $d = \Delta_2\Delta_1$ are counted as *different* factorizations; if we were to identify them, then of course N_d would be cut in half.)

Formula (2.21) is a straightforward consequence of (2.20). To see this, let $m_1, \ldots, m_t$ be the ramified primes, and recall from (2.17) the definition of the t by t matrix

$$S(d) := ((\ \psi_i(m_j)\ )) \ . \tag{2.22}$$

The allowable choices of $\Delta_1 = d_{i_1} d_{i_2} \cdots d_{i_\nu}$ are in one to one correspondence with the subsets $\{i_1, \ldots, i_\nu\} \subset \{1, 2, \ldots, t\}$ for which the dot product of rows $i_1, i_2, \ldots, i_\nu$ of $S(d)$ equals $(1, 1, \ldots, 1)$. These subsets in turn are in one to one correspondence with the left null space of the t by t matrix $R(d)$ over the field of two elements. This null space has dimension $t - \text{rank } R(d) = r + 1$, by (2.20), so the null space has 2^{r+1} elements. This proves (2.21).

3 An upper bound for *k(q)*

The following theorem shows that $k(q)$ has subexponential growth in q.

Theorem 3.1 *Write*

$$G := \text{Floor}[(|d|/3)^{1/2}],$$

where d is the discriminant of $\mathbb{Q}(\sqrt{-q})$. *Then for any constant $c > 1$,*

$$k(q) < \exp(cG), \quad \textit{as} \quad |d| \to \infty.$$

Proof. Fix any ideal class in the class group H for $\mathbb{Q}(\sqrt{-q})$, and denote it by $[E]$, where E is an integral ideal in this class of minimal norm, i.e., $N(E) \leq N(F)$ for all integral ideals $F \in [E]$. By the Gauss bound [4, Theorem 2],

$$N(E) \leq G. \tag{3.1}$$

Let p be any admissible prime with $p = N(P)$, $[P] = [E]^2$. (There are infinitely many such p; see [7, p. 358].) As $P\overline{E}^2$ is principal, it follows upon taking norms that (1.3) holds for $k = N(E)$, i.e., $pN(E)^2 \in \mathcal{N}$.

Define

$$k_0 = \operatorname*{LCM}_{[E] \in H} \{N(E)\}, \tag{3.2}$$

where again E has minimal norm in each $[E]$. Note that k_0 depends only on q. We have $pk_0^2 \in \mathcal{N}$ for *every* admissible prime p, because

$$p\,N(E)^2 = N(\alpha) \in \mathcal{N} \Rightarrow \; pk_0^2 = N(\alpha k_0/N(E)) \in \mathcal{N}.$$

This proves that $k(q)$ exists and

$$k(q) \leq k_0. \tag{3.3}$$

By (3.1) – (3.3),

$$k(q) \leq \mathrm{LCM}\{1,2,\ldots,G\}. \tag{3.4}$$

As $G \to \infty$,

$$\mathrm{LCM}\{1,2,\ldots,G\} \leq \prod_{p\leq G} p^{\log_p G} = \prod_{p\leq G} G = \exp(G+o(G)), \tag{3.5}$$

by the Prime Number Theorem. The result now follows from (3.4) – (3.5). ■

Let $p = N(P),\ E \subset \mathcal{O}$. We observe that while $[P]=[E]^2$ implies $pk^2 \in \mathcal{N}$ for $k = N(E)$, it is not conversely true that $pk^2 \in \mathcal{N}$ implies $k = N(E)$ for some $E \subset \mathcal{O}$ with $[P]=[E]^2$; see Remark 4.1.

4 The prime factors of *k(q)*

For each admissible prime p, the definition of $k(q)$ yields

$$pk(q)^2 = N(\alpha_p) \quad \text{for some} \quad \alpha_p \in \mathcal{O}. \tag{4.1}$$

Suppose for the moment that $q \equiv 1$ or $2 \pmod 4$. Then $N(\alpha_p) = a_p^2 + qb_p^2$ for some integers a_p, b_p. If $k(q)$ were even, then by (4.1), a_p and b_p would have to be even for all p, which violates the minimality of $k(q)$. Therefore $k(q)$ is odd when $q \equiv 1$ or $2 \pmod 4$. Similarly one can show that $k(q)$ is odd when $q \equiv 3 \pmod 8$.

By (4.1), $-q$ is a square modulo each odd prime divisor of $k(q)$. Thus no prime divisor (odd or even) of $k(q)$ can be inert.

Consider the factorization

$$k(q) = \prod_{i=1}^{s} {v_i}^{f_i}, \quad f_i \geq 1, \tag{4.2}$$

where $v_1, \cdots, v_s$ are distinct primes. Since no v_i is inert, there are prime ideals V_i such that

$$v_i = N(V_i), \quad 1 \leq i \leq s. \tag{4.3}$$

Write

$$C = \prod_{i=1}^{s} V_i^{f_i},$$

with the interpretation $C = \mathcal{O}$ if $s = 0$. By (4.2) – (4.3), $N(C) = k(q)$.

For each admissible prime $p = N(P)$, we have $p\,N(C)^2 = N(\alpha_p)$ for some $\alpha_p \in \mathcal{O}$, by (4.1). We will always assume that P divides (α_p), otherwise replace α_p by $\overline{\alpha}_p$. Since $N(PC^2/\alpha_p) = 1$, we have

$$(\alpha_p)/P = C^2\overline{E}/E \tag{4.4}$$

for some ideal $E \subset \mathcal{O}$ depending on P. Since $(\alpha_p)/P$ is an integral ideal, we may stipulate that E divides C^2. Thus (4.4) can be written as

$$(\alpha_p)/P = \prod_{i=1}^{s} V_i^{2f_i - e_i}\overline{V}_i^{e_i}, \tag{4.5}$$

where the e_i are integers depending on P such that $0 \le e_i \le 2f_i$, and where $p = N(P)$ is admissible. Note that while α_p and the e_i depend on p (and on P), the f_i and V_i are independent of p.

Formula (4.5) is crucial in the sequel. Let us illustrate (4.5) for $q = 146$. To facilitate the computations, we first note that the class group H of $\mathbb{Q}(\sqrt{-146})$ is cyclic of order 16, generated by $[P_7]$, where $N(P_7) = 7$. We have

$$[P_7]^j = [P_{a(j)}], \quad 1 \le j \le 8,$$

where $a(1), a(2), \ldots, a(8)$ are the primes 7, 3, 29, 19, 5, 41, 13, 2, respectively, and $N(P_{a(j)}) = a(j)$, $1 \le j \le 8$. Note that the even powers of $[P_7]$ (i.e., square classes) correspond to the admissible primes 3, 19 , 41, 2.

The algorithm in Section 6 can be used to show that $k(146) = 35$; accordingly, in (4.5), take

$$V_1 = P_5,\ V_2 = P_7,\ f_1 = f_2 = 1,\ s = 2.$$

Then we have the following instances of (4.5):

$$\begin{array}{ll}
(\alpha_2)/P_2 = P_5^2\overline{P}_7^2\ , & \alpha_2 = 48 + \sqrt{-146} \\
(\alpha_3)/P_3 = P_5\overline{P}_5\overline{P}_7^2\ , & \alpha_3 = 5 + 5\sqrt{-146} \\
(\alpha_{19})/P_{19} = P_5^2P_7^2\ , & \alpha_{19} = 107 + 9\sqrt{-146} \\
(\alpha_{41})/P_{41} = P_5^2P_7\overline{P}_7\ , & \alpha_{41} = 147 + 14\sqrt{-146}\ .
\end{array}$$

Remark 4.1 The (integral) ideal on the right side of (4.5) has norm $k(q)^2$ and is in the class $[\overline{P}] \in H^2$. This ideal may not be a square; in fact there need not exist any ideal $B \subset \mathcal{O}$ of norm $k(q)$ with $B^2 \in [\overline{P}]$. For example, let $q = 89$ and consider the 89-admissible prime $p = 5 = N(P_5)$. Assume for the purpose of contradiction that there is an ideal $B \subset \mathcal{O}$ of norm $k(89) = 15$ such that $B^2 P_5$ is principal. Then $B^2 P_5 = (x + y\sqrt{-89})$ with $x, y \in \mathbb{Z}$, $x^2 + 89y^2 = 15^2 \cdot 5 = 1125$. This forces $x = \pm 18$, $y = \pm 3$. There is a first degree prime ideal P_3 dividing 3. Since P_3 divides x and y, P_3 must divide B. Thus P_3^2 divides $x + y\sqrt{-89}$. Since P_3^2 divides $x = \pm 18$, P_3^2 must therefore divide $3\sqrt{-89}$, which is absurd.

Remark 4.2 Let $p = N(P)$ and $p' = N(P')$ be primes for which $[P'] = [P]^{\pm 1}$. We say that the primes p and p' are *equivalent.* This is easily seen to give an equivalence relation on the set of non-inert primes. Suppose that $pk^2 = N(\alpha)$ for some $\alpha \in \mathcal{O}$. Then we claim that (for the same k) $p'k^2 = N(\beta)$ for some $\beta \in \mathcal{O}$. To see this, assume that $P|(\alpha)$ (otherwise replace α by $\overline{\alpha}$) and note that $N(Pk/\alpha) = 1$, so $Pk/\alpha = \overline{E}/E$ for some ideal $E \subset \mathcal{O}$. Thus $P(kE/\overline{E}) = (\alpha)$. Since $P|(\alpha)$, we have $kE/\overline{E} \subset \mathcal{O}$. Since $[P'] = [P]^{\pm 1}$, it follows that $P'(kE/\overline{E})$ or $P'(k\overline{E}/E)$ is a principal integral ideal (β), and the claim follows by taking norms. This result shows that for a given k, one can check if (1.3) holds for all admissible primes p without having to check more than one prime p from each equivalence class.

Remark 4.3 Consider any squarefree admissible m with $m = N(M)$ as in (2.9). We can write $[M] = [P]$ for some first degree prime ideal P (see [7, p. 358]), and $p = N(P)$ must be admissible by (2.4) and (2.10). Hence the argument of Remark 4.2 (with m in place of p') shows that for every admissible squarefree m,

$$mk(q)^2 = N(\alpha_m) \quad \text{for some} \quad \alpha_m \in \mathcal{O}.$$

For example, when $q = 146$, $k(q) = 35$, we have

$$\begin{aligned} 91\,k(q)^2 &= 71^2 + 146 \cdot 27^2, \\ 265\,k(q)^2 &= 259^2 + 146 \cdot 42^2. \end{aligned}$$

for the q-admissible integers $m = 91$ and $m = 265$.

Remark 4.4 Let V be a prime ideal dividing $(k(q))$. Lemma 4.5 below shows V has minimal norm in $[V]$, by which we mean V has minimal norm among all the integral ideals in the class $[V]$. Let $k'(q)$ be a (not necessarily minimal) positive integer such that $pk'(q)^2 \in \mathcal{N}$ for all q-admissible primes p. Of course $k'(q) \geq k(q)$, with equality if and only if $k'(q)$ is minimal. Suppose that for each prime ideal V' dividing $(k'(q))$, V' has minimal norm in $[V']$. Is this supposition enough to force $k'(q)$ to equal $k(q)$? The answer is no. For example, let $q = 47$. We have

$$2 \cdot 4^2 = N((9 + \sqrt{-47})/2)$$

and

$$3 \cdot 4^2 = N(1 + \sqrt{-47}).$$

The algorithm in Section 6 shows that for a given k, if $pk^2 \in \mathcal{N}$ for each of the two primes p in $L := \{2, 3\}$, then $pk^2 \in \mathcal{N}$ for *all* 47-admissible primes p. From this and the two identities above, it is easily checked that $k(47) = 4$. Since also

$$2 \cdot 9^2 = N(15 + 3\sqrt{-47})/2)$$

and

$$3 \cdot 9^2 = N(14^2 + \sqrt{-47}),$$

we may take $k'(47) = 9$. Then for each prime ideal V' dividing $(k'(47))$, V' has norm 3 and the class $[V']$ contains no integral ideal of norm 1 or 2, so V' has minimal norm in $[V']$.

Lemma 4.5 *Let $V_1, \ldots, V_s$ be as in (4.3). Then for each i, V_i has minimal norm among all integral ideals in the class $[V_i]$.*

Proof. Suppose for the purpose of contradiction that W_1 is an integral ideal in $[V_1]$ with

$$N(W_1) < N(V_1). \tag{4.6}$$

Define $W_i := V_i$ for $i > 1$. For each P with $p = N(P)$ admissible, consider the integral ideal

$$Y_P = \prod_{i=1}^{s} W_i^{2f_i - e_i}\ \overline{W}_i^{e_i} \tag{4.7}$$

where $e_1, \ldots, e_s$ are as in (4.5). We have $N(Y_P) = j(q)^2$, where

$$j(q) := \prod_{i=1}^{s} N(W_i)^{f_i} < \prod_{i=1}^{s} N(V_i)^{f_i} = \prod_{i=1}^{s} v_i^{f_i} = k(q), \tag{4.8}$$

by (4.6) and (4.2). Note that $j(q)$ is independent of p. Since $[W_1] = [V_1]$, it follows from (4.5) that PY_P is principal. Hence, since Y_P is integral, $PY_P = (\beta_P)$ for some $\beta_P \in \mathcal{O}$. Taking norms, we see that $pj(q)^2 \in \mathcal{N}$ for each admissible p; thus (4.8) contradicts the minimality of $k(q)$. ∎

The following theorem shows that $k(q)$ has only "small" prime factors. Recall that $G := \text{Floor}[(|d|/3)^{1/2}]$.

Theorem 4.6 *For each prime v_i dividing $k(q)$, we have $v_i \leq G$.*

Proof. For each i, Lemma 4.5 and the Gauss bound yield $v_i = N(V_i) \leq G$. ∎

For $q = 4162$, e.g., $k(q) = 22747 = 23^2 \cdot 43$ and the prime factors 23, 43 are less than $G = 74$. On the other hand, some prime power factors of $k(q)$ may exceed G. When $q = 4162$, e.g., $23^2 = 529 > G = 74$. However, the following theorem shows that no prime power factor of $k(q)$ can exceed G^2. This theorem will be applied in Section 5.

Theorem 4.7 *For each prime power $v_i^{f_i}$ dividing $k(q)$, we have $v_i^{f_i} \leq G^2$.*

Proof. Assume for the purpose of contradiction that $v_1^{f_1} > G^2$. Then $v_1^c > G$, where $c := \text{Ceiling}(f_1/2)$. Choose an integral ideal A of smallest norm in the ideal class $[V_1^c]$. By the Gauss bound,

$$N(A) \leq G < v_1^c = N(V_1^c). \tag{4.9}$$

For each P with $p = N(P)$ admissible, let $e_1, \ldots, e_s$ be as in (4.5), and define an ideal B_P by

$$B_P := \begin{cases} A^2 V_1^{2f_1 - e_1 - 2c}\, \overline{V}_1^{e_1}, & \text{if } f_1 > e_1 \\ \overline{A}^2 V_1^{2f_1 - e_1}\, \overline{V}_1^{e_1 - 2c}, & \text{if } e_1 > f_1 \\ A\overline{A} V_1^{f_1 - c}\, \overline{V}_1^{f_1 - c}, & \text{if } e_1 = f_1 \ . \end{cases} \tag{4.10}$$

Note that the ideal B_P is integral, since $2f_1 - e_1 - 2c \geq 0$ when $f_1 > e_1$, and $e_1 - 2c \geq 0$ when $e_1 > f_1$. Consider the integral ideal

$$X_P = B_P \prod_{i=2}^{s} V_i^{2f_i - e_i}\, \overline{V}_i^{e_i}. \tag{4.11}$$

We have $N(X_P) = \ell(q)^2$, where

$$\ell(q) := N(A)N(V_1)^{f_1-c}\prod_{i=2}^{s} N(V_i)^{f_i} < \prod_{i=1}^{s} N(V_i)^{f_i} = k(q), \tag{4.12}$$

by (4.9) and (4.2). Note that $\ell(q)$ does not depend on p. Since $[A] = [V_1^c]$, we have $[X_P] = \prod_{i=1}^{s}[V_i]^{2f_i-2e_i}$ by (4.10) – (4.11). It follows from (4.5) that PX_P is principal, so since X_P is integral, $PX_P = (\gamma_P)$ for some $\gamma_P \in \mathcal{O}$. Taking norms, we see that $p\ell(q)^2 \in \mathcal{N}$ for each admissible p; thus (4.12) contradicts the minimality of $k(q)$. ■

5 A lower bound for *k(q)*

Recall from (4.2) the prime factorization

$$k(q) = \prod_{i=1}^{s} v_i^{f_i}, \quad f_i \geq 1, \tag{5.1}$$

and recall from Theorem 3.1 the definition $G := \mathrm{Floor}[(|d|/3)^{1/2}]$. The next theorem shows that s (the number of distinct prime factors of $k(q)$) tends to infinity as $q \to \infty$ (so in particular $k(q) \to \infty$).

Theorem 5.1 *Let s be as in (5.1). Then for any constant $c < 1$,*

$$s > \frac{c \log G}{\log\log G}, \quad \text{as } d \to -\infty.$$

Proof. By (4.5), for each first degree prime ideal P with $[P] \in H^2$,

$$[P] = \prod_{i=1}^{s}[V_i]^{2f_i-2e_i} \tag{5.2}$$

for some e_i (depending on P) such that $0 \leq e_i \leq 2f_i$. Since every element of H^2 has the form $[P]$ for some first degree prime ideal P [7, p. 358], there must exist at least $|H^2|$ *distinct* integer vectors $(e_1, e_2, \ldots, e_s)$ with $0 \le e_i \le 2f_i$. Therefore,

$$\prod_{i=1}^{s}(2f_i+1) \ge |H^2|.$$

Let $h = |H|$ be the class number of $\mathbb{Q}(\sqrt{-q})$. By genus theory [5, Theorem 2.11], we have $|H^2| = h/2^{t-1}$. Thus

$$\prod_{i=1}^{s}(2f_i+1) \ge h/2^{t-1}. \tag{5.3}$$

By the Prime Number Theorem, the product of the first t primes is $\exp(t\log t + o(t\log t))$, as $t \to \infty$. Since $|d| = |d_1|\cdots|d_t|$ is at least as large as the product of the first t primes, we have $\log|d| \ge t\log t + o(t\log t)$. Thus

$$t = o(\log|d|), \quad \text{as } |d| \to \infty. \tag{5.4}$$

The Brauer-Siegel Theorem [7, p. 446] shows that for any $\varepsilon > 0$,

$$h > |d|^{1/2-\varepsilon}, \quad \text{as } d \to -\infty. \tag{5.5}$$

Combining (5.3) – (5.5), we have for any $\varepsilon > 0$,

$$\prod_{i=1}^{s}(2f_i+1) > |d|^{1/2-\varepsilon}, \quad \text{as } d \to -\infty. \tag{5.6}$$

Thus for any constant $c < 1$,

$$\prod_{i=1}^{s}(2f_i+1) > G^c, \quad \text{as } d \to -\infty. \tag{5.7}$$

Since $v_i^{f_i} \le G^2$ by Theorem 4.7,

$$f_i \log v_i \le 2\log G \quad (i = 1, 2, \ldots, s). \tag{5.8}$$

Thus

$$2f_i + 1 < 9\log G \quad (i = 1, 2, \ldots, s). \tag{5.9}$$

Taking logs in (5.7), we thereby obtain

$$c \log G < \sum_{i=1}^{s} \log(2f_i + 1) < s(\log 9 + \log\log G), \tag{5.10}$$

and the result follows. ∎

We remark that there are many values of q for which equality holds in (5.3). For example, if $q = 3623$, then $k(q) = 384 = 2^7 \cdot 3$, so

$$\prod_{i=1}^{s}(2f_i + 1) = 15 \cdot 3 = 45 = h = h/2^{t-1};$$

if $q = 4373$, then $k(q) = 1323 = 3^3 \cdot 7^2$, so

$$\prod_{i=1}^{s}(2f_i + 1) = 7 \cdot 5 = 35 = h/2 = h/2^{t-1};$$

if $q = 4502$, then $k(q) = 741 = 3 \cdot 13 \cdot 19$, so

$$\prod_{i=1}^{s}(2f_i + 1) = 3 \cdot 3 \cdot 3 = 27 = h/2 = h/2^{t-1}.$$

The next theorem shows that $k(q)$ grows faster than any polynomial in q, as $q \to \infty$.

Theorem 5.2 *For any positive constant $\alpha < 1/\log 3$,*

$$k(q) > G^{\alpha \log s} \quad \textit{as} \quad d \to -\infty,$$

and so (by Theorem 5.1),

$$k(q) > G^{\alpha \log\log G} \quad \textit{as} \quad d \to -\infty.$$

Proof. By (5.1) and the first inequality in (5.10), it suffices to prove that as $d \to -\infty$,

$$\alpha(\log s) \sum_{i=1}^{s} \log(2f_i + 1) < \sum_{i=1}^{s} f_i \log v_i. \tag{5.11}$$

Fix a constant β such that

$$\alpha \log 3 < \beta < 1.$$

The sum on the right of (5.11) equals $R_1 + R_2$, where

$$R_1 := \sum_{v_i \le s^\beta} f_i \log v_i, \quad R_2 := \sum_{v_i > s^\beta} f_i \log v_i.$$

The expression on the left of (5.11) equals $L_1 + L_2$, where

$$L_1 := \alpha(\log s) \sum_{v_i \le s^\beta} \log(2f_i + 1), \quad L_2 := \alpha(\log s) \sum_{v_i > s^\beta} \log(2f_i + 1).$$

Since (5.11) is equivalent to

$$(R_2 - L_2) + R_1 > L_1,$$

it suffices to prove that as $d \to -\infty$,

$$L_1 < s \tag{5.12}$$

and for some positive constant γ,

$$R_2 - L_2 > \gamma s \log s. \tag{5.13}$$

Let $|d|$ be large. By (5.9), $L_1 < \alpha(\log s)\log(9\log G)s^\beta$. By Theorem 5.1, $\log(9\log G) < 2(\log s)$, so (5.12) follows. It remains to prove (5.13). We have

$$R_2 = \sum_{v_i > s^\beta} f_i \log v_i > \beta(\log s) \sum_{v_i > s^\beta} f_i,$$

so

$$R_2 - L_2 > \beta(\log s) \sum_{v_i > s^\beta} (f_i - \frac{\alpha}{\beta}\log(2f_i + 1)). \tag{5.14}$$

Since $f - \frac{\alpha}{\beta}\log(2f+1)$ is an increasing function of f for $f \ge 1$, we have for each i,

$$f_i - \frac{\alpha}{\beta}\log(2f_i + 1) \ge \delta := 1 - \frac{\alpha}{\beta}\log 3 > 0,$$

by definition of β. Thus (5.14) gives

$$R_2 - L_2 > \beta\delta(\log s)(s - s^\beta) > (\beta\delta/2)s\log s,$$

which proves (5.13). ∎

6 Computing numerical values of *k(q)*

We present here an example illustrating the computation of $k(146)$, elaborating where needed on the procedure for general q. Let $q = 146$, so that $\mathbb{Q}(\sqrt{-q})$ has discriminant $d = -584 = d_1 d_2$ with $d_1 = -8,\ d_2 = 73$. As will be explained at the end of this section, $k(146)$ is the smallest positive integer k for which the four elements of the set $\{2k^2, 3k^2, 19k^2, 41k^2\}$ each have the form $x^2 + 146y^2 \ \ (x, y \in \mathbb{Z})$. The smallest such k could be discovered by successively checking $\{2k^2, 3k^2, 19k^2, 41k^2\}$ for each of the candidates $k = 1, 2, 3, \ldots,$ but the search for $k(146)$ can be expedited by skipping certain k based on results from Section 4. For example, by the first paragraph of Section 4, we could skip those k divisible by inert primes $11, 17, 23, \ldots,$ and we could skip those k divisible by 2 (since $k(146)$ is odd). We could also skip those k divisible by the any of the primes $17, 19, 23, 29, 31, \ldots$, because by Theorem 4.6, every prime factor of $k(146)$ is $\leq G = 13$.

For some w to be determined below, H^2 can be expressed as a union of $w + 1$ disjoint sets of the form

$$\{[P_{p_i}], [\overline{P}_{p_i}]\}, \quad 0 \leq i \leq w, \tag{6.1}$$

where $p_0, p_1, \ldots, p_w$ are distinct admissible primes with $p_i = N(P_{p_i})$, and P_{p_0} is principal, i.e.,

$$[P_{p_0}] = [\overline{P}_{p_0}] = [1].$$

Recalling the definition of equivalence in Remark 4.2, we see that $\{p_0, p_1, \ldots, p_w\}$ is a full set of pairwise inequivalent admissible primes. Thus, by Remark 4.2, one can determine $k(q)$ just by testing (1.3) for each of these $w + 1$ primes p_i. However, the prime $p_0 \in \mathcal{N}$ does not aid in the determination because $p_0 k^2 \in \mathcal{N}$ for *every* integer k. Thus, for the determination of $k(q)$, it suffices to consider the w primes in the set

$$L = L(q) = \{p_1, \ldots, p_w\}. \tag{6.2}$$

We next show how to determine w numerically. Clearly $|H^2| = 2a + b$, where a is the number of classes $\mathcal{C} \in H^2$ with $\mathcal{C}^2 \neq [1]$ and b is the number of classes $\mathcal{C} \in H^2$ with $\mathcal{C}^2 = [1]$. Since $w = a + b - 1$,

$$w = |H^2|/2 - 1 + b/2 = h/2^t - 1 + b/2. \tag{6.3}$$

Now, $b = 2^r$, where r is the 4-rank of H, i.e., r is the number of nontrivial cyclic direct factors in the 2-part of H^2. Thus

$$w = h/2^t - 1 + 2^{r-1}. \tag{6.4}$$

We can compute r from (2.20) or (2.21). When q is an odd prime, for example,

$$r = \begin{cases} 0, & \text{if } \; q \equiv 3, \; 5, \; \text{or } 7 \pmod 8 \\ 1, & \text{if } \; q \equiv 1 \pmod 8). \end{cases} \tag{6.5}$$

As another example, when $q = 2u$ for odd prime u,

$$r = \begin{cases} 0, & \text{if } \; u \equiv 3 \text{ or } 5 \pmod 8 \\ 1, & \text{if } \; u \equiv 1 \text{ or } 7 \pmod 8). \end{cases} \tag{6.6}$$

(On the other hand, when $-q$ is either an odd prime or twice an odd prime, then $r = 0$ except when $q \equiv -2 \pmod{16}$, whereupon $r = 1$.) For $q = 146$, we have $r = 1$ by (6.6), so that by (6.4), $w = h/2^t = 16/4 = 4$. This shows that the set $L(146)$ in (6.2) contains four primes.

It is not difficult to see that non-inert primes p, p' are equivalent if and only if $pp' \in \mathcal{N}$. Thus the w members $p_1, \ldots, p_w$ of the set $L(q)$ in (6.2) can be chosen numerically by the following procedure. Let p_1 be the smallest admissible prime with $p_1 \notin \mathcal{N}$. Let p_2 be the smallest admissible prime $> p_1$ such that $p_2 \notin \mathcal{N}$ and such that $pp_2 \notin \mathcal{N}$ for all admissible primes $p < p_2$. Let p_3 be the smallest admissible prime $> p_2$ such that $p_3 \notin \mathcal{N}$ and such that $pp_3 \notin \mathcal{N}$ for all admissible primes $p < p_3$. Continue this way until exactly w primes p_i are chosen, where w is computed from (6.4). This yields the desired set $L(q)$. In the special case $q = 146$, the first four admissible primes are $p_1 = 2, \; p_2 = 3, \; p_3 = 19, \; p_4 = 41$. These four primes already satisfy all the conditions of the procedure, e.g., for every admissible prime $p < 41, \; 41p$ fails to have the form $x^2 + 146y^2$. This shows that we can take $L(146) = \{2, 3, 19, 41\}$.

References

[1] B. Berndt, R. Evans, and K. Williams, Gauss and Jacobi sums, Wiley- Interscience, N.Y., 1998.

[2] D. A. Cox, Primes of the form $x^2 + ny^2$, Fermat, class field theory, and complex multiplication, Wiley - Interscience, N.Y., 1989.

[3] H. Kisilevsky, The Rédei-Reichardt theorem - a new proof, Selected topics on ternary forms and norms, Olga Taussky, ed., (Sem. Number Theory, California Inst. Tech., Pasadena, 1974/75), Paper No. 6, 4pp., California Inst. Tech., Pasadena, 1976.

[4] F. Lemmermeyer, Gauss bounds of quadratic extensions, Publ. Math. Debrecen **50**(1997), 365-368.

[5] F. Lemmermeyer, Reciprocity Laws, From Euler to Eisenstein, Springer-Verlag, Berlin, 2000.

[6] F. Lemmermeyer, The development of the principal genus theorem, to appear, Springer-Verlag, Berlin, 2005.

[7] W. Narkiewicz, Elementary and analytic theory of algebraic numbers, Second ed., Springer-Verlag, Berlin, 1990.

[8] L. Rédei, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, J. Reine Angew. Math. 171(1934), 55-60.