#A21 INTEGERS 10 (2010), 257-264

LOWER BOUNDS FOR THE PRINCIPAL GENUS OF DEFINITE BINARY QUADRATIC FORMS

Kimberly Hopkins
Department of Mathematics, University of Texas at Austin, Austin, Texas, USA
khopkins@math.utexas.edu

Jeffrey Stopple
Department of Mathematics, University of California, Santa Barbara, Santa Barbara, California
stopple@math.ucsb.edu

Received: 4/22/09, Accepted: 2/15/10, Published: 5/24/10

Abstract

We apply Tatuzawa's version of Siegel's theorem to derive two lower bounds on the size of the principal genus of positive definite binary quadratic forms.

1. Introduction

Suppose $-D < 0$ is a fundamental discriminant. By genus theory we have an exact sequence for the class group $\mathcal{C}(-D)$ of positive definite binary quadratic forms:

$$\mathcal{P}(-D) \overset{\text{def.}}{=} \mathcal{C}(-D)^2 \hookrightarrow \mathcal{C}(-D) \twoheadrightarrow \mathcal{C}(-D)/\mathcal{C}(-D)^2 \simeq (\mathbb{Z}/2)^{g-1},$$

where D is the product of g primary discriminants (i.e., D has g distinct prime factors). Let $p(-D)$ denote the cardinality of the principal genus $\mathcal{P}(-D)$. The genera of forms are the cosets of $\mathcal{C}(-D)$ modulo the principal genus, and thus $p(-D)$ is the number of classes of forms in each genus. The study of this invariant of the class group is as old as the study of the class number $h(-D)$ itself. Indeed, Gauss wrote in [3, Art. 303]

> . . . Further, the series of [discriminants] corresponding to the same given classification (i.e. the given number of both genera and classes) always seems to terminate with a finite number . . . However, *rigorous* proofs of these observations seem to be very difficult.

Theorems about $h(-D)$ have usually been closely followed with an analogous result for $p(-D)$. When Heilbronn [4] showed that $h(-D) \to \infty$ as $D \to \infty$, Chowla [1] showed that $p(-D) \to \infty$ as $D \to \infty$. An elegant proof of Chowla's theorem is given by Narkiewicz in [8, Prop 8.8 p. 458].

Similarly, the Heilbronn-Linfoot result [5] that $h(-D) > 1$ if $D > 163$, with at most one possible exception was matched by Weinberger's result [14] that $p(-D) > 1$ if $D > 5460$ with at most one possible exception. On the other hand, Oesterlé's [9] exposition of the Goldfeld-Gross-Zagier bound for $h(-D)$ already contains the observation that the result was not strong enough to give any information about $p(-D)$.

In [13] Tatuzawa proved a version of Siegel's theorem: for every ε there is an explicit constant $C(\varepsilon)$ so that

$$h(-D) > C(\varepsilon)D^{1/2-\varepsilon}$$

with at most one exceptional discriminant $-D$. This result has never been adapted to the study of the principal genus. It is easily done; the proofs are not difficult so it is worthwhile filling this gap in the literature. We present two versions. The first version contains a transcendental function (the Lambert W function discussed below). The second version gives, for each $n \geq 4$, a bound which involves only elementary functions. For each fixed n the second version is stronger on an interval $I = I(n)$ of D , but the first is stronger as $D \to \infty$. The second version has the added advantage that it is easily computable. (N.B. The constants in Tatuzawa's result have been improved in [6] and [7]; these could be applied at the expense of slightly more complicated statements.)

Notation We will always assume that $g \geq 2$, for if $g = 1$ then $-D = -4, -8$, or $-q$ with $q \equiv 3 \bmod 4$ a prime. In this last case $p(-q) = h(-q)$ and Tatuzawa's theorem [13] applies directly.

2. First Version

Lemma 1. *If $g \geq 2$,*

$$\log(D) > g\log(g).$$

Proof. Factor D as $q_1, \ldots q_g$ where the q_i are (absolute values) of primary discriminants, i.e. 4, 8, or odd primes. Let p_i denote the ith prime number, so we have

$$\log(D) = \sum_{i=1}^{g} \log(q_i) \geq \sum_{i=1}^{g} \log(p_i) \stackrel{\text{def.}}{=} \theta(p_g). \tag{1}$$

By [11, (3.16) and (3.11)], we know that Chebyshev's function θ satisfies $\theta(x) > x(1 - 1/\log(x))$ if $x > 41$, and that

$$p_g > g(\log(g) + \log(\log(g)) - 3/2).$$

After substituting $x = p_g$ and a little calculation, this gives $\theta(p_g) > g\log(g)$ as long as $p_g > 41$, i.e. $g > 13$. For $g = 2, \ldots, 13$, one can easily verify the inequality directly. $\square$

Let $W(x)$ denote the Lambert W-function, that is, the inverse function of $f(w) = w\exp(w)$ (see [2], [10, p. 146 and p. 348, ex 209]). For $x \geq 0$ it is positive, increasing, and concave down. The Lambert W-function is also sometimes called the product log, and is implemented as `ProductLog` in *Mathematica*.

Theorem 2. *If* $0 < \varepsilon < 1/2$ *and* $D > \max(\exp(1/\varepsilon), \exp(11.2))$*, then with at most one exception*

$$p(-D) > \frac{1.31}{\pi}\varepsilon D^{1/2-\varepsilon-\log(2)/W(\log(D))}.$$

Proof. Tatuzawa's theorem [13], says that with at most one exception

$$\frac{\pi \cdot h(-D)}{\sqrt{D}} = L(1, \chi_{-D}) > .655\varepsilon D^{-\varepsilon}, \tag{2}$$

and thus

$$p(-D) = \frac{2h(-D)}{2^g} > \frac{1.31\varepsilon \cdot D^{1/2-\varepsilon}}{\pi \cdot 2^g}.$$

The relation $\log(D) > g\log(g)$ is equivalent to

$$\log(D) > \exp(\log(g))\log(g).$$

Thus applying the increasing function W gives, by definition of W

$$W(\log(D)) > \log(g),$$

and applying the exponential gives

$$\exp(W(\log(D)) > g.$$

The left-hand side above is equal to $\log(D)/W(\log(D))$ by the definition of W. Thus,

$$-\log(D)/W(\log(D)) < -g,$$

$$D^{-\log(2)/W(\log(D))} = 2^{-\log(D)/W(\log(D))} < 2^{-g},$$

and the theorem follows. □

Remark 3. Our estimate arises from the bound $\log(D) > g\log(g)$, which is nearly optimal. That is, for every g, there exists a fundamental discriminant (although not necessarily negative) of the form

$$D_g \stackrel{\text{def.}}{=} \pm 3 \cdot 4 \cdot 5 \cdot 7 \ldots p_g,$$

and

$$\log|D_g| = \theta(p_g) + \log(2).$$

From the Prime Number Theorem we know $\theta(p_g) \sim p_g$, so

$$\log|D_g| \sim p_g + \log(2)$$

while [11, 3.13] shows $p_g < g(\log(g) + \log(\log(g))$ for $g \geq 6$.

3. Second Version

Theorem 4. *Let $n \geq 4$ be any natural number. If $0 < \varepsilon < 1/2$ and $D > \max(\exp(1/\varepsilon), \exp(11.2))$, then with at most one exception*

$$p(-D) > \frac{1.31\varepsilon}{\pi} \cdot \frac{D^{1/2-\varepsilon-1/n}}{f(n)},$$

where

$$f(n) = \exp\left[(\pi(2^n) - 1/n)\log 2 - \theta(2^n)/n\right];$$

here π is the prime counting function and θ is the Chebyshev function.

Proof. First observe

$$f(n) = \frac{2^{\pi(2^n)}}{2^{1/n}\prod_{\text{primes } p<2^n} p^{1/n}}.$$

From Tatuzawa's Theorem (2), it suffices to show $2^g \leq f(n)D^{1/n}$. Suppose first that D is not $\equiv 0 \pmod 8$.

Let $S = \{4, \text{odd primes} < 2^n\}$, so $|S| = \pi(2^n)$. Factor D as $q_1 \cdots q_g$ where q_i are (absolute values) of coprime primary discriminants, that is, 4 or odd primes, and satisfy $q_i < q_j$ for $i < j$. Then, for some $0 \leq m \leq g$, we have $q_1, \ldots, q_m \in S$ and $q_{m+1}, \ldots, q_g \notin S$, and thus $2^n < q_i$ for $i = m+1, \ldots, g$. This implies

$$\begin{aligned} 2^{gn} &= \underbrace{2^n \cdots 2^n}_{m} \cdot \underbrace{2^n \cdots 2^n}_{g-m} \leq 2^{mn}\ q_{m+1}q_{m+2}\cdots q_g \\ &= \frac{2^{mn}}{q_1\cdots q_m} D \leq \frac{2^{|S|\cdot n}}{\prod_{q\in S} q} \cdot D \end{aligned}$$

as we have included in the denominator the remaining elements of S (each of which is $\leq 2^n$). The above is

$$= \frac{2^{\pi(2^n)\cdot n}}{2\prod_{\text{primes } p<2^n} p} \cdot D = f(n)^n \cdot D.$$

This proves the theorem when D is not $\equiv 0 \bmod 8$. In the remaining case, apply the above argument to $D' = D/2$; so

$$2^{gn} \leq f(n)^n D' < f(n)^n D.$$

$\square$

Examples. If $0 < \varepsilon < 1/2$ and $D > \max(\exp(1/\varepsilon), \exp(11.2))$, then with at most one exception, Theorem 4 implies

$$p(-D) > 0.10199 \cdot \varepsilon \cdot D^{1/4-\varepsilon} \quad (n = 4)$$

$$p(-D) > 0.0426 \cdot \varepsilon \cdot D^{3/10-\varepsilon} \quad (n = 5)$$

$$p(-D) > 0.01249 \cdot \varepsilon \cdot D^{1/3-\varepsilon} \quad (n = 6)$$

$$p(-D) > 0.00188 \cdot \varepsilon \cdot D^{5/14-\varepsilon} \quad (n = 7)$$

4. Comparison of the Two Theorems

How do the two theorems compare? Canceling the terms which are the same in both, we seek inequalities relating

$$D^{-\log 2/W(\log D)} \quad \text{v.} \quad \frac{D^{-1/n}}{f(n)}.$$

Theorem 5. *For every n, there is a range of D where the bound from Theorem 4 is better than the bound from Theorem 2. However, for any fixed n the bound from Theorem 2 is eventually better as D increases.*

For fixed n, the first statement of Theorem 5 is equivalent to proving

$$D^{\log(2)/W(\log(D))-1/n} \geq f(n)$$

on a non-empty compact interval of the D axis. Taking logarithms, it suffices to show:

Lemma 6. *Let $n \geq 4$. Then*

$$x\left(\frac{\log 2}{W(x)} - \frac{1}{n}\right) \geq \log f(n)$$

on some non-empty compact interval of positive real numbers x.

Proof. Let $g(n,x) = x\,(\log 2/W(x) - 1/n)$. Then

$$\frac{\partial g}{\partial x} = \frac{\log 2}{W(x)+1} - \frac{1}{n} \qquad \text{and} \qquad \frac{\partial^2 g}{\partial x^2} = \frac{-\log 2 \cdot W(x)}{x(W(x)+1)^3}.$$

This shows g is concave down on the positive real numbers and has a maximum at

$$x = 2^n(n\log 2 - 1)/e.$$

Because of the concavity, all we need to do is show that $g(n,x) > \log f(n)$ at *some* x. The maximum point is slightly ugly so instead we let $x_0 = 2^n n \log 2/e$.

Using $W(x) \sim \log x - \log\log x$, a short calculation shows

$$g(n,x_0) \sim \frac{1}{e}\cdot\frac{2^n}{n}.$$

By [12, 5.7)], a lower bound on Chebyshev's function is

$$\theta(t) > t\left(1 - \frac{1}{40\log t}\right), \quad t > 678407.$$

(Since we will take $t = 2^n$ this requires $n > 19$ which is not much of a restriction.) By [11, (3.4)], an upper bound on the prime counting function is

$$\pi(t) < \frac{t}{\log t - 3/2}, \quad t > e^{3/2}.$$

Hence $-\theta(2^n) < 2^n\,(1/(40n\log 2) - 1)$ and so

$$\begin{aligned}
\log f(n) &= \left(\pi(2^n) - \frac{1}{n}\right)\log 2 - \frac{\theta(2^n)}{n} \\
&< \left(\frac{2^n}{n\log 2 - 3/2} - \frac{1}{n}\right)\log 2 + \frac{2^n}{n}\left(\frac{1}{40n\log 2} - 1\right) \\
&\sim \frac{61}{40\log 2}\cdot\frac{2^n}{n^2}.
\end{aligned}$$

Comparing the two asymptotic bounds for g and $\log f$ respectively we see that

$$\frac{1}{e}\cdot\frac{2^n}{n} > \frac{61}{40\log 2}\cdot\frac{2^n}{n^2},$$

for $n \geq 6$; small n are treated by direct computation.[1] □

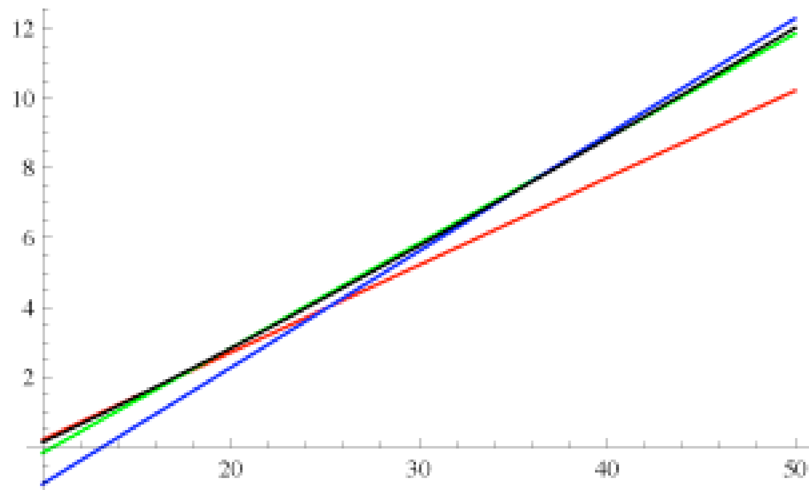

Figure 1: log-log plots of the bounds from Theorems 2 and 4

Figure 1 shows a log-log plot of the two lower bounds, omitting the contribution of the constants, which are the same in both, and the terms involving ε. That is, Theorem 4 gives for each n a lower bound $b(D)$ of the form

$$b(D) = C(n)\varepsilon D^{1/2-1/n-\varepsilon}, \quad \text{so}$$
$$\log(b(D)) = (1/2 - 1/n - \varepsilon)\log(D) + \log(C(n)) + \log(\varepsilon).$$

Observe that for fixed n and ε, this is linear in $\log(D)$, with the slope an increasing function of the parameter n. What is plotted is actually $(1/2 - 1/n)\log(D) + \log(C(n))$ as a function of $\log(D)$, and analogously for Theorem 2. In red, green, and blue are plotted the lower bounds from Theorem 4 for $n = 4$, 5, and 6 respectively. In black is plotted the lower bound from Theorem 2.

Examples. The choice $\varepsilon = 1/\log(5.6 \cdot 10^{10})$ in Theorem 2 shows that $p(-D) > 1$ for $D > 5.6 \cdot 10^{10}$ with at most one exception. (For comparison, Weinberger [14, Lemma 4] needed $D > 2 \cdot 10^{11}$ to get this lower bound.) And, $\varepsilon = 1/\log(3.5 \cdot 10^{14})$ in Theorem 2 gives $p(-D) > 10$ for $D > 3.5 \cdot 10^{14}$ with at most one exception. Finally, $n = 6$ and $\varepsilon = 1/\log(4.8 \cdot 10^{17})$ in Theorem 4 gives $p(-D) > 100$ for $D > 4.8 \cdot 10^{17}$ with at most one exception.

[1]The details of the asymptotics have been omitted for conciseness.

References

[1] S. Chowla, *An extension of Heilbronn's class-number theorem*, Quarterly J. Math., **5** (1934), 150-160.

[2] L. Euler, *De serie Lambertiana plurimisque eius insignibus proprietatibus*, Opera Omnia Ser. 1 Vol. 6, 350-369.

[3] C. F. Gauss, Disquisitiones Arithmeticae, Yale Univ. Press, 1966.

[4] H. Heilbronn, *On the class-number in imaginary quadratic fields*, Quarterly J. Math., **5** (1934), 304-307.

[5] H. Heilbronn and E. Linfoot, *On the imaginary quadratic corpora of class-number one*, Quarterly J. Math., **5** (1934), 293-301.

[6] J. Hoffstein, *On the Siegel-Tatuzawa theorem*, Acta Arith. **XXXVIII** (1980), 167-174.

[7] C.G. Ji and H.W. Lu, *Lower bound of real primitive L-function at* $s = 1$, Acta Arith. **111** (2004) no. 4, 405-409.

[8] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 2nd. ed. Springer-Verlag, 1990.

[9] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Sém. Bourbaki, vol. 1983/84, Astérisque, no. 121-122 (1985), 309-323.

[10] G. Pólya and G. Szegö, Aufgaben und Lehrstze der Analysis. Berlin, 1925. Reprinted as Problems and Theorems in Analysis I. Berlin: Springer-Verlag, 1998.

[11] J.B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math., **6** (1962), 64-94.

[12] J.B. Rosser and L. Schoenfeld, *Sharper bounds for the Chebyshev functions* $\theta(x)$ *and* $\psi(x)$, Math. Comp., **29** (1975), 243-369.

[13] T. Tatuzawa, *On a theorem of Siegel*, Jap. J. Math. **21** (1951), 163-178.

[14] P. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. **XXII**, 1973, 117-124.