MINIMAL HEIGHTS IN NUMBER FIELDS

DISSERTATION

Presented in Partial Fulfillment of the Requirements for
the Degree Doctor of Philosophy in the Graduate
School of the Ohio State University

By
Scott Arms, B.S., M.S.

The Ohio State University
2008

Dissertation Committee:
Professor Warren Sinnott, Advisor
Professor James Cogdell
Professor K. Alan Loper

Approved by
Advisor
Graduate Program in Mathematics
ABSTRACT

Minimal heights of bases for number fields $K$ over $\mathbb{Q}$ have been studied by Roy and Thunder, Masser, and Silverman, among others. The main results of this work focus on minimal heights of generator elements for number fields in general and quadratic number fields in particular. It is shown that the minimal height of a generator of an imaginary quadratic extension $\mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$ coincides with the minimal polynomial-height of the set of quadratic polynomials whose discriminant has squarefree-part (core) equal to $d$. This leads to a limit result concerning the size of the height of such a generator, using results of Ruppert. Invoking the Generalized Riemann Hypothesis in order to use an effective version of the Chebotarev Density Theorem allows for results of a non-limiting nature as well as a proof of a conjecture of Ruppert. In addition, the heights of algebraic integers in quadratic extensions are analyzed and it is shown that the usual dichotomy between real and imaginary quadratic extensions exists here while this is no longer present when one considers general quadratic algebraic numbers. A corollary of this is a characterization of which quadratic fields have algebraic integers achieving the minimal height of a generator. A further corollary is a basic characterization, in terms of heights, of which imaginary quadratic fields have class number 1, contingent upon the Generalized Riemann Hypothesis.
ACKNOWLEDGMENTS

I wish to thank my advisor, Professor Warren Sinnott, for his willingness to discuss all sorts of interesting problems with me in the process of finding a topic for this work and especially for his extreme generosity with his time all the way from Math H190 through finishing this project. His insights, experience, and constant desire to teach have been thoroughly appreciated. I have looked forward to our meetings to discuss mathematics (and whatever else) and will certainly miss them once I leave.

I would also like to thank my other committee members, Professor James Cogdell and Professor Alan Loper, for agreeing to serve on my committee. I was fortunate enough to be a student of each for multiple quarters during graduate school and their enthusiasm for teaching always made me anxious to learn.

Lastly, I would like to thank the Ohio Supercomputer Center for providing a start-up grant account at their computing facility. This work was supported in part by an allocation of computing time from the Ohio Supercomputer Center.
VITA

2007-Present  Graduate Teaching Associate,  
              Department of Mathematics,  
              The Ohio State University  

2002-2007  VIGRE Fellow,  
            Department of Mathematics,  
            The Ohio State University  

2005  M.S. in Mathematics,  
      The Ohio State University  

2002  University Fellow,  
      Department of Mathematics,  
      The Ohio State University  

2002  B.S. in Mathematics,  
      The Ohio State University  

1998  High School Diploma,  
      Marysville High School,  
      Marysville, Ohio  

1979  Born, Columbus, Ohio  

iv
PUBLICATIONS


FIELDS OF STUDY

Major Field: Mathematics

Specialization: Number Theory: Professor Warren Sinnott
**TABLE OF CONTENTS**

Abstract ................................................................. ii
Acknowledgments ......................................................... iii
Vita ................................................................. iv

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Definitions, Basic Results, and History</td>
</tr>
<tr>
<td>1.1.1</td>
<td>Height and Complexity</td>
</tr>
<tr>
<td>1.2</td>
<td>General Results Using Heights</td>
</tr>
<tr>
<td>1.2.1</td>
<td>Mordell-Weil Groups</td>
</tr>
<tr>
<td>1.2.2</td>
<td>Lehmer's Problem</td>
</tr>
<tr>
<td>1.2.3</td>
<td>Lower Bounds for Heights in Certain Classes of Algebraic Numbers and Other Results</td>
</tr>
<tr>
<td>1.3</td>
<td>Elements and Bases of Minimal Height</td>
</tr>
<tr>
<td>1.3.1</td>
<td>Results of Roy and Thunder</td>
</tr>
<tr>
<td>1.3.2</td>
<td>Results of Ruppert and Kihel</td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Preliminaries for Theorems 2.2.1, 2.2.2, and 2.2.3.</td>
</tr>
<tr>
<td>2.2</td>
<td>Integral Generators of Smallest Height in ( \mathbb{Q}(\sqrt{d}) ).</td>
</tr>
<tr>
<td>2.3</td>
<td>Some Height Results</td>
</tr>
<tr>
<td>2.4</td>
<td>On a Result of Ruppert Concerning Polynomials of Smallest Polynomial-Height Whose Roots Generate Imaginary Quadratic Extensions of ( \mathbb{Q} ).</td>
</tr>
<tr>
<td>2.5</td>
<td>Generators of Smallest Height in Imaginary Quadratic Extensions of ( \mathbb{Q} ).</td>
</tr>
</tbody>
</table>
2.6 Generators of Smallest Height in Real Quadratic Extensions of $\mathbb{Q}$. ................................. 70

3 Further Work ................................................................. 76
   3.1 The Real Quadratic Case and More ................................. 76
   3.2 Relative Heights ....................................................... 77

APPENDICES

A PARI/GP Code ............................................................... 79
Bibliography ................................................................. 83
CHAPTER 1
INTRODUCTION

1.1 Definitions, Basic Results, and History

A notion of height perhaps originated with Fermat. His descent arguments revolve around the idea of finding “smaller” solutions to certain equations, assuming that solutions exists at all. The usual example of this is his proof of the following result:

**Theorem 1.1.1.** The equation \( x^4 + y^4 = z^2 \) has no integer solutions with \( xyz \neq 0 \).

Since Fermat, the idea of attaching some sort of “size” to numbers has been the topic of much research. Most notably, the proofs of Mordell’s Theorem and subsequently of the Mordell-Weil theorem, which states that the set of \( K \)-rational points of an Abelian variety over the number field \( K \) is finitely generated, rely heavily on a size measure of certain numbers. Innovations of Weil and Northcott have been further developed into a rich theory that is the topic of hundreds of research papers and many books, including those of Waldschmidt [Wa], Bombieri and Gubler [BoGu], and Hindry and Silverman [HiSi].

With the benefit of hindsight, it is very natural to give a simple measure of size to a rational number:
Definition. Let $a$ and $b$ be co-prime, non-zero integers. The height of $\frac{a}{b}$, denoted by $H\left(\frac{a}{b}\right)$, is defined by $H\left(\frac{a}{b}\right) = \max(|a|, |b|)$.

This notion of height has many advantages over the other simple measure of size, namely that given by the usual absolute value on the rational (real) numbers. In particular, there are only finitely many rational numbers of bounded height while there are infinitely many rational numbers of bounded absolute value. This kind of finiteness result is useful both theoretically and computationally.

Unfortunately, when one wants to consider more general numbers, like algebraic numbers, this definition of height does not immediately generalize. In order to find a generalization, one must use the following characterization of height for a rational number, which makes use of not only the usual absolute value on the rational numbers, but also all of the $p$-adic absolute values as well.

Theorem 1.1.2. Let $a$ and $b$ be co-prime, non-zero integers, let $|\cdot|$ denote the usual absolute value on the rational numbers, and for each prime number $p$, let $|\cdot|_p$ denote the $p$-adic absolute value on the rational numbers which is given by $\left|\frac{a}{b}\right|_p = p^{-\text{ord}_p(a/b)}$.

$$H\left(\frac{a}{b}\right) = \max \left(1, \left|\frac{a}{b}\right|\right) \prod_{p \text{ prime}} \max \left(1, \left|\frac{a}{b}\right|_p\right).$$

This leads to the following definition of height for a general algebraic number:

Definition. Let $\alpha \in K^\times$, where $K$ is a number field. The height of $\alpha$ (with respect to $K$), denoted by $H_K(\alpha)$, is defined by

$$H_K(\alpha) = \prod_{v \in M_K} \max \left(1, |\alpha|_v\right)^{n_v}.$$
where $M_K$ is the set of places of $K$ and $n_v$ is the local degree of $K$ at $v$. Here, $| \cdot |_v$ is the absolute value associated to $v$ that restricts to $| \cdot |_p$ on the rational numbers where $v | p$. When $K = \mathbb{Q}(\alpha)$, this will be denoted by $H(\alpha)$.

For standard facts about and properties of absolute values on number fields, see any book on algebraic number theory, like [La]. However, since it is crucially used later, with this notation the product formula reads as follows:

**Theorem 1.1.3. (The Product Formula)** Let $K$ be an algebraic number field, let $M_K$ denote the set of places of $K$, and for each $v \in M_K$ let $n_v$ denote the local degree of $K$ at $v$. For any $\alpha \in K^\times$,

$$\prod_{v \in M_K} |\alpha|_v^{n_v} = 1.$$  

This definition of height is apparently a twentieth century development, although there are older results that are more naturally stated in terms of height. For example, perhaps the first result concerning heights of algebraic numbers is the following theorem of Kronecker from 1857:

**Theorem.** [Kr] Every nonzero algebraic integer that lies with its conjugates in the closed unit disc $|z| \leq 1$ is a root of unity.

This result is now commonly stated as:

**Theorem 1.1.4.** Let $x \in \overline{\mathbb{Q}}^\times$. $H(x) = 1$ if and only if $x$ is a root of unity.

This is the “right” definition of height for an algebraic number because it agrees with the original definition when restricted to the rational numbers and it satisfies the following fundamental theorem, due to Northcott. It is the fact that allows arguments like Fermat’s descent to work in more general situations.
Theorem 1.1.5. [No] There are only finitely many algebraic numbers having bounded degree and bounded height.

A concept closely related to height is that of Mahler measure.

Definition. Let \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = a_n \prod_{i=1}^{n} (x - \alpha_i) \) be a polynomial of degree \( n \) with integer coefficients and roots \( \alpha_i \). The Mahler measure of \( f(x) \), denoted by \( M(f) \), is defined by

\[
M(f) = \exp \left( \int_0^1 \log \left| f(e^{2\pi i t}) \right| \, dt \right).
\]

As stated, this was introduced by Mahler in 1962 [Ma]. However, the same concept was defined earlier by Lehmer in 1933 [Le]:

\[
M(f) = |a_n| \prod_{|\alpha_i| > 1} |\alpha_i| = |a_n| \prod_{v \in M_K^\infty} \max(1, |\alpha|_v)^{n_v},
\]

where the equivalence of these definitions follows from an even older result of Jensen from 1899 [Je] (here, \( M_K^\infty \) is the set of infinite places of \( K \)). This is related to height by the following theorem. The notation \( M(\alpha) \) will sometimes be used to denote the Mahler measure of the primitive minimal polynomial of the algebraic number \( \alpha \) over \( \mathbb{Q} \).

Theorem 1.1.6. ([Wa], p.79) If \( \alpha \in \overline{\mathbb{Q}}^\times \) has primitive minimal polynomial \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = a_n \prod_{i=1}^{n} (x - \alpha_i) \) of degree \( n \) with integer coefficients and roots \( \alpha_i \) with positive leading coefficient, then \( H(\alpha) = M(f) \).

Proof. It suffices to show that, for every prime \( p \) of \( \mathbb{Z} \),

\[
|a_n|_p \prod_{i=1}^{n} \max(1, |\alpha_i|_p) = 1
\]
because this implies that

\[ a_n = \prod_p |a_n|_p^{-1} = \prod_p \prod_{v | p} \max (1, |\alpha|_v)^{n_v} = \prod_{v \in M^0_K} \max (1, |\alpha|_v)^{n_v}, \]

where \( M^0_K \) is the set of finite places of \( K = \mathbb{Q}(\alpha) \).

Assume that the roots \( \alpha_i \) lie in \( \mathbb{C}_p \), the completion of \( \overline{\mathbb{Q}}_p \) for the absolute value \( | \cdot |_p \) which contains an algebraic closure of \( \mathbb{Q} \). Further, assume that \( |\alpha_1|_p \leq \ldots \leq |\alpha_n|_p \). Since \( f \) is (primitive) irreducible, \( \max (|a_n|_p, \ldots, |a_0|_p) = 1 \). By expanding the product \( a_n \prod_{i=1}^n (x - \alpha_i) \), each term \( \frac{a_i}{a_n} \) for \( 1 \leq i \leq n \) is expressible as a symmetric function of the \( \alpha_j \):

\[ \frac{a_i}{a_n} = (-1)^n \sum_{0 \leq s_1 < \ldots < s_i \leq n-1} \alpha_{s_1} \cdots \alpha_{s_i}. \]

If \( |\alpha_i|_p \leq 1 \) for all \( i = 1, \ldots, n \) then \( |a_i|_p \leq |a_n|_p \) and \( \max (|a_n|_p, \ldots, |a_0|_p) = |a_n|_p = 1 \), which gives the desired result. Otherwise, let \( 1 \leq j \leq n \) be such that \( |\alpha_{j-1}|_p \leq 1 < |\alpha_j|_p \). Since \( | \cdot |_p \) is non-Archimedean,

\[ \max_{0 \leq i \leq n-1} \left( \left| \frac{a_i}{a_n} \right|_p \right) = \left| \frac{a_{n-j+1}}{a_n} \right|_p = \left| \prod_{i=j}^n \alpha_i \right|_p = \prod_{i=1}^n \max (1, |\alpha_i|_p). \]

Hence,

\[ \max (|a_{n-1}|_p, \ldots, |a_0|_p) = |a_n|_p \prod_{i=1}^n \max (1, |\alpha_i|_p) \geq |a_n|_p. \]

This shows that

\[ \max (|a_n|_p, \ldots, |a_0|_p) = |a_n|_p \prod_{i=1}^n \max (1, |\alpha_i|_p), \]

which completes the proof. \( \square \)
There are many other quantities that various authors refer to as “height” or some variant of height. One of them is based on the following interesting calculation. If $L$ is any number field containing $K = \mathbb{Q}(\alpha)$, then

$$H_K(\alpha)^{1/[K:\mathbb{Q}]} = H(\alpha)^{1/[K:\mathbb{Q}]}$$

$$= H(\alpha)^{[L:K]/[L:\mathbb{Q}]}$$

$$= \left( \prod_{v\in M_K} \max (1, |\alpha|_v n_v(\mathbb{K})) \right)^{[L:K]/[L:\mathbb{Q}]}$$

$$= \left( \prod_{v\in M_K} \max (1, |\alpha|_v n_v(\mathbb{K}[L:K])) \right)^{1/[L:\mathbb{Q}]}$$

$$= \left( \prod_{v\in M_K} \max (1, |\alpha|_v \sum_{w|v} n_w(L)) \right)^{1/[L:\mathbb{Q}]}$$

$$= \left( \prod_{w\in M_L} \max (1, |\alpha|_w n_w(\mathbb{L})) \right)^{1/[L:\mathbb{Q}]}$$

$$= H_L(\alpha)^{1/[L:\mathbb{Q}]}.$$  

This shows that the number $H_L(\alpha)^{1/[L:\mathbb{Q}]}$ is independent of the number field $L$ and prompts the following somewhat more satisfying definition of a height:

**Definition.** Let $\alpha \in \overline{\mathbb{Q}}^\times$ and let $L$ be any number field containing $\alpha$. The **absolute logarithmic Weil height** of $\alpha$, denoted by $h(\alpha)$, is defined by

$$h(\alpha) = \frac{1}{[L : \mathbb{Q}]} \log H_L(\alpha).$$

It is natural to further extend the definition of Weil height to allow one to consider heights of points in some projective space over a number field. This will be used later in reference to heights of bases of number fields.
**Definition.** Let $P = [x_0, x_1, \ldots, x_n] \in \mathbb{P}^n(L)$ for some number field $L$. The *absolute logarithmic Weil height* of $P$, denoted by $h(P)$, is defined by

$$h(P) = \frac{1}{[L : \mathbb{Q}]} \log H_L(P),$$

where

$$H_L(P) = \prod_{v \in M_L} \max(|x_0|_v, |x_1|_v, \ldots, |x_n|_v)^{n_v}.$$

The product formula shows that $h(P)$ is independent of the choice of homogeneous coordinates for $P$.

The following proposition shows that the Weil height is well-behaved under the action of Galois.

**Proposition 1.1.7.** ([Si2], p.213) Let $P = [x_0, x_1, \ldots, x_N] \in \mathbb{P}^N(\mathbb{Q})$. For $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $h(\sigma(P)) = h(P)$.

**Proof.** Let $K/\mathbb{Q}$ be a field with $P \in \mathbb{P}^N(K)$. $\sigma$ gives an automorphism $\sigma : K \to \sigma(K)$, and it likewise identifies the sets of absolute values,

$$\sigma : M_K \to M_{\sigma(K)}$$

$$v \mapsto \sigma(v).$$
(I.e. for \( x \in K \) and \( v \in M_K \), \(|\sigma(x)|_{\sigma(v)} = |x|_v \).) Clearly \( \sigma \) also gives an isomorphism \( K_v \to \sigma(K)_{\sigma(v)} \), so \( n_v = n_{\sigma(v)} \). Since \([K : \mathbb{Q}] = [\sigma(K) : \mathbb{Q}] \) and

\[
H_{\sigma(K)}(\sigma(P)) = \prod_{w \in M_{\sigma(K)}} \max(|\sigma(x_i)|_w)^{n_w}
\]

\[
= \prod_{v \in M_K} \max(|\sigma(x_i)|_{\sigma(v)})^{n_{\sigma(v)}}
\]

\[
= \prod_{v \in M_K} \max(|x_i|_v)^{n_v}
\]

\[
= H_K(P),
\]

the result follows.  

With this new definition, the Weil height of an algebraic number \( \alpha \) is simply the Weil height of the projective point \([1, \alpha] \in \mathbb{P}^1(\mathbb{Q}(\alpha))\). The important Northcott Theorem remains true when one considers projective points and uses the corresponding Weil height. Another basic, yet very important, fact is given in the following theorem. In addition, the Weil height and the height are each amalgamations of local height functions. This fact often allows one to exploit geometric and/or analytic properties of local heights in order to make global arithmetic deductions.[Si3]

**Proposition 1.1.8.** Let \( \zeta \) be a root of unity and let \( \alpha \) be a nonzero algebraic number. If \( K \) is a number field containing \( \alpha \) and \( \zeta \), then \( H_K(\zeta \alpha) = H_K(\alpha) \).

**Proof.**

\[
H_K(\zeta \alpha) = \prod_{v \in M_K} \max(1, |\zeta \alpha|_v)^{n_v}
\]

\[
= \prod_{v \in M_K} \max(1, |\alpha|_v)^{n_v}
\]

\[
= H_K(\alpha).
\]
Other variations on the idea of a height function include the house of an algebraic number, the diameter of an algebraic number, and the denominator of an algebraic number. (See [Wa] for the definitions.) But perhaps the most basic, and most important, is the following:

**Definition.** Let \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \) be a polynomial with integer coefficients. The *naïve height* or *polynomial-height* of \( f \), denoted by \( \hat{H}(f) \), is defined by \( \hat{H}(f) = \max(|a_n|, |a_{n-1}|, \ldots, |a_0|) \). If \( \alpha \) is an algebraic number, then \( \hat{H}(\alpha) = \hat{H}(f) \), where \( f \) is the primitive minimal polynomial of \( \alpha \) over \( \mathbb{Q} \).

Given an algebraic number \( \alpha \) with minimal polynomial \( f \), the polynomial-height of \( f \) and height of \( \alpha \) are closely related, but they are not usually the same. For example, any polynomial-height is an integer, while the heights of algebraic numbers are real numbers in general. Polynomial-height will play a crucial role in the main results of this work. The following theorem shows one aspect of the relationship between these two quantities.

**Theorem 1.1.9.** ([Wa], p.113) If \( \alpha \) is an algebraic number of degree \( n \) with primitive minimal polynomial \( f \), then \( (n+1)^{-1/2} M(f) = (n+1)^{-1/2} H(\alpha) \leq \hat{H}(f) \leq 2^n H(\alpha) = 2^n M(f) \).

1.1.1 Height and Complexity

It is worth offering a word of caution here about the nebulous idea that heights measure arithmetic complexity. Silverman [Si3] observes that the rational numbers
\[ \frac{1}{2} \text{ and } \frac{100000}{200001} \] are close to each other in the sense of the usual absolute value on the rationals, but the latter is more arithmetically complicated than the former—and this fact is illuminated via the heights of these numbers. However, the latter number has smaller height than 200002, but one could hardly argue that 200002 is more “complex” than 100000/200001. Further, the height of any rational number is always equal to the height of some integer. This leads one to the intuition that if one understands how the heights of integers behave well enough, then one understands how the heights of rational numbers behave. Unfortunately, this is simply not the case when one considers general algebraic integers and algebraic numbers. This is very well illustrated by the main results of this work, even in the quadratic case.

On the other hand, there are instances where height clearly does afford some measure of complexity. One example, again from Silverman [Si3], is given below in Figure 1.1. The growth on the number of digits is clearly quadratic in nature.

The moral here is that heights give some idea of size and sometimes give more delicate information that one might describe as complexity.

### 1.2 General Results Using Heights

#### 1.2.1 Mordell-Weil Groups

As mentioned above, the proof of Mordell’s Theorem (the Mordell-Weil Theorem in the case that the Abelian variety is an elliptic curve and the base field is \( \mathbb{Q} \)) relies heavily on heights. Rather than reproduce the standard proof here, using the
Figure 1.1: For the elliptic curve $E : y^2 = x^3 + x + 1$ and point $P = (0,1)$, this table lists $n$ and $H(x(nP))$ for $n = 1, 2, \ldots, 30$.

following two preliminary lemmas, this subsection presents a weaker result which generalizes to certain infinite algebraic extensions of $\mathbb{Q}$. Recall, throughout this section, that $h(x)$ denotes the Weil height of the algebraic number $x$.

**Lemma 1.2.1.** ([Fu], p. 51.) A countable, torsion-free Abelian group $A$ is free if and only if every subgroup of $A$ of finite rank is free.

**Proof.** It is well known that every subgroup of a free Abelian group is free. This gives sufficiency. Suppose that every subgroup of $A$ of finite rank is free. (Here, “rank”
refers to the dimension of $A \otimes \mathbb{Q}$ as a $\mathbb{Q}$-vector space.) Let $A = \{a_1, a_2, \ldots \}$ be an enumeration of $A$. Define $A_n$ as the subgroup generated by the set of all $x \in A$ which have a non-zero multiple in $\{a_1, a_2, \ldots, a_n\}$. Then $A_n$ is a subgroup of rank $r(A_n) \leq n$, and since $r(A_{n+1}) \leq r(A_n) + 1$, there is a subsequence $B_n$ of the $A_n$ such that

$$B_1 \subseteq B_2 \subseteq \ldots \subseteq B_n \subseteq \ldots$$

and $r(B_n) = n$ for every $n$. The union of the $B_n$ is clearly $A$. By hypothesis, the subgroups $B_n$ are free, whence $B_n = < b_1, b_2, \ldots, b_n >$ for some elements $b_i \in B_n$. Now $B_{n+1}/B_n$ is torsion free of rank one and finitely generated, thus it is infinite cyclic. Hence, the short exact sequence

$$0 \rightarrow B_n \rightarrow B_{n+1} \rightarrow \mathbb{Z} < b_{n+1} > \rightarrow 0$$

splits and $B_{n+1} = < b_1, b_2, \ldots, b_n, b_{n+1} >$. Therefore, the $b_i$ may be chosen independently of $n$. This implies that $A = \sum_{n=1}^{\infty} \mathbb{Z} < b_i >$ as desired. 

**Lemma 1.2.2.** Let $K$ be a number field and let $E$ be an elliptic curve defined over $K$. By abuse of notation, let $h$ also denote the Weil height on $E(K)$ the $K$-rational points of $E$ (that is, if $P = (x, y) \in E(K)$ then $h(P) = h(x)$).

1. For all $P \in E(K)$ and $m \in \mathbb{Z}$, $h(P) \geq 0$ and $h(mP) = h((-m)P)$.

2. For all $P, Q \in E(K)$,

$$h(P + Q) + h(P - Q) = 2h(P) + 2h(Q) + O(1).$$

Here, the constants in the $O(1)$ are independent of the points $P, Q$.  

12
(3) For every $m \in \mathbb{Z}$ and every $P \in E(K)$,

$$h(mP) = m^2h(P) + f(m) \cdot O(1),$$

where the $O(1)$ is the quantity in (2) above that is bounded (say, by $C > 0$) independent of $m$ and $P$ and $f$ is some function of $m$ that is $O(m^2)$ that is independent of $P$.

(4) For every $r \in \mathbb{R}$, there are only finitely many $P \in E(K)$ satisfying $h(P) < r$.

(5) The torsion subgroup of $E(K)$ is finite.

\[\text{Proof.} \ (1) \text{ is clear, by definition, and (4) follows from Northcott’s Theorem. For (2), see [Si2], p.216, and for (5) see [Si2], p.220. For (3), the result is trivial for $|m| = 0, 1$. If $|m| = 2$, replacing $Q$ in (2) by $P$ gives the result. For the other values of $|m|$, first note that by replacing $P$ by $-P$ if $m < 0$ it suffices to assume that $m > 0$. Next, proceed by induction. Assume the result holds for $m - 1$ and $m$. Replacing $P, Q$ in (2) by $mP, P$ and using (1) above gives}

$$h((m + 1)P) = h(mP + P)$$

$$= -h((m - 1)P) + 2h(mP) + 2h(P) + O(1)$$

$$= (- (m - 1)^2 + 2m^2 + 2)h(P) + (- f(m - 1) + 2f(m) + 1)O(1)$$

$$= (m + 1)^2h(P) + F(m) \cdot O(1),$$

\[\text{where} \ F(m) = 2f(m) - f(m - 1) + 1 \text{ is } O(m^2) = O((m + 1)^2). \text{ This completes the proof.} \]
Theorem 1.2.3. Let $E$ be an elliptic curve defined over a number field $K$, let $E(K)$ denote the set of $K$-rational points of $E$, and let $E(K)_{\text{tors}}$ denote its (finite) subgroup of torsion points. $G = E(K)/E(K)_{\text{tors}}$ is a free Abelian group.

Proof. One way to proceed is to use the first Lemma above and examine $H/nH$ for subgroups $H \leq G$ of finite rank. Instead, here is a different argument.

Note that since $K$ is countable as a set, $E(K)$ (and hence $G$) is also countable as a set. By the proof of Lemma 1.2.1, it suffices to show that $G$ is the union of an ascending chain of pure free subgroups. (Recall that a pure subgroup $B$ of a torsion free Abelian group $A$ is one such that $A/B$ is torsion free.) Order (under $\leq$) the points of $E(K)$ by their Weil heights. For each $r \in \mathbb{R}$ there are only finitely many points in $E(K)$ of Weil height $r$, by Lemma 1.2.2, part (4); order these in any way.

Let $S_0 = E(K)_{\text{tors}}$. For each $i \in \mathbb{N}$, inductively define $S_i =< S_{i-1} \cup \{Q : Q \leq P \text{ where } P \text{ is the smallest point of infinite order independent of } S_{i-1}\} >$. It is clear that $S_0 \subseteq S_1 \subseteq S_2 \ldots$ and $G = \bigcup_i S_i/S_0$. For each $i$, $S_i/S_0$ is finitely generated and torsion free, hence free. And $G$ is the union of the ascending chain of these groups, but they need not necessarily be pure subgroups of $G$. Fix $i \in \mathbb{N}$ and suppose that $P \in E(K) \setminus S_i$ is such that there is some $n \in \mathbb{N}$ with $nP \in S_i$. Let $Q_1, Q_2, \ldots, Q_r$ be a basis for the free part of $S_i$. There exist integers $m_1, m_2, \ldots, m_r$ and a torsion point $T$ such that $nP = m_1 Q_1 + m_2 Q_2 + \cdots + m_r Q_r + T$. For each $i$, let $m_i = nk_i + l_i$ with $l_i, k_i \in \mathbb{Z}$ and $|l_i| < |n|$. Notice that the smallest pure subgroup $S'_i$ of $E(K)$ containing $S_i$ is exactly $\{Q \in E(K) : \text{there exists } n \in \mathbb{Z} \text{ such that } nQ \in S_i\}$. Also notice that including $P$ in $S'_i$ is equivalent to including $P + R$ where $R \in S_i$, i.e.
\[ <S_i, P> = <S_i, P - k_1Q_1 - k_2Q_2 - \ldots - k_rQ_r>. \]
So suppose that each \(|m_i| < |n|\), without loss of generality. By Lemma 1.2.2 (and using the notation given there),

\[
\begin{align*}
  h(nP) &= h(m_1Q_1 + m_2Q_2 + \cdots + m_rQ_r + T) \\
  &= 2h(m_1Q_1 + m_2Q_2 + \cdots + m_rQ_r) + 2h(T) - \\
  &\quad h(m_1Q_1 + m_2Q_2 + \cdots + m_rQ_r - T) + O(1) \\
  &\leq 2h(m_1Q_1 + m_2Q_2 + \cdots + m_rQ_r) + 2h(T) + C' \\
  &\leq 2(2h(m_1Q_1 + m_2Q_2 + \cdots + m_{r-1}Q_{r-1}) + 2h(m_rQ_r) + C) + 2h(T) + C \\
  &\quad \vdots \\
  &\leq 2^r(h(m_1Q_1) + h(m_2Q_2) + \cdots + h(m_rQ_r)) + 2h(T) + (2r + 1)C.
\end{align*}
\]

Also by Lemma 1.2.2, there is some \(C' > 0\) such that for every integer \(m\) and every \(Q \in E(K)\),

\[
\begin{align*}
  h(Q) &= \frac{h(mQ) - f(m)O(1)}{m^2} \\
  &\leq \frac{h(mQ)}{m^2} + C'C,
\end{align*}
\]
since

\[ h(mQ) = m^2h(Q) + f(m)O(1). \]
Hence,

\[
 h(P) \leq \frac{2^r(h(m_1Q_1) + h(m_2Q_2) + \cdots + h(m_rQ_r)) + 2h(T) + (2r + 1)C + C'}{n^2} + 2h(T) + (2r + 1 + C')C
\]

where \( T' \) is a torsion point of maximum Weil height. The right-hand side is independent of the point \( P \). By Lemma 1.2.2, there are only finitely many points whose Weil height is bounded by this number. Hence, \( S'_i \) is finitely generated since one must only include finitely many ‘extra’ points to insure that all of the desired points are included and \( S_i \) is already finitely generated. This implies that \( S'_i/S_0 \) is pure, finitely generated, and torsion free. Note that \( S'_i \subseteq S'_{i+1} \) for every \( i \). Since \( G = \bigcup_i S'_i/S_0 \), the result follows.

An immediate corollary of this result, and especially its proof, is the following:

**Corollary 1.2.4.** Let \( K \) be an algebraic extension of \( \mathbb{Q} \) such that Northcott’s Theorem holds for elements of \( K \) (i.e. there are only finitely many elements of \( K \) of bounded Weil height). If \( E \) is an elliptic curve defined over \( \mathbb{Q} \) such that \( E(K)_{\text{tors}} \) is finite, then \( E(K)/E(K)_{\text{tors}} \) is a free Abelian group.

There is a corollary of this corollary, once one has the following result of Bombieri and Zannier. It is of independent interest because it has a very number-theoretic
proof and displays some of the arithmetic properties of the Weil height, so the proof is given below.

**Theorem 1.2.5.** [BoZa] Let $K$ be a number field, let $d$ be a positive integer, and let $K^{(d)}$ denote the composite of all number fields of degree at most $d$ over $K$. Northcott’s Theorem holds for $K^{(d)}_{\text{Ab}}$ the maximal Abelian subfield of $K^{(d)}$. In particular, Northcott’s Theorem holds for $\mathbb{Q}^{(2)}$.

**Corollary 1.2.6.** If $E$ is an elliptic curve defined over $\mathbb{Q}$, then, with notation as in the previous theorem, $E\left(\mathbb{Q}^{(2)}\right)/E\left(\mathbb{Q}^{(2)}\right)_{\text{tors}}$ is a free Abelian group.

*Proof.* The previous theorem shows that Northcott’s Theorem holds for elements of $\mathbb{Q}^{(2)}$ and it is a result in [Gr], p.23, that $E\left(\mathbb{Q}^{(2)}\right)_{\text{tors}}$ is finite. The previous corollary now applies.

This extends the result stated in [Gr] which says only that $E\left(\mathbb{Q}^{(2)}\right)/E\left(\mathbb{Q}^{(2)}\right)_{\text{tors}}$ has infinite rank as an Abelian group.

*Proof.* (of Theorem 1.2.5) Let $D = d!$. Without loss of generality, $K$ contains the field $\mathbb{Q}(\sqrt[1]{T})$ generated by roots of unity of order $D$. Let $T$ be a fixed, positive, real number and let $\alpha \in K^{(d)}_{\text{Ab}}$ be any element satisfying $h(\alpha) \leq T$. As a subfield of an Abelian field, $L = K^{(d)}$ is a finite Abelian extension of $K$. Note that the Galois group of $L/K$ has exponent dividing $D$.

Let $p$ be a prime that is unramified in $K$ and let $v$ be a place of $K$ above $p$. Let $e = e_{w/v}$ be the ramification index of any place (hence, every place) $w$ of $L$ lying over $v$. If $p > d$, then $p$ does not divide the order of $\text{Gal}(L/K)$ since this group has
exponent dividing $D$. Hence, $w$ will be tamely ramified over $v$ and the inertia group of $w$ over $v$ is cyclic of order $e$. Hence, $e \mid D$.

Let $\theta = p^{1/e}$ for some choice of the root and consider the field $L(\theta)$ with a place $u$ lying over $w$. As a compositum of two Abelian extensions whose exponents divide $D$, $L(\theta)/K$ is also Abelian with exponent dividing $D$. (Recall, $K$ contains the $D$-th roots of unity and $e \mid D$.) Note that the ramification index of $u|_{K(\theta)}$ over $v$ is $e$ and the residue degree is 1. By Abhyankar’s Lemma, this and $u|_{K(\theta)}$ tamely ramified over $v$ imply that $u$ is unramified over $w$. Hence, $e_{u/v} = e$.

Let $I \subseteq \text{Gal}(L(\theta)/K)$ be the inertia group of $u$ over $v$, a group of order $e$. Since $L(\theta)/K$ is Abelian, all inertia groups above $v$ are equal to $I$. For $U$ the fixed field of $I$, $U$ is normal over $K$, $U/K$ is unramified over $v$, and $[L(\theta):U] = |I| = e$. Since $u|_{U}$ is unramified over $p$, $u|_{U(\theta)}$ has ramification index $e = [U(\theta):U]$ over $u|_{U}$, proving in particular that $U(\theta) = L(\theta)$. Hence, $\alpha \in U(\theta)$ so that $\alpha = \beta_0 + \beta_1 \theta + \ldots + \beta_{e-1} \theta^{e-1}$ for some $\beta_i \in U$. The conjugates of $\theta$ over $U$ are $\zeta^r \theta$, where $\zeta$ is a primitive $e$-th root of unity and $r \in \{0, 1, \ldots, e - 1\}$. Therefore, the trace $Tr_{U(\theta)/U}(\theta^j)$ vanishes if $j$ is not a multiple of $e$ and equals $e$ if $j = 0$. This implies that

$$\beta_j = \frac{1}{e} Tr_{U(\theta)/U}(\alpha \theta^{-j}) = \frac{1}{e \theta} \sum_{r=0}^{e-1} \alpha_r \zeta^{-rj},$$

where the $\alpha_r$ are certain conjugates of $\alpha$. Note that Propositions 1.1.7 and 1.1.8 show that $h(\alpha_r \zeta^{-rj}) = h(\alpha) \leq T$ for $0 \leq r \leq e - 1$. By a standard inequality about the height of a sum, these two statements imply that

$$h(\beta_j \theta) \leq \log(e) + \sum_r h(\alpha_r) + \log(e) \leq 2 \log(D) + DT.$$
As before, let \( u \) be any place of \( U(\theta) = L(\theta) \) above \( v \) and use the same letter to denote the associated discrete valuation normalized by \( u(L(\theta)^\times) = \mathbb{Z} \). Since \( \beta_j \in U \), \( u(\beta_j) \) is either equal to 0 or divisible by \( e \). If \( 1 \leq j \leq e - 1 \), then \( u(p^{j/e}) = j \) is not divisible by \( e \). Hence, \( u(\beta_j p^{j/e}) \neq 0 \). This shows that \( |u(\beta_j p^{j/e})| \geq u(p^{1/e}) = 1 \).

Let \( \gamma = \beta_j p^{j/e} \) and suppose that \( \gamma \neq 0 \). If \( n_u = \lfloor U(\theta)_u : \mathbb{Q}_p \rfloor \) is the local degree, then

\[
|\log |\gamma|_u| \geq \frac{-1}{e} \log |p|_u = \frac{n_v \log p}{e[U(\theta) : \mathbb{Q}]}
\]

Hence,

\[
2h(\gamma) = h(\gamma) + h(\gamma^{-1}) \\
\geq \sum_{u\mid v} |\log |\gamma|_u| \\
\geq \frac{1}{e[U(\theta) : \mathbb{Q}]} \left( \sum_{u\mid v} n_v \right) \log p \\
= \frac{1}{e[U(\theta) : \mathbb{Q}]} [U(\theta) : K] \log p \\
= \frac{\log p}{e[K : \mathbb{Q}]}.
\]

Hence, either \( \beta_j = 0 \) or \( \log p \leq 2e[K : \mathbb{Q}](2 \log D + DT) \), by this inequality and the inequality from two paragraphs above.

Let \( S \) be the set of rational primes containing all prime divisors of the discriminant of \( K \) over \( \mathbb{Q} \) and all primes that are at most \( \exp(2e[K : \mathbb{Q}](2 \log D + DT)) \). If \( v \in M_K \) lies over a prime \( p \not\in S \), then \( v \) is unramified over \( p \). Hence, the last sentence of the previous paragraph shows that \( \beta_j = 0 \) for \( 1 \leq j \leq e - 1 \) so that \( \alpha = \beta_0 \in U \). Recall that \( U \) is an Abelian extension of \( K \) with exponent dividing \( D \).
and is unramified over \( v \). This implies that \( K(\alpha) \) is unramified above any \( p \not\in S \) and 
\( K(\alpha) \) is a composite of cyclic extensions of \( K \) of degree at most \( D \) and each of these 
extensions is unramified outside of \( S \). There are only finitely such fields, so there are 
only finitely many possibilities for \( K(\alpha) \). Hence, \( \alpha \) has bounded degree and bounded 
height which, by Northcott’s Theorem, implies that there are only finitely many such 
\( \alpha \). This completes the proof.

### 1.2.2 Lehmer’s Problem

An active area of research involving heights revolves around the so-called Lehmer’s Problem.

**Problem.** Is it true that, for every \( \epsilon > 0 \), there exists an algebraic number \( \alpha \) for which 
\( 1 < M(\alpha) < 1 + \epsilon \)? Alternatively, for \( \alpha \in \overline{\mathbb{Q}}^\times \) with \( [\mathbb{Q}(\alpha) : \mathbb{Q}] = d \) that is not 
a root of unity, is \( h(\alpha) \geq c/d \) for some absolute constant \( c \)?

Amazingly, the smallest known value \( M(\alpha) > 1 \) for \( \alpha \in \overline{\mathbb{Q}}^\times \) was discovered by 
Lehmer himself in 1933 [Le] and is achieved by a root of the (reciprocal) polynomial 
\[
x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1.
\]

A solution to the general problem has proved elusive. But there are special cases 
where solutions are known, some of which are listed below.

**Theorem 1.2.7.**

1. **[Sm1]** Let \( \alpha \in \overline{\mathbb{Q}}^\times \) with \( [\mathbb{Q}(\alpha) : \mathbb{Q}] = d \). If \( d \) is odd and \( \alpha \) is not a root of unity, 
then \( h(\alpha) \geq c/d \) for the absolute constant \( c = 0.2811 \ldots \). Moreover, if \( \alpha^{-1} \) is
not a conjugate of $\alpha$, then $h(\alpha) \geq c/d$ for some absolute constant $c$ which may be taken to be $\log \theta_0$, where $\theta_0 > 1$ is the smallest P-V number (i.e. the real root of $x^3 - x - 1$).

(2) [BoDoMo] Let $\mathcal{D}_m$ denote the set of polynomials with integer coefficients all of whose coefficients are congruent to 1 modulo $m$. If $f \in \mathcal{D}_m$ has degree $n - 1$ and no cyclotomic factors, then $\log M(f) \geq c_m \left(1 - \frac{1}{n}\right)$, where $c_2 = \frac{\log 5}{4}$ and $c_m = \log \left(\sqrt{m^2 + 1}/2\right)$.

(3) [Do] For every $\epsilon > 0$, there exists a positive integer $d_0(\epsilon)$ such that, for any integer $d \geq d_0$ and any nonzero algebraic number $\alpha$ of degree $\leq d$ which is not a root of unity,

$$h(\alpha) \geq \frac{1 - \epsilon}{d} \left(\frac{\log \log d}{\log d}\right)^3.$$ 

[Vo] Moreover, for all $d \geq 2$,

$$h(\alpha) \geq \frac{1}{4d} \left(\frac{\log \log d}{\log d}\right)^3.$$ 

1.2.3 Lower Bounds for Heights in Certain Classes of Algebraic Numbers and Other Results

The arithmetic properties of height and Weil height manifest themselves in surprising places. As seen above, the proof of Bombieri and Zannier’s result concerning $K_{Ab}^{(d)}$ relies heavily on algebraic number theory facts. Another such result is the following, due to Amoroso and Dvornicich:

**Theorem 1.2.8.** [AmDv] Let $L/\mathbb{Q}$ be an Abelian extension and let $\alpha \in L^\times$. If $\alpha$ is not a root of unity, then $h(\alpha) \geq \frac{\log 5}{12} \approx 0.1341$. 

21
There are some results that do not rely on Abelian conditions.

**Theorem 1.2.9.**

1. [Sc] If $L$ is a totally real number field or a totally complex quadratic extension of a totally real number field, then for any $\alpha \in L^\times$,

$$h(\alpha) \geq \frac{1}{2} \log \frac{1 + \sqrt{5}}{2} \approx 0.2406.$$  

Moreover, this bound is sharp since $\frac{1 + \sqrt{5}}{2}$ attains this height.†

2. [Sm2] The set $\{h(\alpha) : \alpha$ is a totally real algebraic number$\} \cap (0.2732832 \ldots, \infty)$ is dense in $(0.2732832 \ldots, \infty)$. The minimum value given by Schinzel is isolated within the set of heights of totally real algebraic numbers.

**Theorem 1.2.10.** [BoZa] Let $L$ be the field of totally $p$-adic numbers (i.e. the composite of the fields $K = \mathbb{Q}(\alpha)$ where $p$ splits completely in $K$). There exists a positive real number $C$ such that $\{\alpha \in L : h(\alpha) \leq C\}$ consists of all roots of unity in $L$. That is, for every $\alpha \in L^\times$ that is not a root of unity, there is an constant $C > 0$, possibly depending $p$, such that $h(\alpha) > C$.

**Theorem 1.2.11.** [Ga] Let $\alpha$ be an algebraic number not equal to $0$ or $\pm 1$ whose degree is $d$. Let $\Lambda$ be the set of Galois conjugates of $\alpha$ that are real, let $R_\alpha = |\Lambda|/d$, and let $\beta = 1 - 1/R_\alpha$. If $|\Lambda| \neq 0$, then

$$M(\alpha) \geq \left(\frac{2^\beta + \sqrt{4^\beta + 4}}{2}\right)^{dR_\alpha/2}.$$  

†A one-page proof of the totally real result is given in [HoSk].

22
Theorem 1.2.12. [Dr] Let \( \alpha \) be an algebraic number not equal to 0 or 1.

1. For \( \alpha \) a primitive sixth root of unity,
\[
h(\alpha) + h\left(\frac{1}{1-\alpha}\right) + h\left(1 - \frac{1}{\alpha}\right) = 0.
\]

2. Otherwise,
\[
h(\alpha) + h\left(\frac{1}{1-\alpha}\right) + h\left(1 - \frac{1}{\alpha}\right) \geq 0.4218\ldots,
\]
with equality for \( \alpha \) any root of the polynomial \( P(z) = (z^2 - z + 1)^3 - (z^2 - z)^2 \).

Theorem 1.2.13. [Si1] Let \( K \) be a number field of degree \( d \). If \( a_1, a_2, \ldots, a_d \) are linearly independent over \( \mathbb{Q} \), then \( H_K([a_1, a_2, \ldots, a_d]) \geq d^{-d/2}|D(K)|^{1/2} \), where \( D(K) \) is the discriminant of \( K \).

1.3 Elements and Bases of Minimal Height

Another line of research focuses on bounding the smallest height of certain elements of field bases from above. This is somewhat different than the results of the last section which all seem to have their origins in Lehmer’s Problem. There are a few principle articles that discuss these problems and they serve as the foundation for the main results of this work that are presented in the next chapter.

1.3.1 Results of Roy and Thunder

This section describes the ideas and results found in [RoTh]. Throughout this section, let \( K \) be a number field of degree \( d \) over \( \mathbb{Q} \).
Among all bases \( \{a_1, a_2, \ldots, a_d\} \) of \( K \) as a \( \mathbb{Q} \)-vector space, there is one that has smallest Weil height, when one considers the elements of the basis as a projective point defined over \( K \). Denote this smallest height value by \( B(K) \). Roy and Thunder consider the following question:

**Question.** For all \( d \geq 1 \), is there a constant \( c = c(d) \) such that

\[
B(K) \leq c(d)|D(K)|^{1/2}.
\]

For certain classes of number fields, the answer turns out to be “yes”. In particular, for totally real number fields this is the case. The proofs of the following three theorems are based on Minkowski’s Geometry of Numbers.

**Theorem 1.3.1.** If \( K \) is totally real, then

\[
B(K) \leq C_1(d)|D(K)|^{1/2},
\]

where \( C_1(d) = 2^{d(3d+1)/2} \). Moreover, there is a \( \mathbb{Z} \)-basis \( \{b_1, \ldots, b_d\} \) of \( \mathcal{O}_K \) with

\[
H_K([b_1, b_2, \ldots, b_d]) \leq \left( \frac{d}{2} \right)^d C_1(d)|D(K)|^{1/2}.
\]

Unfortunately, the proof of this theorem hinges on the fact that \( K \) is totally real, so it does not generalize to number fields that are not totally real. In order to compensate for this, a number arising from the ideal class group is needed.

**Definition.** Let \( K \) be a number field with ideal class group \( H \). The **class index** of \( K \), denoted by \( i(K) \), is defined by

\[
i(K) = \max_{C \in H} \min_{a \in C, \text{integral}} N(a).
\]

Note that \( K \) has class number 1 if and only if \( i(K) = 1 \).
Theorem 1.3.2. With $C_1(d)$ as in the previous theorem,

$$B(K) \leq C_1(d)^2 \frac{|D(K)|^{1/2}}{i(K)}.$$  

This result is good, as far as it goes. However, the relationship between $B(K)$ and $i(K)$ is not at all clear. When one restricts to imaginary quadratic extensions of $\mathbb{Q}$, this relationship is very explicit.

Theorem 1.3.3. If $K$ is an imaginary quadratic extension of $\mathbb{Q}$, then

$$\frac{|D(K)|}{4i(K)} \leq B(K) \leq \frac{|D(K)|}{3i(K)}.$$  

1.3.2 Results of Ruppert and Kihel

Ruppert discusses polynomial-heights of number field generators and this subsection is devoted to describing the ideas and results in [Ru]. Kihel proves one of Ruppert’s conjectures in certain cases [Ki]. This conjecture is settled completely in the next chapter, assuming the Generalized Riemann Hypothesis.

His first result is reminiscent of Silverman’s result mentioned at the end of the previous section.

Theorem 1.3.4. For every $n \in \mathbb{N}$ there is a real number $c_n > 0$ such that if $\alpha$ generates a number field $K$ of degree $n$ and discriminant $D_K$ then

$$\hat{H}(\alpha) \geq c_n |D_K|^{\frac{1}{2n-2}}.$$  

One can take $c_n = \frac{1}{n\sqrt{n}}$.

It leads him to ask the following question:
**Question.** Is there a number $d_n$ such that every number field of degree $n$ over $\mathbb{Q}$ has a generator with

$$\hat{H}(\alpha) \leq d_n|D_K|^{\frac{1}{2n-2}}?$$

While he is unable to answer this question in general, he is able to answer it in the quadratic field case.

**Theorem 1.3.5.**

(1) There is a real number $d_2$ such that every imaginary quadratic field $K$ has a generator $\alpha$ with $\hat{H}(\alpha) \leq d_2\sqrt{|D_K|}$.

(2) Every real quadratic field $K$ has a generator $\alpha$ with $\hat{H}(\alpha) \leq \sqrt{|D_K|}$. The element $\alpha$ may be chosen to be integral.

In order to show part (1) of this theorem, Ruppert first proves the following theorem, which shows the existence of a constant $d_2$ such that $\hat{H}_{\text{min}}(D) \leq d_2\sqrt{|D|}$.

**Theorem 1.3.6.**

$$\lim_{D \to -\infty} \frac{\hat{H}_{\text{min}}(D)}{\sqrt{|D|}} = \frac{1}{2},$$

where $D$ runs through the discriminant of imaginary quadratic fields and $\hat{H}_{\text{min}}(D) = \min\{\hat{H}(\alpha) : \mathbb{Q}(\alpha) \text{ is a quadratic extension of } \mathbb{Q} \text{ with discriminant } D\}$.

The constant $d_2$ is ineffective. Based on numeric calculations, he makes the following conjecture:

**Conjecture 1.3.7.**

$$\hat{H}_{\text{min}}(D) \leq \frac{41}{\sqrt{163}}\sqrt{|D|} < 3.22\sqrt{|D|}$$

for every imaginary quadratic discriminant $D$. 

26
Assuming the Generalized Riemann Hypothesis, this conjecture is shown to be true in Corollary 2.5.8 below. However, Kihel [Ki] proves this conjecture unconditionally when $D \equiv 1 \pmod{3}, D \equiv \pm 1 \pmod{5}$, or $D \equiv 1 \pmod{8}$ by proving the following result:

**Theorem 1.3.8.** If $K$ is an imaginary quadratic extension of discriminant $D$ and $p$ is the smallest prime that splits completely in $K$, then there exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$ and $\hat{H}(\alpha) \leq \frac{p}{\sqrt{5}} \sqrt{|D|}$.

Ruppert draws two conclusions from part (2) of Theorem 1.3.5 and some calculations:

$$\frac{1}{\sqrt{5}} \leq \frac{\hat{H}_{\min}(D)}{\sqrt{D}} < 1 \quad \text{and} \quad \liminf_{D \to \infty} \frac{\hat{H}_{\min}(D)}{\sqrt{D}} = \frac{1}{\sqrt{5}},$$

where $D$ ranges over discriminants of real quadratic extensions. This leads him to the following conjecture:

**Conjecture 1.3.9.**

$$\lim_{D \to \infty} \frac{\hat{H}_{\min}(D)}{\sqrt{D}} = \frac{1}{\sqrt{5}}.$$

He is unable to prove this conjecture, but points to numeric evidence that seems to support it. A similar conjecture is presented as Conjecture 2.6.7 in the next chapter.

In addition to these, Ruppert shows the following interesting result by appealing to the geometry of numbers and points out that it does not generalize to number fields that are not totally real.

**Theorem 1.3.10.** If $K$ is a totally real number field of prime degree $p$, then there is an integral $\alpha \in K$ with $K = \mathbb{Q}(\alpha)$ such that

$$\hat{H}(\alpha) \leq 2^p \sqrt{D_K}.$$
CHAPTER 2
MAIN RESULTS

2.1 Preliminaries for Theorems 2.2.1, 2.2.2, and 2.2.3.

This section presents a series of computational lemmas that are needed for the proofs of Theorems 2.2.1, 2.2.2, and 2.2.3 in the next section. The symbol $\lfloor x \rfloor$ denotes the floor of the real number $x$; that is, it denotes the largest integer smaller or equal to $x$.

**Lemma 2.1.1.** For any positive integer $d$, $\lfloor \sqrt{d} \rfloor^2$ is the largest square smaller than or equal to $d$.

*Proof.* Clear: if $n^2 \leq d$, then $|n| = \lfloor \sqrt{n^2} \rfloor \leq \lfloor \sqrt{d} \rfloor$ so that $n^2 \leq \lfloor \sqrt{d} \rfloor^2$. $\square$

**Lemma 2.1.2.** Let $d$ be a positive integer.

$$d - (\lfloor \sqrt{d} \rfloor - 1)^2 = (\sqrt{d} - \lfloor \sqrt{d} \rfloor + 1)(\sqrt{d} + \lfloor \sqrt{d} \rfloor - 1) < \sqrt{d} + \lfloor \sqrt{d} \rfloor$$

if and only if $d$ is a square or $d - 1$ is a square.

*Proof.*

$$\begin{align*}
(\sqrt{d} - \lfloor \sqrt{d} \rfloor + 1)(\sqrt{d} + \lfloor \sqrt{d} \rfloor - 1) - (\sqrt{d} + \lfloor \sqrt{d} \rfloor) &= \\
&= d + 2\lfloor \sqrt{d} \rfloor - [\sqrt{d}]^2 - 1 - \sqrt{d} - [\sqrt{d}] = \\
&= d - [\sqrt{d}]^2 - 1 - \sqrt{d} + [\sqrt{d}],
\end{align*}$$
so the inequality in the statement of the lemma is the same as

\[ d - \lfloor \sqrt{d} \rfloor^2 + (\lfloor \sqrt{d} \rfloor - \sqrt{d} - 1) < 0. \]

By Lemma 2.1.1, \( d - \lfloor \sqrt{d} \rfloor^2 \) is exactly how much \( d \) differs from the largest square smaller than itself; in particular, \( d - \lfloor \sqrt{d} \rfloor^2 \geq 2 \) if and only if neither \( d \) nor \( d - 1 \) is a square. Since \( \lfloor \sqrt{d} \rfloor - \sqrt{d} \in (-1, 0) \) if \( d \) is not a square and \( \lfloor \sqrt{d} \rfloor - \sqrt{d} = 0 \) if \( d \) is a square, \( d - \lfloor \sqrt{d} \rfloor^2 + (\lfloor \sqrt{d} \rfloor - \sqrt{d} - 1) \in \begin{cases} (0, \infty) & \text{if neither } d \text{ nor } d - 1 \text{ is a square} \\ \{ -1 \} & \text{if } d \text{ is a square} \\ (-1, 0) & \text{if } d - 1 \text{ is a square.} \end{cases} \]

\[ \square \]

**Lemma 2.1.3.** Let \( d \geq 4 \) be an integer. For \( n \in \{ 0, 1, 2, \ldots, \lfloor \sqrt{d} \rfloor - 2 \} \), \((\sqrt{d} - 1)^2 \geq n^2 + 1\).

*Proof.* The right-hand side of this inequality increases as \( n \) increases, so the desired inequality is implied by the one with \( n \) replaced by \( \lfloor \sqrt{d} \rfloor - 2 \).

\[
(\sqrt{d} - 1)^2 - (\lfloor \sqrt{d} \rfloor - 2)^2 - 1 = d - 2\sqrt{d} + 1 - \lfloor \sqrt{d} \rfloor^2 + 4\lfloor \sqrt{d} \rfloor - 4 - 1
\]

\[
= d - \lfloor \sqrt{d} \rfloor^2 + 2(2\lfloor \sqrt{d} \rfloor - \sqrt{d}) - 4,
\]

so the inequality in the statement is implied by the inequality

\[ d - \lfloor \sqrt{d} \rfloor^2 + 2(2\lfloor \sqrt{d} \rfloor - \sqrt{d}) - 4 \geq 0. \]

Since Lemma 2.1.1 shows that \( d - \lfloor \sqrt{d} \rfloor^2 \geq 0 \), in order to show that this new inequality holds it suffices to show that \( 2\lfloor \sqrt{d} \rfloor - \sqrt{d} \geq 2 \). Note that for \( d \geq 9 \), \( \lfloor \sqrt{d} \rfloor \geq 3 \). Hence, \( 2\lfloor \sqrt{d} \rfloor - \sqrt{d} = [\sqrt{d}] + ([\sqrt{d}] - \sqrt{d}) \geq 3 - 1 = 2 \). For \( d \in \{4, 5, 6, 7, 8\} \), \( n = 0 \) and \((\sqrt{d} - 1)^2 \geq (2 - 1)^2 = 0^2 + 1 \).

\[ \square \]
Lemma 2.1.4. Let $d \geq 16$ be an integer such that $\frac{\sqrt{d}}{2} \in \mathbb{N}$. For $n$ in the set $
ids{1, 2, \ldots, \left(\frac{\sqrt{d}}{2} - 1\right)}$, 
\[
\left(\frac{d - \lfloor \sqrt{d} \rfloor^2}{4}\right) - \left(n^2 + (1 - \lfloor \sqrt{d} \rfloor)n + \frac{1}{4} - \frac{\lfloor \sqrt{d} \rfloor}{2}\right) > \frac{\sqrt{d} + \lfloor \sqrt{d} \rfloor - 1}{2}.
\]

Proof. Let $m = \lfloor \sqrt{d} \rfloor \in \mathbb{N}$ and $r \in [0, 1)$ such that $\sqrt{d} = m + r$ so that $d = (m + r)^2$. The inequality in the statement of the theorem is the same as 
\[
\frac{(m + r)^2 - m^2}{4} - \left(n^2 + (1 - m)n + \frac{1}{4} - \frac{m}{2}\right) > \frac{m + r + m - 1}{2},
\]
where $n \in \{1, 2, \ldots, \frac{m}{2} - 1\}$. Since $n^2 + (1 - m)n + \frac{1}{4} - \frac{m}{2} = (n + \frac{1}{2})(n - m + \frac{1}{2})$, this inequality is the same as 
\[
\left(n + \frac{1}{2}\right)\left(n - m + \frac{1}{2}\right) < \frac{(2m + r)(r - 2) + 2}{4}.
\]

The (convex) quadratic polynomial in $n$ on the left-hand side has minimum at 
\[
\frac{\frac{1}{2} + \frac{m - 1}{2}}{2} = \frac{m - 1}{2} = \frac{m}{2} - \frac{1}{2} > \frac{m}{2} - 1.
\]
Hence, the maximum value of this polynomial on the interval $[1, \frac{m}{2} - 1]$ occurs at $n = 1$. Therefore, the desired inequality is implied by 
\[
\left(1 + \frac{1}{2}\right)\left(1 - m + \frac{1}{2}\right) < \frac{(2m + r)(r - 2) + 2}{4},
\]
i.e. by 
\[
8 - 2m < 2mr + (r - 1)^2.
\]

For $m \geq 4$, this inequality holds because the left-hand side is non-positive while the right-hand side is strictly positive. Since $d \geq 16$ and $m = \lfloor \sqrt{d} \rfloor, m \geq 4$ so that the desired inequality holds for all $d \geq 16$. \hfill $\Box$
Lemma 2.1.5. Let $d \geq 25$ be an integer such that $\frac{\lceil \sqrt{d} \rceil - 1}{2} \in \mathbb{N}$. For each $n$ in the set \( \{1, 2, \ldots, \frac{\lceil \sqrt{d} \rceil - 1}{2} - 1\} \),
\[
\left( \frac{d - \lceil \sqrt{d} \rceil^2}{4} \right) - (n^2 - (\lceil \sqrt{d} \rceil - 2)n - (\lceil \sqrt{d} \rceil - 1)) > \frac{\sqrt{d} + \lceil \sqrt{d} \rceil}{2}.
\]

Proof. Let $m = \lceil \sqrt{d} \rceil \in \mathbb{N}$ and $r \in [0, 1)$ such that $\sqrt{d} = m + r$ so that $d = (m + r)^2$. The inequality in the statement of the theorem is the same as
\[
\frac{(m + r)^2 - m^2}{4} - (n^2 - (m - 2)n - (m - 1)) > \frac{m + r + m}{2},
\]
where $n \in \{1, 2, \ldots, \frac{m-1}{2} - 1\}$. Since $n^2 - (m - 2)n - (m - 1) = (1 - m + n)(n + 1)$, this inequality is the same as
\[
(1 - m + n)(n + 1) < \frac{(2m + r)(r - 2)}{4}.
\]
The (convex) quadratic polynomial in $n$ on the left-hand side has minimum at \( \frac{-1 + m - 1}{2} = \frac{m-2}{2} = \frac{m}{2} - 1 > \frac{m-1}{2} - 1 \). Hence, the maximum value of this polynomial on the interval $[1, \frac{m}{2} - 1]$ occurs at $n = 1$. Therefore, the desired inequality is implied by
\[
(1 - m + 1)(1 + 1) < \frac{(2m + r)(r - 2)}{4},
\]
i.e. by
\[
8(m - 2) > (2 - r)(2m + r).
\]
The (concave) quadratic polynomial in $r$ on the right-hand side of this inequality has maximum at $1 - m < 0$ so that it attains its maximum on $[0, 1)$ at 0. Hence, the desired inequality is implied by
\[
8(m - 2) > 4m \geq (2 - r)(2m + r),
\]
31
i.e. by

\[ 4m > 16. \]

For \( m \geq 5 \), this inequality holds. Since \( d \geq 25 \) and \( m = \lfloor \sqrt{d} \rfloor \), \( m \geq 5 \) so that the desired inequality holds for all \( d \geq 25 \). \( \square \)

**Lemma 2.1.6.** For any positive integer \( d \), \( 2\lfloor \sqrt{d} \rfloor \geq d - \lfloor \sqrt{d} \rfloor^2 \).

**Proof.** For each value of \( \lfloor \sqrt{d} \rfloor \), the right-hand side of the inequality is maximized when \( d + 1 \) is a square, by Lemma 2.1.1. Suppose that this is the case, since the general inequality will then follow. Note that, in this case, \( \sqrt{d+1} - \lfloor \sqrt{d} \rfloor = 1 \).

\[
2\lfloor \sqrt{d} \rfloor \geq d - \lfloor \sqrt{d} \rfloor^2 \iff 2\lfloor \sqrt{d} \rfloor + 1 \geq d - \lfloor \sqrt{d} \rfloor^2 + 1 \\
\iff 2\lfloor \sqrt{d} \rfloor + 1 \geq (\sqrt{d+1} - \lfloor \sqrt{d} \rfloor)(\sqrt{d+1} + \lfloor \sqrt{d} \rfloor) \\
\iff 2\lfloor \sqrt{d} \rfloor + 1 \geq \sqrt{d+1} + \lfloor \sqrt{d} \rfloor \\
\iff \lfloor \sqrt{d} \rfloor + 1 \geq \sqrt{d+1}.
\]

The final inequality is actually an equality. \( \square \)

**Lemma 2.1.7.** Let \( d \) be a positive integer.

\[
(\sqrt{d} - \lfloor \sqrt{d} \rfloor + 2)(\sqrt{d} + \lfloor \sqrt{d} \rfloor - 2) < 2(\sqrt{d} + \lfloor \sqrt{d} \rfloor)
\]

if and only if one of \( d, d - 1, d - 2, d - 3, d - 4 \) is a square or \( d \) equals 14 or 21.
Proof.

\[
(\sqrt{d} - \lfloor \sqrt{d} \rfloor + 2)(\sqrt{d} + \lfloor \sqrt{d} \rfloor - 2) - 2(\sqrt{d} + \lfloor \sqrt{d} \rfloor) = \\
d + \sqrt{d}\lfloor \sqrt{d} \rfloor - 2\sqrt{d} - \sqrt{d}\lfloor \sqrt{d} \rfloor - \lfloor \sqrt{d} \rfloor^2 + \\
2\lfloor \sqrt{d} \rfloor + 2\sqrt{d} + 2\lfloor \sqrt{d} \rfloor - 4 - 2\sqrt{d} - 2\lfloor \sqrt{d} \rfloor = \\
d - 2\sqrt{d} - \lfloor \sqrt{d} \rfloor^2 + 2\lfloor \sqrt{d} \rfloor - 4 = \\
(d - \lfloor \sqrt{d} \rfloor^2 - 4) - 2(\sqrt{d} - \lfloor \sqrt{d} \rfloor),
\]

so the inequality in the statement is the same as

\[
d - \lfloor \sqrt{d} \rfloor^2 - 4 < 2(\sqrt{d} - \lfloor \sqrt{d} \rfloor).
\]

The function \(\sqrt{d} - \lfloor \sqrt{d} \rfloor\) is cumbersome to work with directly as \(d\) increases. Instead, fix a natural number \(\ell\) and consider the function \(\sqrt{m^2 + \ell} - \lfloor \sqrt{m^2 + \ell} \rfloor\) where \(m\) is a natural number. (That is, \(d\) is \(\ell\) more than the square integer \(m^2 = \lfloor \sqrt{d} \rfloor^2\) so that the left-hand side of the above inequality is equal to \(\ell - 4\).) For \(m\) such that \(m^2 + \ell < (m+1)^2\), this is equal to \(\sqrt{m^2 + \ell} - m\). By using calculus, it is clear that this function decreases to zero as \(m\) increases to infinity. Hence, Lemma 2.1.1 shows that, for \(\ell\) equal to 5 and \(d\) ranging over the values of \(m^2 + \ell\) such that \(m^2 + \ell < (m+1)^2\) (recall that the left-hand side is equal to \(\ell - 4\) and \((\sqrt{d} - \lfloor \sqrt{d} \rfloor) \in [0,1]\)), the above inequality will fail to hold for large enough values of \(m\) and for \(\ell \geq 6\) with \(d\) ranging over the values of \(m^2 + \ell\) such that \(m^2 + \ell < (m+1)^2\) the inequality will always fail. Testing small values of \(d\) gives exactly those numbers in the statement of the lemma.

Finally, direct computation or Lemma 2.1.1 shows that the inequality holds when one of \(d, d-1, d-2, d-3\), or \(d-4\) is a square. \(\square\)
The final lemma of this section is a reduction lemma. It allows one to reduce some arguments about generators of quadratic fields to generators of certain convenient forms.

**Lemma 2.1.8.** Let $d$ be a squarefree integer. For $x \in \mathbb{Q}(\sqrt{d})$, let $\overline{x}$ denote the Galois conjugate of $x$ and recall that $H(x)$ denotes the height of $x$.

1. If $d \not\equiv 1 \pmod{4}$ and $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathbb{Q}(\sqrt{d})$ with $a, b, c \in \mathbb{Z}$ and $bc \neq 0$, then there is $\beta \in \{\alpha, \overline{\alpha}, -\alpha, -\overline{\alpha}\}$, $\beta = \frac{a'+b'\sqrt{d}}{c'}$ and $a', b', c' \in \mathbb{Z}$ with $a' \geq 0$ and $b', c' > 0$ such that $H\left(\frac{a'+b'\sqrt{d}}{c'}\right) = H(\alpha)$.

2. If $d \equiv 1 \pmod{4}$ and $\alpha = \frac{a+b\frac{1+\sqrt{d}}{2}}{c} \in \mathbb{Q}(\sqrt{d})$ with $a, b, c \in \mathbb{Z}$ and $bc \neq 0$, then there is $\beta \in \{\alpha, \overline{\alpha}, -\alpha, -\overline{\alpha}\}$, $\beta = \frac{a'+b'\frac{1+\sqrt{d}}{2}}{c'}$ and $a', b', c' \in \mathbb{Z}$ either with $a' \geq 0$ and $b', c' > 0$ or with $a' < 0$ and $b', c' > 0$ with $|a'| \leq \left\lfloor \frac{b'}{2} \right\rfloor$ such that $H\left(\frac{a'+b'\frac{1+\sqrt{d}}{2}}{c'}\right) = H(\alpha)$.

**Proof.** In all cases, take $c' = \text{sgn}(c) \cdot c$. Recall that height is unchanged by taking Galois conjugates and multiplying by roots of unity, Propositions 1.1.7 and 1.1.8.

For (1), note that $\overline{\alpha} = \frac{a-b\sqrt{d}}{c}$. If $a \leq 0$ and $b < 0$, then replace $\alpha$ by $-\alpha$, i.e. take $a' = -a$ and $b' = -b$. If $a \geq 0$ and $b < 0$, then replace $\alpha$ by $\overline{\alpha}$, i.e. take $a' = a$ and $b' = -b$. If $a \leq 0$ and $b > 0$, then replace $\alpha$ by $-\overline{\alpha}$, i.e. take $a' = -a$ and $b' = b$.

For (2), note that $\overline{\alpha} = \frac{a+b\frac{1-\sqrt{d}}{2}}{c}$. If $a = 0$ and $b < 0$, then replace $\alpha$ by $-\alpha$, i.e. take $a' = 0$ and $b' = -b$. If $a < 0$ and $b < 0$, then replace $\alpha$ by $-\alpha$, i.e. take $a' = -a$ and $b' = -b$. If $a > 0$, $b < 0$, and $|a| \geq \left\lfloor \frac{b}{2} \right\rfloor$, then replace $\alpha$ by $\overline{\alpha}$, i.e. take $a' = a+b$ and $b' = -b$; when $|a| \geq |b|$, this gives $a', b' > 0$, and when $|a| < |b|$ (recall...
that $|a| \geq |\frac{b}{2}|$) this gives $a' < 0, b' > 0$ and $|a'| \leq |\frac{b'}{2}|$. If $a > 0, b < 0$, and $|a| < |\frac{b}{2}|$, then replace $\alpha$ by $-\alpha$, i.e. take $a' = -a$ and $b' = -b$. If $a < 0, b > 0$, and $|a| > |\frac{b}{2}|$, then replace $\alpha$ by $-\overline{\alpha}$, i.e. take $a' = -a - b$ and $b' = b$; when $|a| \geq |b|$, this gives $a', b' \geq 0$, and when $|a| < |b|$ (recall that $|a| > |\frac{b}{2}|$) this gives $a' < 0, b' > 0$ and $|a'| < |\frac{b'}{2}|$.

2.2 Integral Generators of Smallest Height in $\mathbb{Q}(\sqrt{d})$.

Theorems 2.2.1, 2.2.2, and 2.2.3 give very explicit results about minimal heights of integral generators of quadratic fields. The dichotomy between real and imaginary quadratic fields is evident in terms of the orders of magnitude of these heights. The order of magnitude results are very interesting in light of the results of Section 2.5 and make some proofs in Section 2.6 very easy.

**Theorem 2.2.1.** Let $d \not\equiv 1 \pmod{4}$ be a positive, squarefree integer. Let $N$ denote the smallest height of an algebraic integer that generates $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$.

$$N = \begin{cases} 
\sqrt{d} + \lfloor \sqrt{d} \rfloor & \text{if } d - 1 \text{ is not a square} \\
2\lfloor \sqrt{d} \rfloor = d - (\lfloor \sqrt{d} \rfloor - 1)^2 & \text{if } d - 1 \text{ is a square.}
\end{cases}$$

These heights are achieved by $\sqrt{d} + \lfloor \sqrt{d} \rfloor$ and $\sqrt{d} + \lfloor \sqrt{d} \rfloor - 1$, respectively, as well as their negatives and the Galois conjugates of all of these elements; these are all of the integral generators with minimal height.
Theorem 2.2.2. Let $d \neq 1, d \equiv 1 \pmod{4}$ be a positive, squarefree integer. Let $N$ denote the smallest height of an algebraic integer that generates $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$.

$$N = \begin{cases} \frac{\sqrt{d} + |\sqrt{d}|}{2} & \text{if } |\sqrt{d}| \text{ is odd and } d - 4 \text{ is not a square} \\ |\sqrt{d}| & \text{if } |\sqrt{d}| \text{ is odd and } d - 4 \text{ is a square} \\ \frac{\sqrt{d} + |\sqrt{d}| - 1}{2} & \text{if } |\sqrt{d}| \text{ is even} \end{cases}$$

These heights are achieved by $\frac{\sqrt{d} + |\sqrt{d}|}{2}, \frac{\sqrt{d} + |\sqrt{d}|}{2} - 1$, and $\frac{\sqrt{d} + |\sqrt{d}| - 1}{2}$ respectively, as well as their negatives and the Galois conjugates of all of these elements; these are all of the integral generators with minimal height.

Theorem 2.2.3. Let $d$ be a negative, squarefree integer. Let $N$ denote the smallest height of an algebraic integer that generates $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$.

$$N = \begin{cases} \frac{|d| + 1}{4} & \text{if } d \equiv 1 \pmod{4} \\ |d| & \text{if } d \not\equiv 1 \pmod{4} \end{cases}$$

These heights are achieved by $\frac{1 + \sqrt{|d|}}{2}$ and $\sqrt{|d|}$, respectively, as well as their products with any roots of unity lying in the field and the Galois conjugates of all of these elements; these are all of the integral generators with minimal height.

In the last statements of these theorems, it is possible that there are other (non-integer) elements that also have the minimal heights among integers. (In particular, the inverses of the listed elements also have the desired heights.) This can lead to some interesting examples.

Example 1. In $\mathbb{Q}(\sqrt{3})$, $\frac{\sqrt{3} - 1}{2}$ has the same height as $\sqrt{3} - 1$ (and $\sqrt{3} + 1 = \sqrt{3} + |\sqrt{3}|$) since $2 = (\sqrt{3} - 1)(\sqrt{3} + 1)$.
Example 2. In $\mathbb{Q}(\sqrt{-163})$, it turns out that an integral generator of smallest height, $\frac{1+\sqrt{-163}}{2}$, has the smallest height of all generators in this field. It shares the same height as both $\frac{1+\sqrt{-163}}{82}$ and $\frac{1+\sqrt{-163}}{41}$. The element with denominator 82 is the Galois conjugate of the inverse of the element with denominator 2. An explanation for why the elements with denominators 41 and 82 have the same height is given later, in Theorem 2.3.4.

Proof. (of Theorem 2.2.1) The first part of the last sentence is clear by the definition of height and direct computation. The second part of the last sentence follows from Proposition 1.1.7. The third part of the last sentence will become evident below, following from Lemma 2.1.8.

The ring of integers $\mathcal{O}_d$ in $\mathbb{Q}(\sqrt{d})$ is exactly $\mathbb{Z} + \sqrt{d}\mathbb{Z}$. The height of an element in this ring is $\max\{1, |a + b\sqrt{d}|\} \cdot \max\{1, |a - b\sqrt{d}|\}$. Let $\alpha = a + b\sqrt{d} \in \mathcal{O}_d$ and $\beta = \sqrt{d} + \lfloor \sqrt{d} \rfloor$. It suffices to assume that $a \geq 0$ and $b > 0$, since every $\alpha \in \mathcal{O}_d$ shares height with such an element, by Lemma 2.1.8.

If $b > 1$, then $H(\alpha) > \sqrt{d} + \lfloor \sqrt{d} \rfloor = H(\beta)$ because

$$H(\alpha) \geq \alpha = a + b\sqrt{d} \geq \sqrt{d} + \sqrt{d} > \sqrt{d} + \lfloor \sqrt{d} \rfloor.$$ 

If $b = 1$, then Lemmas 2.1.2 and 2.1.3 will combine to give the result. First, if $a \leq \lfloor \sqrt{d} \rfloor - 1$, then $H(\alpha) = (\sqrt{d} - a)(\sqrt{d} + a) = d - a^2$ since $\sqrt{d} + a$ and $\sqrt{d} - a$ are
both larger than 1. If \( a \leq \lfloor \sqrt{d} \rfloor - 2 \), then \( \lfloor \sqrt{d} \rfloor \geq 2 \) so that \( d > 4 \) and Lemma 2.1.3 shows that \( d - 2\sqrt{d} + 1 \geq a^2 + 1 \) i.e. that

\[
H(\alpha) = d - a^2 \\
\geq 2\sqrt{d} \\
> \beta \\
= H(\beta).
\]

Next, if \( a > \lfloor \sqrt{d} \rfloor \), then

\[
H(\alpha) \geq \alpha \\
> \beta \\
= H(\beta).
\]

Finally, there are only two remaining cases: \( a = \lfloor \sqrt{d} \rfloor \) and \( a = \lfloor \sqrt{d} \rfloor - 1 \), i.e. \( \alpha = \beta \) and \( \alpha = \beta - 1 \). Lemma 2.1.2 shows that \( H(\beta - 1) \leq H(\beta) \) if and only if \( d - 1 \) is a square. (Note that Lemma 2.1.2 shows that \( d - 1 \) not a square implies that \( H(\beta) \leq H(\beta - 1) \). But since \( H(\beta) \in \mathbb{Q} \) and \( H(\beta - 1) \not\in \mathbb{Q} \), the inequality is in fact strict.) Hence, up to sign and Galois conjugation, \( \beta \) (or \( \beta - 1 \)) is the unique generator when \( d - 1 \) is not (or is) a square.

\( \square \)

**Proof.** (of Theorem 2.2.2) The first part of the last sentence is clear by the definition of height and direct computation. The second part of the last sentence follows from Proposition 1.1.7. The third part of the last sentence will become evident below, following from Lemma 2.1.8.
The ring of integers $\mathcal{O}_d$ in $\mathbb{Q}(\sqrt{d})$ is exactly $\mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}$. The height of an element in this ring is $\max\left\{1, \left|a + b\frac{1+\sqrt{d}}{2}\right|\right\} \cdot \max\left\{1, \left|a + b\frac{1-\sqrt{d}}{2}\right|\right\}$. Let $\alpha = a + b\frac{1+\sqrt{d}}{2} \in \mathcal{O}_d$.

It suffices to assume that either $a \geq 0, b > 0$ or $|a| \leq \left\lfloor \frac{b}{2} \right\rfloor$ with $a < 0, b > 0$, since every $\alpha \in \mathcal{O}_d$ shares height with such an element, by Lemma 2.1.8.

If $a \geq 0, b > 1$, then

$$H(\alpha) \geq a + b\frac{1+\sqrt{d}}{2} \geq b\frac{1+\sqrt{d}}{2} \geq 1 + \sqrt{d} > \sqrt{d} > \frac{\sqrt{d} + |\sqrt{d}|}{2}.$$  

If $|a| \leq \left\lfloor \frac{b}{2} \right\rfloor$ with $a < 0, b > 1$, then since $|a| = \left|\frac{b}{2} - |a| + \frac{b}{2}\sqrt{d}\right| \geq \frac{b}{2}\sqrt{d} \geq \sqrt{d} > 1$ and $|\alpha| = \left|\frac{b}{2} - |a| - \frac{b}{2}\sqrt{d}\right| = \frac{b}{2}\sqrt{d} - (\frac{b}{2} - |a|) > b - \frac{b}{2} = \frac{b}{2} \geq 1$,

$$H(\alpha) = N((\alpha)) = \left|a^2 + ab - \frac{b^2}{4}(d - 1)\right| = \frac{b^2}{4}(d - 1) - ab - a^2 \geq d - 1 + 1 = d > \sqrt{d} > \frac{\sqrt{d} + |\sqrt{d}|}{2}.$$  

Here, the second equality is by definition, the third follows from the conditions on $a$ and $b$ ($a < 0$ and $b \geq -a > 0$ so that $-ab - a^2 > 0$, i.e. $-ab - a^2 \geq 1$), and the first inequality follows from the fact that $b \geq 2$ and $-ab - a^2 > 0$. Hence, if $b > 1$, then $H(\alpha) > \frac{\sqrt{d} + |\sqrt{d}|}{2}$.

If $b = 1$, then $a \geq 0$ because either $a \geq 0$ or $0 < |a| \leq \left\lfloor \frac{b}{2} \right\rfloor = \frac{1}{2}$ and the latter
is impossible. Now suppose that $b = 1$. As noted above, it suffices to assume that $a \geq 0$.

**Subcase 1:** $\lfloor \sqrt{d} \rfloor$ is even.

If $d = 5$, then direct computation shows that $\frac{1+\sqrt{5}}{2} = \sqrt{\frac{\lfloor \sqrt{d} \rfloor + 1}{2}}$ has minimal height.

If $0 \leq a \leq \frac{\lfloor \sqrt{d} \rfloor}{2} - 2$, say $a = \frac{\lfloor \sqrt{d} \rfloor}{2} - 1 - n$ for some integer $n \in \{1, 2, \ldots, \left(\frac{\lfloor \sqrt{d} \rfloor}{2} - 1\right)\}$, then $|\alpha| = \left| (a + 1) - \frac{1+\sqrt{d}}{2} \right| = \sqrt{\frac{d-\lfloor \sqrt{d} \rfloor + 1}{2}} + n$. Since this is larger than $\frac{3}{2}$,

$$H(\alpha) = N(\alpha) = \left| \left( d - \left\lfloor \sqrt{\frac{d}{4}} \right\rfloor \right)^2 \right| + \left\lfloor \sqrt{\frac{d}{4}} \right\rfloor \left| \frac{\sqrt{d}}{2} - \left( n^2 + (1 - \left\lfloor \sqrt{d} \right\rfloor) n + \frac{1}{4} \right) \right|.$$  

Hence, since $0 \leq a \leq \frac{\lfloor \sqrt{d} \rfloor}{2} - 2$ implies that $\lfloor \sqrt{d} \rfloor \geq 4$ so that the squarefree integer $d$ is at least 17, Lemma 2.1.4 shows that this is larger than $\frac{\sqrt{d}+\lfloor \sqrt{d} \rfloor - 1}{2}$.

If $a \geq \frac{\lfloor \sqrt{d} \rfloor}{2}$, say $a = \frac{\lfloor \sqrt{d} \rfloor}{2} + n$ for some non-negative integer $n$, then, since

$$|\alpha| = \left| a + 1 - \frac{1+\sqrt{d}}{2} \right|$$

$$= \left| \frac{\sqrt{d}}{2} + n + 1 - \frac{1}{2} - \frac{\sqrt{d}}{2} \right|$$

$$= \left| n + 1 - (\sqrt{d} - \lfloor \sqrt{d} \rfloor) \right|$$

$$\begin{cases} > n \geq 1 & \text{if } n > 0 \\ < 1 & \text{if } n = 0, \end{cases}$$

$$H(\alpha) = N(\alpha) \text{ when } n > 0 \text{ and } H(\alpha) = \alpha > \frac{\sqrt{d}+\lfloor \sqrt{d} \rfloor - 1}{2} = H\left( \frac{\sqrt{d}+\lfloor \sqrt{d} \rfloor - 1}{2} \right)$$
\( n = 0. \) Using Lemmas 2.1.1 and 2.1.6 when \( n \geq 1 \) shows that

\[
N((\alpha)) = \frac{1 + 2n|\sqrt{d}| - (d - |\sqrt{d}|^2)}{4} + \frac{n + 1}{2} [\sqrt{d}] + n^2 + n
\]

\[
> \frac{|\sqrt{d}|}{2}
\]

\[
= \frac{|\sqrt{d}| + |\sqrt{d}|}{2}
\]

\[
> \frac{\sqrt{d} - 1 + |\sqrt{d}|}{2}.
\]

Hence, the minimal height in this case occurs when \( a = \frac{|\sqrt{d}|}{2} - 1, b = 1, \) i.e. when \( \alpha = \sqrt{d} + |\sqrt{d}| - 1. \)

Subcase 2: \( |\sqrt{d}| \) is odd.

If \( 0 \leq a \leq \frac{|\sqrt{d}| - 1}{2} - 1 \), say \( a = \frac{|\sqrt{d}| - 1}{2} - 1 - n \) for some \( n \in \{1, 2, \ldots, \frac{|\sqrt{d}| - 1}{2} - 1\} \), then \( |\alpha| = |(a + 1) - \frac{1 + \sqrt{d}}{2}| = \frac{1 + \sqrt{d}}{2} - 1 - \frac{|\sqrt{d}| - 1}{2} + n + 1 = \frac{\sqrt{d} + |\sqrt{d}|}{2} + n + 1. \) Since this is larger than 1,

\[
H(\alpha) = N((\alpha)) = \left| \left( d - \frac{|\sqrt{d}|^2}{4} \right) - (n^2 - ([\sqrt{d}] - 2)n - ([\sqrt{d}] - 1)) \right|. \]

Lemma 2.1.5 shows that, when \( n > 0 \), this is larger than \( \frac{\sqrt{d} + |\sqrt{d}|}{2} \) (which is larger than \( |\sqrt{d}| \)).

If \( a \geq \frac{|\sqrt{d}| - 1}{2} + 1 \), say \( a = \frac{|\sqrt{d}| - 1}{2} + 1 + n \) for some non-negative integer \( n \), then,
since

\[ |\alpha| = \left| a + 1 - \frac{1 + \sqrt{d}}{2} \right| \]

\[ = \left| \frac{\sqrt{d} - 1}{2} n + 2 - \frac{1 - \sqrt{d}}{2} \right| \]

\[ = \left| n + 1 + \frac{\sqrt{d} - \sqrt{d}}{2} \right| \]

\[
\begin{cases}
> n \geq 1 & \text{if } n > 0 \\
< 1 & \text{if } n = 0,
\end{cases}
\]

\[ H(\alpha) = N((\alpha)) \text{ when } n \geq 1 \text{ and } H(\alpha) = \alpha = \frac{\sqrt{d} + 1}{2} + \frac{1 + \sqrt{d}}{2} > \frac{\sqrt{d} + \sqrt{d}}{2} \text{ when } n = 0. \]

But, by Lemma 2.1.6,

\[ N((\alpha)) = \frac{2(\sqrt{d} - (d - [\sqrt{d}]^2)) + n^2 + (2 + [\sqrt{d}]n + \frac{\sqrt{d}}{2} + 1}{4} \]

\[ \geq \frac{3}{2} [\sqrt{d}] \]

\[ > \frac{\sqrt{d} + [\sqrt{d}]}{2}. \]

There are only two remaining values of \( a \left( \frac{[\sqrt{d}]-1}{2} \text{ and } \frac{[\sqrt{d}]-1}{2} - 1 \right) \). Lemma 2.1.7 now completes the proof. Note that, since \( d \equiv 1 \text{ (mod 4) } \), neither of \( d - 2 \) or \( d - 3 \) can be squares. Also note that, since \( [\sqrt{d}] \) is odd and \( d \equiv 1 \text{ (mod 4) } \), \( d - 1 \) cannot be a square.

**Proof. (of Theorem 2.2.3)** The first part of the last sentence is clear by the definition of height and direct computation. The second part of the last sentence follows from Proposition 1.1.7. The third part of the last sentence will become evident below, following from Lemma 2.1.8.
The rings of integers in this case are as noted in the proofs of Theorems 2.2.1 and 2.2.2. Since \( \mathbb{Q}(\sqrt{d}) \) is totally imaginary with only one complex-conjugate pair of embeddings, the height of any integer is equal to the absolute value of its norm. In the \( d \not\equiv 1 \pmod{4} \) case, \( \alpha = a + b\sqrt{d} \) has norm \( a^2 + |d|b^2 \) which is clearly minimized among integral generators when \( a = 0 \) and \( |b| = 1 \). In the \( d \equiv 1 \pmod{4} \) case, \( \alpha = a + b\frac{1+\sqrt{d}}{2} \) has norm \( |a^2 + ab - b^2\frac{d+1}{4}| \). By Lemma 2.1.8, it suffices to assume that either \( a \geq 0, b \geq 1 \) or \( |a| \leq \frac{|b|}{2} \) with \( a < 0, b \geq 1 \). In the first case, \( N((\alpha)) = a^2 + ab + b^2\frac{|d|+1}{4} \) is clearly minimized among integral generators when \( a = 0 \) and \( b = 1 \). In the second case, \( N((\alpha)) = a^2 + b^2\left(\frac{|d|+1}{4} - \frac{|a|}{b}\right) > 1 + \left(\frac{|d|+1}{4} - 1\right) = \frac{|d|+1}{4} \). \( \square \)

2.3 Some Height Results

The results of this section are quite general in nature. Theorem 2.3.1 shows that in any number field, when one seeks an element of minimal height, it is sufficient to consider elements of a certain form. In general, an algebraic number may be written as a ratio of an algebraic integer and a rational integer. But it turns out that one can put a strong restriction on the rational integers that appears in the denominators of such numbers when one is interested in generators of minimal height. Theorems 2.3.3 and 2.3.4 each provide insights into some of the unexpected ways that two generators of the same field can share a common height.

**Theorem 2.3.1.** Let \( \alpha \in \overline{\mathbb{Q}} \) and let \( K = \mathbb{Q}(\alpha) \). Suppose that \( \alpha = \frac{a}{b} \beta \), where \( a \) and \( b \) are relatively prime integers, \( a, b > 0 \), and \( \beta \in \mathcal{O}_K \) is not divisible by any rational
integers not equal to ±1. If \( b = cd \), where \( d = (N((\beta)), b) \), i.e. \( d \mid N((\beta)) \) but \( de \nmid N((\beta)) \) for any positive divisor \( e \neq 1 \) of \( c \), then \( H(\alpha) \geq H\left(\frac{\beta}{d}\right)\).

**Proof.** If \( f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \) denotes the minimal polynomial of \( \beta \) with coefficients in \( \mathbb{Z} \), then, up to factoring out a constant, the minimal polynomial of \( \alpha \) is \( G(x) = c^n d^n x^n + c^{n-1} d^{n-1} a a_{n-1} x^{n-1} + c^{n-2} d^{n-2} a^2 a_{n-2} x^{n-2} + \ldots + a^n a_0 \); this follows from the fact that the degree of \( \beta \) over \( \mathbb{Q} \) is equal to the degree of \( \alpha \) over \( \mathbb{Q} \). The non-trivial common factor of all the coefficients of \( G \) divides \( d^n \) and is divisible by \( d \), by the choice of \( a, b, c, \) and \( d \) (it divides \( a^n a_0 \) and \( c^n d^n \); \( (a, cd) = 1 \) and \( c, d \) are defined in a special way). This implies that the (primitive) minimal polynomial of \( \alpha \) is \( g(x) = c^n b_n x^n + c^{n-1} b_{n-1} x^{n-1} + \ldots + b_0 \). Hence, since \( H(\alpha) = M(g) \), where \( M(h) \) denotes the Mahler measure of the polynomial \( h \),

\[
\frac{H(\alpha)}{H\left(\frac{\beta}{d}\right)} = \frac{c^n b_n \prod_{v \in M_{\infty}} \max(1, |\alpha|_v)^{n_v}}{b_n \prod_{v \in M_{\infty}} \max\left(1, |\frac{\beta}{d}|_v\right)^{n_v}},
\]

where \( n_v \) denotes the local degree of \( v \) over the infinite prime of \( \mathbb{Q} \). Note that \( b_n \) is exactly the leading coefficient of the (primitive) minimal polynomial of \( \frac{\beta}{d} \) because the greatest common factor of the coefficients of \( d^n x^n + d^{n-1} a_{n-1} x^{n-1} + d^{n-2} a_{n-2} x^{n-2} + \ldots + a_0 \) divides the greatest common factor of the coefficients of \( G(x) \), which is divisible by \( d \) and no additional factors of \( c \) as mentioned above.

Recall that, for any number field, the number of real embeddings plus two times the number of complex-conjugate pairs of embeddings is equal to the degree of the
field over the rationals. Therefore,

\[
\frac{H(\alpha)}{H(\frac{\beta}{\delta})} = \prod_{v \in M_\infty} \left( c \max \left( 1, \left| \frac{a\beta}{cd_v} \right| \right) \right)^{n_v} \frac{\max \left( 1, \left| \frac{\beta}{d_v} \right| \right)^{n_v}}{\max \left( 1, \left| \frac{\beta}{d_v} \right| \right)^{n_v}} \\
\geq \prod_{v \in M_\infty} \left( 1, c \left| \frac{a\beta}{cd_v} \right| \right)^{n_v} \frac{\max \left( 1, \left| \frac{\beta}{d_v} \right| \right)^{n_v}}{\max \left( 1, \left| \frac{\beta}{d_v} \right| \right)^{n_v}} \\
= \prod_{v \in M_\infty} \left( 1, a \left| \frac{\beta}{d_v} \right| \right)^{n_v} \frac{\max \left( 1, \left| \frac{\beta}{d_v} \right| \right)^{n_v}}{\max \left( 1, \left| \frac{\beta}{d_v} \right| \right)^{n_v}} \\
\geq 1.
\]

\[\square\]

**Corollary 2.3.2.** When looking for a generator of a number field \( K \) which has minimal height, it is enough to consider elements of the form \( \frac{\beta}{\delta} \), where \( \beta \in \mathcal{O}_K \) is not divisible by any rational integers not equal to \( \pm 1 \) and \( b \) is a positive rational integer dividing \( N((\beta)) \).

It is not necessarily true that an element of minimal height must have \( a = 1 \). It is also not necessarily true that an element of minimal height must have \( b \) dividing \( N((\beta)) \)

**Example 3.** \( \frac{2\sqrt{-22}}{11}, \frac{\sqrt{-22}}{4} \), and \( \frac{\sqrt{-22}}{11} \) have minimal height among generators of \( \mathbb{Q}((\sqrt{-22})) \) over \( \mathbb{Q} \) (see Example 5 below).

**Theorem 2.3.3.** Let \( \gamma \) be an algebraic number and suppose that \( \beta \) is an algebraic integer such that \( \mathbb{Q}(\gamma) = \mathbb{Q}(\frac{\gamma}{\beta}) \); denote this common field by \( K \). Let \( (\gamma) = \frac{I}{J_\gamma} \) where
$I_\gamma$ and $J_\gamma$ are relatively prime integral ideals of $K$. If $|\gamma|_v \geq 1$ and $|\gamma|_v \geq |\beta|_v$ for all infinite places $v$ of $K$ and $I_\gamma + (\beta) = (1)$, then $H(\gamma) = H\left(\frac{\gamma}{\beta}\right)$. In particular, if $\beta = n \in \mathbb{N}$ is such that $|\frac{\gamma}{n}|_v \geq 1$ for all infinite places $v$ of $K$ and $n$ is relatively prime to $N(I_\gamma)$, then $H(\gamma) = H\left(\frac{\gamma}{n}\right)$.

Proof.

\[
H\left(\frac{\gamma}{\beta}\right) = \prod_{v \in M_K} \max\left(1, \frac{|\gamma|_v}{|\beta|_v}\right)^{n_v}
= \prod_{v \in M^0_K} \max\left(1, \frac{|\gamma|_v}{|\beta|_v}\right)^{n_v} \prod_{v \in M^K_{\infty}} \frac{|\gamma|_v^{n_v}}{|\beta|_v^{n_v}}
= \prod_{v \in M^0_K} \frac{1}{|\beta|_v^{n_v}} \prod_{v \in M^0_K} \max(1, |\gamma|_v)^{n_v} \prod_{v \in M^K_{\infty}} \frac{1}{|\beta|_v^{n_v}} \prod_{v \in M^K_{\infty}} |\gamma|_v^{n_v}
= \prod_{v \in M_K} \frac{1}{|\beta|_v^{n_v}} \prod_{v \in M^0_K} \max(1, |\gamma|_v)^{n_v} \prod_{v \in M^K_{\infty}} \max(1, |\gamma|_v)^{n_v}
= H(\gamma),
\]

where the sixth equality follows from the product formula and the fourth equality follows from the assumptions that $I_\gamma$ and $(\beta)$ are relatively prime, $|\gamma|_v \geq 1$ for all infinite places, and $\beta$ is an algebraic integer.

There is a similar (but easier) result to this one, in that it will also sometimes exhibit the existence of seemingly unrelated elements that have the same height, but its hypotheses are opposite in nature. It explains the result mentioned at the end of Example 2 above.
Theorem 2.3.4. Let \( \gamma \) be an algebraic number and suppose that \( \beta \) and \( \delta \) are algebraic integers such that \( \mathbb{Q}(\frac{\delta}{\beta \gamma}) = \mathbb{Q}(\frac{\delta}{\gamma}) \); denote this common field by \( K \). Let \( (\gamma) = \frac{1}{\gamma} \).

Suppose that \( \beta \) is relatively prime to both \( I_\gamma \) and \( J_\gamma \) and suppose that \( |\gamma|_v \geq 1 \) for every infinite place \( v \). Moreover, suppose that \( \left| \frac{\delta}{\beta} \right|_v \leq 1 \) for all infinite places \( v \) of \( K \).

If \( \frac{\delta}{\gamma} \in \mathcal{O}_K \), then \( H\left( \frac{\delta}{\beta} \right) = H\left( \frac{\delta}{\beta \gamma} \right) \). In particular, if \( \beta = m \) and \( \gamma = n \) are relatively prime rational integers with \( \left| \frac{\delta}{m} \right|_v \leq 1 \) for all infinite places of \( K \) and \( \frac{\delta}{n} \in \mathcal{O}_K \), then \( H\left( \frac{\delta}{m} \right) = H\left( \frac{\delta}{mn} \right) \).

Proof. For any infinite place \( v \), \( \left| \frac{\delta}{\beta \gamma} \right|_v = \left| \frac{\delta}{\beta} \right|_v \left| \frac{1}{\gamma} \right|_v \leq 1 \). For any finite place \( v \) of \( K \) dividing \( \beta \), \( \left| \frac{\delta}{\beta \gamma} \right|_v = \left| \frac{\delta}{\beta} \right|_v \left| \frac{1}{\gamma} \right|_v = \left| \frac{\delta}{\gamma} \right|_v \), because \( \beta \) is relatively prime to both \( I_\gamma \) and \( J_\gamma \). Also, for any finite place \( v \) dividing \( \frac{\delta}{\gamma} \) that does not divide \( \beta \), \( \left| \frac{\delta}{\beta} \right|_v = \left| \frac{1}{\gamma} \right|_v \left| \frac{\delta}{\gamma} \right|_v = \left| \frac{\delta}{\gamma} \right|_v < 1 \) since \( \frac{\delta}{\gamma} \in \mathcal{O}_K \). Hence,

\[
H\left( \frac{\delta}{\beta} \right) = \prod_{v \in M_K} \max\left( 1, \left| \frac{\delta}{\beta \gamma} \right|_v \right)^{n_v} \\
= \prod_{v \in M_K^0} \max\left( 1, \left| \frac{\delta}{\beta \gamma} \right|_v \right)^{n_v} \\
= \prod_{v|\beta} \max\left( 1, \left| \frac{\delta}{\beta \gamma} \right|_v \right)^{n_v} \prod_{v|\gamma, v|\beta} \max\left( 1, \left| \frac{\delta}{\beta \gamma} \right|_v \right)^{n_v} \prod_{v|\gamma, v|\beta} \max\left( 1, \left| \frac{\delta}{\beta \gamma} \right|_v \right)^{n_v} \\
= \prod_{v|\beta} \max\left( 1, \left| \frac{\delta}{\beta} \right|_v \right)^{n_v} \prod_{v|\gamma, v|\beta} \left( 1 \prod_{v|\gamma, v|\beta} 1 \right) \\
= \prod_{v \in M_K^0} \max\left( 1, \left| \frac{\delta}{\beta} \right|_v \right)^{n_v} \left( \text{recall, } \delta \in \mathcal{O}_K \right) \\
= \prod_{v \in M_K} \max\left( 1, \left| \frac{\delta}{\beta} \right|_v \right)^{n_v} \\
= H\left( \frac{\delta}{\beta} \right).
\]
2.4 On a Result of Ruppert Concerning Polynomials of Smallest Polynomial-Height Whose Roots Generate Imaginary Quadratic Extensions of $\mathbb{Q}$.

Recall Theorem 1.3.6. Throughout this section, $d < 0$.

**Theorem 2.4.1.** Let $D$ denote the discriminant of $\mathbb{Q}(\sqrt{D})$ (so $D = 4d$ if $d \not\equiv 1 \pmod{4}$, and $D = d$ if $d \equiv 1 \pmod{4}$). Let $\hat{H}_{\text{min}}(D)$ denote the minimal polynomial-height of a generator for the imaginary quadratic extension of $\mathbb{Q}$ with discriminant $D$.

$$\lim_{D \to -\infty} \frac{\hat{H}_{\text{min}}(D)}{\frac{1}{2}\sqrt{|D|}} = 1.$$  

This theorem allows for an explicit description of an irreducible quadratic polynomial with a sufficiently large squarefree part of its discriminant having minimal polynomial-height. It implies that there is a natural number $N_0$ such that

$$\frac{\hat{H}_{\text{min}}(D)}{\frac{1}{2}\sqrt{|D|}} < 2$$

if $|d| > N_0$. The constant $N_0$ is ineffective. The wording of the statements here is the same as that used in Theorems 2.5.2 and 2.5.4 in order to provide a proof of Corollary 2.5.6 in the next section.

**Theorem 2.4.2.** Let $\hat{H}(f)$ denote the polynomial-height of the polynomial $f$. The following statements hold for $|d| > N_0$. 

48
(1) Let \( d \not\equiv 1 \pmod{4} \) be a negative, squarefree integer. There exists a triple of integers \((x, y, z)\) satisfying the Conditions

\[ z^2 = xy + d, \quad x > \sqrt{|d|}, \quad x \geq y \geq 0, \quad \text{and} \quad 0 \leq z \leq \frac{x}{2}. \]  

(2.1)

For any triple \((x, y, z)\) satisfying Conditions 2.1, the polynomial \( f(w) = xw^2 - 2zw + y \) is primitive and irreducible and \( \widehat{H}(f) = x \). If \((x, y, z)\) is a triple satisfying Conditions 2.1 with \( x \) as small as possible, then \( f(w) \) has minimal polynomial-height among all polynomials whose discriminant has squarefree part equal to \( d \). As a consequence, \( x < 2\sqrt{|d|} \).

(2) Let \( d \equiv 1 \pmod{4} \) be a negative, squarefree integer. There exists a triple of integers \((x, y, z)\) satisfying the Conditions

\[ z^2 = xy + d, \quad x > \sqrt{|d|}, \quad x \text{ and } y \text{ even, } z \text{ odd, } x \geq y \geq 0, \quad \text{and} \quad 0 \leq z \leq \frac{x}{2}. \]  

(2.2)

For any triple \((x, y, z)\) satisfying Conditions 2.2, the polynomial \( F(w) = \frac{z}{2}w^2 - zw + \frac{y}{2} \) is primitive and irreducible and \( \widehat{H}(F) = \frac{z}{2} \). If \((x, y, z)\) is a triple satisfying Conditions 2.2 with \( x \) as small as possible, then \( F(w) \) has minimal polynomial-height among all polynomials whose discriminant has squarefree part equal to \( d \). As a consequence, \( x < \sqrt{|d|} \).

Proof. For part (1), the quadratic formula gives the solutions to \( f(w) = 0 \) as \( w = \frac{2z \pm \sqrt{4z^2 - 4xy}}{2x} \). Canceling the common factor of 2 gives \( w = \frac{z \pm \sqrt{z^2 - xy}}{x} \). Since \( z^2 - xy = d \) is squarefree, there are no other common factors. This shows that the polynomial is irreducible. If it is not primitive, then either 2 divides each of \( x \) and \( y \) or there is a prime \( p \) dividing \( z \) that also divides \( x \) and \( y \). If 2 divides each of \( x \) and \( y \), then...
reducing $z^2 - xy = d$ modulo 4 gives $z^2 \equiv d \pmod{4}$; this is impossible since $d$ is congruent to either 2 or 3 modulo 4 so it is not a square modulo 4. If there is a prime $p$ dividing $z$ that also divides $x$ and $y$, then $p^2$ divides $z^2 - xy = d$; this is impossible since $d$ is squarefree. Therefore, $f$ is primitive, irreducible, and, since $x \geq y$ and $x \geq 2z$, $f$ has polynomial-height $x$.

Suppose that $g(w) = aw^2 - 2bw + c$ is primitive and irreducible, the squarefree part of its discriminant is $d$, and $g(w)$ has minimal polynomial-height among all such polynomials. (The coefficient of $w$, say $B$, must be even for any such polynomial. This is because $B^2 - 4AC = dE^2$ for some integers $A, C, E$. Reducing this equation modulo 4 shows that $B$ cannot be odd since $d \not\equiv 1 \pmod{4}$.) The discriminant is negative, i.e. $b^2 - ac < 0$, so $|b| < \max\{|a|, |c|\}$ and $a$ and $c$ have the same sign.

Since switching $a$ and $c$ or changing $b$ or $-b$ does not change the discriminant or the polynomial-height of the polynomial, one may assume that $b \geq 0$ and $a \geq c > 0$.

There is some natural number $m$ such that $b^2 - ac = dm^2$, i.e. $ac - b^2 = |d|m^2$. The polynomial-height of $g(w)$ is either $a$ or $2b$. Since $a^2 \geq ac \geq ac - b^2 = |d|m^2$, $a \geq m\sqrt{|d|}$. Hence, $\hat{H}(g) \geq m\sqrt{|d|}$. For $|d| > N_0$, $\hat{H}(g) < 2\sqrt{|d|}$; so, for these values of $d$, $m$ must be 1. Therefore, for $|d| > N_0$, one may assume that the coefficients $a, b, c$ of a polynomial $g(w) = aw^2 - 2bw + c$ with minimal polynomial-height among primitive irreducible polynomials whose discriminant has squarefree part $d$ satisfy $a > b \geq 0, a \geq c > 0$, and $b^2 - ac = d$.

In this case, it will turn out that $a \geq 2b$ so that $g(w)$ has polynomial-height $a$. Suppose on the contrary that $a < 2b$, so that $g(w)$ has polynomial-height $2b$. Consider the polynomial $g(1 - w)$, which is also primitive, irreducible, and has discriminant
d. Note that \( g(1 - w) = aw^2 - 2(a - b)w + a + c - 2b \). Since \( g(1 - w) \) has negative discriminant and \( a > 0 \), \( g(1) = a + c - 2b \) is positive. In addition, since \( a < 2b \) by assumption, \( a + c - 2b < c \). But, \( c \leq a \) and \( 0 < a - b \leq a \) so that \( g(1 - w) \) has polynomial-height \( a \). Hence, \( g(1 - w) \) is a polynomial with smaller polynomial-height than \( g(w) \). This contradicts the choice of \( g(w) \).

Therefore, the coefficients of \( g(w) \) satisfy \( b^2 = ac + d, a \geq c \geq 0 \), and \( 0 \leq b \leq \frac{a}{2} \). Moreover, \( a > \sqrt{|d|} \) (lest \( b^2 = d + ac \) be negative) and, since \( \hat{H}(g) = a \) and \( \hat{H}(g) < 2\sqrt{|d|}, a < 2\sqrt{|d|} \). Hence, the triple \((a, b, c)\) will satisfy Conditions 2.1 and any triple \((x, y, z)\) satisfying Conditions 2.1 with minimal \( x \) will give rise to a polynomial \( f(w) = xw^2 - 2zw + y \) with minimal polynomial-height \( \hat{H}(f) = x < 2\sqrt{|d|} \) among primitive irreducible polynomials whose discriminant has squarefree part \( d \). This completes the proof of (1).

For part (2), the quadratic formula gives the solutions to \( F(w) = 0 \) as

\[
w = \frac{z \pm \sqrt{z^2 - 4zw}}{2z} = \frac{z^2 \pm \sqrt{z^2 - xy}}{x}.
\]

Since \( z^2 - xy = d \) is squarefree, the polynomial is irreducible. If it is not primitive, then there is a prime \( p \) dividing \( z \) that also divides \( \frac{a}{2} \) and \( \frac{c}{2} \). In this case, \( p^2 \) divides \( z^2 - xy = d \); this is impossible since \( d \) is squarefree. Therefore, \( F \) is primitive, irreducible, and, since \( x \geq y \) and \( \frac{a}{2} \geq z \), \( F \) has polynomial-height \( \frac{a}{2} \).

Suppose that \( G(w) = a'w^2 - b'w + c' \) is primitive and irreducible, the squarefree part of its discriminant is \( d \), and \( G(w) \) has minimal polynomial-height among all such polynomials. The discriminant is negative, i.e. \( b'^2 - 4a'c' < 0 \), so \( |b'| \leq \max\{2|a'|, 2|c'|\} \) and \( a' \) and \( c' \) have the same sign. Since switching \( a' \) and \( c' \) or changing \( b' \) to \(-b'\) does
not change the discriminant or the polynomial-height of the polynomial, one may assume that \( b' \geq 0 \) and \( a' \geq c' > 0 \). There is some natural number \( m \) such that
\[
b^2 - 4a'c' = dm^2 ,
\]
i.e. such that \( 4a'c' - b^2 = |d|m^2 \). The polynomial-height of \( G(w) \) is either \( a' \) or \( b' \). Since \( 4a'^2 \geq 4a'c' \geq 4a'c' - b^2 = |d|m^2, 2a' \geq m\sqrt{|d|} \). Hence, \( \hat{H}(G) \geq m\frac{\sqrt{d}}{2} \). For \( |d| > N_0 \), \( \hat{H}(G) < \sqrt{|d|} \); so, for these values of \( d, m \) must be 1.

Therefore, for \( |d| > N_0 \), one may assume that the coefficients \( a', b', c' \) of a polynomial \( G(w) = a'w^2 - b'w + c' \) with minimal polynomial height among primitive irreducible polynomials whose discriminant has squarefree part \( d \) satisfy \( 2a' \geq b' \geq 0, a' \geq c' > 0 \), and \( b^2 - 4a'c' = d \) with \( \max\{a', b'\} \) minimal.

In this case, it will turn out that \( a' \geq b' \) so that \( G(w) \) has polynomial-height \( a \). Suppose on the contrary that \( b' > a' (> 0) \), so that \( G(w) \) has polynomial-height \( b' \). Consider the polynomial \( G(1 - w) \), which is also primitive, irreducible, and has discriminant \( d \). Note that \( G(1 - w) = a'w^2 - (2a' - b')w + c' - b' + a' \). Since \( G(1 - w) \) has negative discriminant and \( a' > 0, G(1) = a' + c' - b' \) is positive. In addition, since \( a' < b' \) by assumption, \( a' + c' - b' < c' \). But, \( c' \leq a' \) and \( 0 < b' \leq a' + c' - b' \) so that \( G(1 - w) \) has polynomial-height \( a' \). Hence, \( G(1 - w) \) is a polynomial with smaller polynomial-height than \( G(w) \). This contradicts the choice of \( G(w) \).

Therefore, the coefficients of \( G(w) \) satisfy \( b^2 - 2a'2c' = d, 2a' \geq 2c' > 0, \) and \( 0 \leq b' \leq \frac{2a'}{2} \). Moreover, \( 2a' > \sqrt{|d|} \) (lest \( b'^2 = d + 2a'2c' \) be negative) and, since \( \hat{H}(G) = a' \) and \( \hat{H}(G) < \sqrt{|d|} \), \( a' < \sqrt{|d|} \). Hence, the triple \((2a', b', 2c')\) will satisfy Conditions 2.2 and any triple \((x, y, z)\) satisfying Conditions 2.2 with \( x \) minimal will give rise to a polynomial \( F(w) = \frac{x}{2} - zw + \frac{y}{2} \) with minimal polynomial-height \( \hat{H}(F) = \frac{x}{2} < \sqrt{|d|} \)
among primitive irreducible polynomials whose discriminant has squarefree part \( d \). This completes the proof of (2).

\[
\square
\]

2.5 Generators of Smallest Height in Imaginary Quadratic Extensions of \( \mathbb{Q} \).

The integers in an imaginary quadratic extension have minimal height on the order of \(|d|\). This is clearly much larger than the real quadratic case, when the minimal height among integers is on the order of \( \sqrt{d} \). It turns out that by considering general field elements, the minimal height of a generator of an imaginary quadratic extension is on the order of \( \sqrt{|d|} \). To show this, the following lemma will be necessary and is perhaps of independent interest although it follows directly from an effective version of the Chebotarev Density Theorem.

**Lemma 2.5.1.** Let \( d \) be a non-zero, squarefree integer and assume the Generalized Riemann Hypothesis.

1. If \( d \not\equiv 1 \pmod{4} \) and \(|d| > 902,354,958,197\), then there is a prime number \( p \in (\sqrt{|d|}, 2\sqrt{|d|}) \) that splits completely in \( \mathbb{Q}(\sqrt[d]{d}) \). If \( d \not\equiv 1 \pmod{4} \) and \(|d| > 902,365,105,040\), then there is a prime number \( p \in (\sqrt{|d|}, 2\lfloor\sqrt{|d|}\rfloor - 2) \) that splits completely in \( \mathbb{Q}(\sqrt[d]{d}) \).

2. If \( d \equiv 1 \pmod{4} \) and \(|d| > 3,609,419,832,785\), then there is a prime number \( p \in \left(\frac{\sqrt{|d|}}{2}, \sqrt{|d|}\right) \) that splits completely in \( \mathbb{Q}(\sqrt[d]{d}) \). If \( d \equiv 1 \pmod{4} \) and
$|d| > 3, 609, 445, 221, 315$, then there is a prime number $p \in \left( \frac{\sqrt{|d|}}{2}, \frac{\sqrt{|d|} + \sqrt{|d|}}{2} - 3 \right)$ that splits completely in $\mathbb{Q}(\sqrt{d})$.

**Proof.** Here is a proof for the first sentence of part (1). The other cases are all very similar.

Let $\pi_{sp}(x)$ denote the number of prime integers $p$ that are less than or equal to the positive real number $x$ which split completely in $\mathbb{Q}(\sqrt{d})$. According to Oesterlé [Oe], for any $x \geq 2$,

$$\left| \pi_{sp}(x) - \frac{1}{2} \int_{2}^{x} \frac{dt}{\log t} \right| \leq \frac{1}{2} \sqrt{x} \left( \left( \frac{1}{\pi} + \frac{5.3}{\log x} \right) \log(D) + 2 \left( \frac{\log x}{2\pi} + 2 \right) \right),$$

where $D$ is the absolute value of the discriminant of $\mathbb{Q}(\sqrt{d})$. Note that $d \not\equiv 1 \pmod{4}$ implies that $D = 4|d|$. Hence,

$$-\frac{1}{2} \sqrt{2|d|} \left( \left( \frac{1}{\pi} + \frac{5.3}{\log(2\sqrt{|d|})} \right) \log(4|d|) + 2 \left( \frac{\log(2\sqrt{|d|})}{2\pi} + 2 \right) \right) \leq \pi_{sp}(2\sqrt{|d|}) - \frac{1}{2} \int_{2}^{2\sqrt{|d|}} \frac{dt}{\log t}$$

and

$$-\frac{1}{2} \sqrt{|d|} \left( \left( \frac{1}{\pi} + \frac{5.3}{\log(\sqrt{|d|})} \right) \log(4|d|) + 2 \left( \frac{\log(\sqrt{|d|})}{2\pi} + 2 \right) \right) \leq \frac{1}{2} \int_{2}^{\sqrt{|d|}} \frac{dt}{\log t} - \pi_{sp}(\sqrt{|d|}).$$

Adding these inequalities and isolating the term $\pi_{sp}(2\sqrt{|d|}) - \pi_{sp}(\sqrt{|d|})$ shows that

$$\pi_{sp}(2\sqrt{|d|}) - \pi_{sp}(\sqrt{|d|}) \geq \frac{1}{2} \int_{2}^{\sqrt{|d|}} \frac{dt}{\log t} - \frac{1}{2} \sqrt{2\sqrt{|d|}} \left( \left( \frac{1}{\pi} + \frac{5.3}{\log(2\sqrt{|d|})} \right) \log(4|d|) + 2 \left( \frac{\log(2\sqrt{|d|})}{2\pi} + 2 \right) \right).$$

54
\[ \frac{1}{2} \sqrt{|d|} \left( \left( \frac{1}{\pi} + \frac{5.3}{\log(\sqrt{|d|})} \right) \log(4|d|) + 2 \left( \frac{\log(\sqrt{|d|})}{2\pi} + 2 \right) \right). \]

The right-hand side of this inequality goes to infinity as \(|d|\) goes to infinity (for example, because \(\log t < t^{1/2}\) for large \(t\)) and is eventually increasing (for example, once \(|d| > 7 \cdot 10^{10}\)). For \(|d| = 902354958198\), the right-hand side is larger than \(4.45288 \cdot 10^{-9}\). Since this is positive, the function \(\pi_{sp}(2\sqrt{|d|}) - \pi_{sp}(\sqrt{|d|})\) evaluated at \(|d| = 902354958198\) is an integer larger than zero, i.e., it is at least equal to 1. \(\square\)

For the sake of clarity (and brevity) in what follows, here is a definition.

**Definition.** If \(d \not\equiv 1 \pmod{4}\) is a squarefree integer, then an element \(\frac{a+b\sqrt{d}}{e}\) is called **height-reduced** if \(a \geq 0\) is an integer, \(b\) and \(e\) are positive integers, \(a\) and \(b\) are relatively prime, and \(e | N((a+b\sqrt{d}))\). If \(d \equiv 1 \pmod{4}\) is a squarefree integer, then an element \(\frac{a+b\sqrt{d}}{e}\) is called **height-reduced** if \(a, b, e\) are integers with \(e > 0\), \(a\) and \(b\) are relatively prime, \(e | N\left(\left(a+b\frac{\sqrt{d}}{2}\right)\right)\), and either \(a \geq 0, b \geq 1\) or \(a < 0, b \geq 1\) with \(|a| < \frac{|b|}{2}\).

Corollary 2.3.2 and Lemma 2.1.8 show that every element in \(\mathbb{Q}(\sqrt{d})\) has height at least as large as some height-reduced element in that field.

**Theorem 2.5.2.** Let \(d \not\equiv 1 \pmod{4}\) be a negative, squarefree integer. Let \(c\) denote the smallest height among all generators of \(\mathbb{Q}(\sqrt{d})\) over \(\mathbb{Q}\). Let \(\alpha = \frac{a+b\sqrt{d}}{e}\) range over height-reduced elements of \(\mathbb{Q}(\sqrt{d})\).

1. The height of any element \(\frac{A+B\sqrt{d}}{E}\) is a natural number. In particular, \(c\) is a natural number.

2. \(\alpha\) has height less than \(2\sqrt{|d|}\) only if \(b = 1\).
(3) If $|d| > N_0$, then $c < 2\sqrt{|d|}$. More generally, for any $\gamma \in \left[\frac{5}{2\sqrt{3}}, 2\right]$, if $|d|$ is large enough, then $c < \gamma \sqrt{|d|}$. Assuming the Generalized Riemann Hypothesis, if $|d| > 177$, then $c < 2\sqrt{|d|}$.

(4) Suppose that $\alpha$ lies in the set of generators with height $c$. It is possible to choose $\alpha$ with $e = c$. If $|d| > N_0$, then it is possible to choose $\alpha$ with $e = c$ and $b = 1$; assuming the Generalized Riemann Hypothesis, this is always possible.

(5) Let $n$ be the smallest integer larger than $\sqrt{|d|}$ such that $d$ is a square modulo $n$.
   If $n \geq \frac{2}{\sqrt{3}} \sqrt{|d|}$, then $c \leq n$. If $n < \frac{2}{\sqrt{3}} \sqrt{|d|}$, then $c \leq \frac{5n}{4} < \frac{5}{2\sqrt{3}} \sqrt{|d|}$.

(6) Let $(x, y, z)$ be a solution to the equation $z^2 = xy + d$ subject to the conditions that $x > \sqrt{|d|} > 0$, $\frac{x}{2} \geq z \geq 0$, with $x$ minimal among all solutions satisfying $x \geq \sqrt{z^2 - d}$ (equivalently, $x \geq y$). Assuming the Generalized Riemann Hypothesis, and in any case if $|d| > N_0$, $x = c$, and the element $\frac{z + \sqrt{d}}{x}$ has height $c$.

Proof. Here is a proof of (1) for general field elements. Another proof, specific to height-reduced elements is given below. For $\frac{A + B\sqrt{d}}{E} \in \mathbb{Q}(\sqrt{d})$, if $B = 0$, then the element lies in $\mathbb{Q}$ and hence has natural number height. Suppose now that $B \neq 0$
and let its primitive minimal polynomial be given by \( a_2x^2 + a_1x + a_0 \).

\[
H \left( \frac{A + B\sqrt{d}}{E} \right) = a_2 \max \left( 1, \left| \frac{A + B\sqrt{d}}{E} \right| \right) \max \left( 1, \left| \frac{A - B\sqrt{d}}{E} \right| \right)
\]

\[
= a_2 \max \left( 1, \left| \frac{A + B\sqrt{d}}{E} \right| \right)^2
\]

\[
= a_2 \max \left( 1, N \left( \left( \frac{A + B\sqrt{d}}{E} \right) \right) \right)
\]

\[
= a_2 \max \left( 1, \frac{|a_0|}{|a_2|} \right)
\]

\[
= \max(|a_2|, |a_0|) \in \mathbb{N}.
\]

Now consider the case when the element is height-reduced. First, note that \( e \) is the smallest natural number such that \( e\alpha \in \mathcal{O}_K \), where \( K = \mathbb{Q}(\sqrt{d}) \). If \( x^2 + a_1x + a_0 \) is the minimal polynomial of \( a + b\sqrt{d} \) (so that \( a_1 = -2b \) and \( a_0 = a^2 - db^2 \)), then \((e\alpha)^2 + a_1(e\alpha) + a_0 = 0\). Since \( e \mid a_0 \) by assumption, the polynomial \( ex^2 + a_1x + \frac{a_0}{e} \) lies in \( \mathbb{Z}[x] \) and has \( \alpha \) as a root. Hence, \( ex^2 + a_1x + \frac{a_0}{e} \) is an integral multiple of the primitive minimal polynomial of \( \alpha \). If \( g \) is the leading coefficient of the primitive minimal polynomial of \( \alpha \) (so that \( g \mid e \)), then \( g\alpha \) is integral so that \( e \leq g \) by the first sentence of this paragraph. Hence, the primitive minimal polynomial of \( \alpha \) is in fact \( ex^2 + a_1x + \frac{a_0}{e} \) and has leading coefficient \( e \).

If \( e \geq \sqrt{N((a + b\sqrt{d}))} = |a + b\sqrt{d}| = |a - b\sqrt{d}| \geq |b\sqrt{|d|}| \), then, by the formula for height in terms of Mahler measure (Theorem 1.1.6),

\[
H(\alpha) = e \max \left( 1, \left| \frac{a + b\sqrt{d}}{e} \right| \right) \cdot \max \left( 1, \left| \frac{a - b\sqrt{d}}{e} \right| \right) = e.
\]

If \( e < \sqrt{N((a + b\sqrt{d}))} \), then \( H(\alpha) = \frac{N((a + b\sqrt{d}))}{e} > \sqrt{N((a + b\sqrt{d}))} \geq |b\sqrt{|d|}| \). Hence, the height of every height-reduced element of \( \mathbb{Q}(\sqrt{d}) \) is an integer at least as
large as $[b\sqrt{|d|}]$. Therefore, $H(\alpha) < 2\sqrt{|d|}$ only if $b = 1$, which proves (2). Since a generator of minimal height may be taken to be height-reduced, this proves the second part of (1). Moreover, if $\alpha = \frac{a + bv\sqrt{d}}{e}$ is height-reduced and has height $c$, then $c$ equals either $e$ or $\frac{N((a + bv\sqrt{d}))}{e}$. Now, the Galois conjugate of $\frac{1}{\alpha}$ is also height-reduced with height $c$ and replacing $\alpha$ by the Galois conjugate of $\frac{1}{\alpha}$ replaces $e$ by $\frac{N((a + bv\sqrt{d}))}{e}$; hence, there is a height-reduced generator $\alpha$ such that $H(\alpha) = c$ and $c = e$. This proves the first claim in (4).

Next, suppose that there is an integer $r \in \left(\sqrt{|d|}, 2\sqrt{|d|}\right)$ such that $d$ is a square modulo $r$. This implies that there is an integer $k \in \{0, 1, \ldots, \lfloor r/2 \rfloor\}$ and a natural number $m$ such that $k^2 - d = rm$.

$$|k + \sqrt{d}| = \sqrt{k^2 - d} \leq \sqrt{\left(\frac{r}{2}\right)^2 - d} = \sqrt{\frac{r^2 + 4|d|}{4}}.$$  

Suppose first that $r \in \left(2\sqrt{\frac{2}{3}}\sqrt{|d|}, 2\sqrt{|d|}\right)$. In this case, $|d| < \frac{3}{4}r^2$ so that

$$|k + \sqrt{d}| < \sqrt{\frac{r^2 + 4\frac{3}{4}r^2}{4}} = r.$$  

Hence, the element $\frac{k + \sqrt{d}}{r}$ has height equal to $r$ which is less than $2\sqrt{|d|}$. This implies that, when such an integer $r$ exists, the minimal height of a generator is less than $2\sqrt{|d|}$. In this case, when looking for height-reduced elements $\alpha$ with minimal height and $e = c$, it suffices to further assume that $b = 1$. Now suppose that $r \in \left(\sqrt{|d|}, \frac{2}{\sqrt{3}}\sqrt{|d|}\right)$. If it happens to be the case that $|k + \sqrt{d}| \leq r$, then, as
above, the element $\frac{k + \sqrt|d|}{r}$ has height equal to $r$ which is less than $2\sqrt{|d|}$. If, instead, $|k + \sqrt|d|| > r$, then $m = \frac{k^2 - d}{r} = \frac{k^2 - d}{|k + \sqrt|d||} = |k - \sqrt|d|| = |k + \sqrt|d||$ so that $\frac{k + \sqrt|d|}{r}$ has height $m$ and $m \leq \frac{5r}{4} < \frac{5}{2\sqrt{3}}\sqrt{|d|} < 2\sqrt{|d|}$ because dividing the equation $k^2 + |d| = rm$ through by $r^2$ and using the constraints on $k$ and $r$ shows that

$$\frac{m}{r} = \left(\frac{k}{r}\right)^2 + \frac{|d|}{r^2} \leq \frac{1}{4} + 1 = \frac{5}{4}.$$  

Hence, in this case as well, when looking for height-reduced elements $\alpha$ with minimal height and $e = c$, it suffices to further assume that $b = 1$.

Theorem 2.4.2 shows that, for all $|d| > N_0$, there is an element $r \in (\sqrt{|d|}, 2\sqrt{|d|})$ such that $d$ is a square modulo $r$. (Consider the polynomial $f(w)$ in the statement of Theorem 2.4.2. The height of either of its roots is:

$$x \max\left(1, \frac{|z + \sqrt|d||}{x}\right) \max\left(1, \frac{|z - \sqrt|d||}{x}\right) = x \max\left(1, \frac{\sqrt{z^2 - d}}{x}\right)^2$$

$$= x \max\left(1, \frac{\sqrt{x^2y}}{x}\right)^2$$

$$\leq x \max\left(1, \frac{\sqrt{x^2}}{x}\right)^2$$

$$= x,$$

and for large enough $|d|$, $x \leq 2\sqrt{|d|}$, as indicated in the proof; $x$ is always larger than $\sqrt{|d|}$, by assumption.) Assuming the Generalized Riemann Hypothesis, for $|d| \geq 902354958197$, Lemma 2.5.1 shows that there is actually a prime $p \in (\sqrt{|d|}, 2\sqrt{|d|})$ such that $d$ is a square modulo $p$. Direct computation ([OSC]) shows that the only values of $d$ that are negative, squarefree, not congruent to 1 modulo 4, and have absolute value less than 902354958197 such that there is no element with height less
than $2\sqrt{|d|}$ are $-22$, $-37$, $-58$ and $-177$. An element of minimal height in each of these cases is $\frac{-22}{11}$, $\frac{1+\sqrt{-37}}{19}$, $\frac{-58}{29}$, and $\frac{3+\sqrt{-177}}{31}$, respectively. Hence, for all $|d| > N_0$, or for all $|d|$ assuming the Generalized Riemann Hypothesis, it is possible to choose $\alpha$ with height $c$ such that $e = c$ and $b = 1$. This proves (3) and the rest of (4).

The results of (5) and (6) will now follow from the previous paragraph and Theorem 2.3.1. There is an element of smallest height of the form $\frac{a+\sqrt{d}}{c}$ where $c \mid N((a + \sqrt{d}))$ and $c \geq \sqrt{a^2 - d}$, for all $|d| > N_0$, or for all $|d|$ assuming the Generalized Riemann Hypothesis; when this holds, this implies that there is some integer $\ell$ such that $a^2 = c\ell + d$. Suppose that this condition holds. If $a \geq c$, then by subtracting the appropriate multiple of $c$ from both sides shows that there is an element of smallest height of the form $\frac{a+\sqrt{d}}{c}$ where $c \mid N((a + \sqrt{d}))$, $a < c$, and $c \geq \sqrt{a^2 - d}$ (use the division algorithm to write $a = cq + a'$ for some $0 \leq a' < c$). If $a > \frac{c}{2}$, then replacing $a$ by $c - a$ and changing $\ell$ to $\ell + c - 2a$ shows that there is an element of smallest height of the form $\frac{a+\sqrt{d}}{c}$ where $c \mid N((a + \sqrt{d}))$, $a \leq \lfloor \frac{c}{2} \rfloor$, and $c \geq \sqrt{a^2 - d}$. Now, in the equation $a^2 = c\ell + d$, if $\ell > c$, then $\ell > \sqrt{a^2 - d}$ so that $c\ell > (\sqrt{a^2 - d})^2 = a^2 - d$. Since this contradicts the definition of $\ell$, $\ell$ is at most $c$. Conversely, any solution of the equation $z^2 = xy + d$ with $x \geq y$ and $z \leq \lfloor \frac{c}{2} \rfloor$ gives an element $\frac{a+\sqrt{d}}{x} \in \mathbb{Q}(\sqrt{d})$ with height $x$. This completes the proof.

Note that, when searching for a generator of minimal height in the situation addressed in Theorem 2.5.2, part (6) gives a computational method for searching that is much faster than the brute force method implied by the relationship between the Weil

\[\text{\textsuperscript{†}}\text{It is interesting to note that } d \text{ is a square modulo } c.\]
height of an algebraic number and the polynomial-height of its minimal polynomial.
Initially, it is only known that $\sqrt{|d|} < c \leq |d|$. If the number $n$ in part (5) is not the smallest height, then depending on where $n$ lies in relation to $\frac{2}{\sqrt{3}} \sqrt{|d|}$, it is either an upper bound for the minimal height or it is a better lower bound for the minimal height and the number $m$ is an upper bound. Finding $m$ may not be efficient, but since, in this case, $\sqrt{|d|} < n < c \leq m \leq \frac{5n}{4}$, the number $\frac{5n}{4}$ provides an upper bound. A similar comment applies for the situation addressed in Theorem 2.5.4.

The theorem shows that the algebraic integers in the imaginary quadratic extensions under consideration are not good sources of minimal height elements. This is perhaps counterintuitive, based on experience with the rational numbers and on the fact that every algebraic number is a ratio of algebraic integers. Again, a similar comment applies for the situation addressed in Theorem 2.5.4.

**Corollary 2.5.3.** Let $d \not\equiv 1 \pmod{4}$ be a negative, squarefree integer. The minimal height value of a generator of $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$ is never attained by an algebraic integer for $|d|$ sufficiently large. Assuming the Generalized Riemann Hypothesis, the minimal height value of a generator of $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$ is attained by an algebraic integer if and only if $d = -1$ or $d = -2$.

**Proof.** $|d| \geq 2\sqrt{|d|}$ for $|d| \geq 4$. Hence, given the theorem and its proof (which lists the instances where the minimal height is greater than $2\sqrt{|d|}$ under the Generalized Riemann Hypothesis), along with Theorem 2.2.3, the only possibilities are $d = -1$ or $d = -2$. Elements of minimal height are $\sqrt{d}$ in each of these instances. The
unconditional statement follows directly from the current theorem and Theorem 2.2.3.

\[ \square \]

**Theorem 2.5.4.** Let \( d \equiv 1 \pmod{4} \) be a negative, squarefree integer. Let \( c \) denote the smallest height among all generators of \( \mathbb{Q}(\sqrt{d}) \) over \( \mathbb{Q} \). Let \( \alpha = \frac{a + b \sqrt{d}}{e} \) range over height-reduced elements of \( \mathbb{Q}(\sqrt{d}) \).

1. The height of any element \( \frac{A + B \sqrt{d}}{E} \) is a natural number. In particular, \( c \) is a natural number.

2. \( \alpha \) has height less than \( \sqrt{|d|} \) only if \( b = 1 \).

3. If \( |d| > N_0 \), then \( c < \sqrt{|d|} \). More generally, for any \( \gamma \in \left[ \frac{5}{4\sqrt{3}}, 1 \right] \), if \( |d| \) is large enough, then \( c < \gamma \sqrt{|d|} \). Assuming the Generalized Riemann Hypothesis, if \( |d| > 955 \), then \( c < \sqrt{|d|} \).

4. Suppose that \( \alpha \) lies in the set of generators with height \( c \). It is possible to choose \( \alpha \) with \( e = c \). If \( |d| > N_0 \), then it is possible to choose \( \alpha \) with \( e = c \) and \( b = 1 \); assuming the Generalized Riemann Hypothesis, this is always possible.

5. Let \( n \) be the smallest odd integer larger than \( \frac{\sqrt{|d|}}{2} \) such that \( d \) is a square modulo \( n \). If \( n \geq \frac{1}{\sqrt{3}} \sqrt{|d|} \), then \( c \leq n \). If \( n < \frac{1}{\sqrt{3}} \sqrt{|d|} \), then \( c \leq \frac{5n}{4} < \frac{5}{4\sqrt{3}} \sqrt{|d|} \).

6. If \( |d| > N_0 \), then the element \( \frac{\tilde{a} + \sqrt{\tilde{d}}}{2c} \) satisfies the equation \( z^2 = xy + d \) subject to the conditions that \( x > \sqrt{|d|} > 0 \), \( x \geq y > 0 \), \( x \) and \( y \) are even, \( \frac{x}{2} \geq z \geq 0 \) is odd, and \( x \) is minimal among all such solutions, has height equal to \( c = \frac{2c}{2} \). Assuming the Generalized Riemann Hypothesis, this is always the case.
Proof. For (1), the proof given for general field elements in Theorem 2.5.2 again works in this case. A proof for height-reduced elements is given below.

As in the proof of Theorem 2.5.2, the primitive minimal polynomial of $\alpha$ has leading coefficient $e$. If $e \geq \sqrt{N\left(\left(a + b\frac{d}{e}\right)\right)} = \left|a + b\frac{d}{e}\right| = \left|a + b\frac{\sqrt{d}}{e}\right| \geq \left\lceil b\frac{\sqrt{|d|}}{2} \right\rceil$, then

$$H(\alpha) = e \max\left(1, \left|a + b\frac{\sqrt{d}}{e}\right|\right) \cdot \max\left(1, \left|a + b\frac{\sqrt{d}}{e}\right|\right) = e.$$

If $e < \sqrt{N\left(\left(a + b\sqrt{d}\right)\right)}$, then $H(\alpha) = \frac{N((\alpha))}{e} > \sqrt{N\left(\left(a + b\frac{\sqrt{d}}{e}\right)\right)} \geq \left\lceil b\frac{\sqrt{|d|}}{2} \right\rceil$. Hence, the height of every height-reduced element of $Q(\sqrt{d})$ is an integer at least as large as $\left\lceil b\frac{\sqrt{|d|}}{2} \right\rceil$. Therefore, $H(\alpha) < \sqrt{|d|}$ only if $b = 1$, which proves (2). Since a generator of minimal height may be taken to be height-reduced, this proves the second sentence of (1). Moreover, if $\alpha = \frac{a + b\frac{\sqrt{d}}{e}}{e}$ is height-reduced and has height $c$, then $c$ equals either $e$ or $\frac{N((\alpha))}{e}$. Now, the Galois conjugate of $\frac{1}{\alpha}$ is also height-reduced with height $c$ and replacing $\alpha$ by the Galois conjugate of $\frac{1}{\alpha}$ replaces $e$ by $\frac{N((\alpha))}{e}$; hence, there is a height-reduced generator $\alpha$ such that $H(\alpha) = c$ and $c = e$. This proves the first claim in (4).

Suppose that there is an integer $r \in \left(\frac{\sqrt{|d|}}{2}, \sqrt{|d|}\right)$ such that $d$ is a square modulo $r$. This implies that there is an odd integer $k \in \{1, \ldots, \left\lfloor \frac{r}{2} \right\rfloor \}$ and a natural number $m$ that is divisible by 4 such that $k^2 - d = rm$. (If $d$ is a square modulo the odd number $r$, then the equation $x^2 - d = ry$ has a solution in integers with $x \leq \left\lfloor \frac{r}{2} \right\rfloor$. If $x$ is even, then $r - x \leq r$ is odd. Reducing the equation modulo 4 shows that $ry \equiv 0 \pmod{4}$ since any odd square is congruent to 1 modulo 4 and $-d \equiv 3 \pmod{4}$.)

$$|k + \sqrt{d}| = \sqrt{k^2 - d} \leq \sqrt{r^2 + |d|}.$$
Suppose first that \( r \in \left( \frac{1}{\sqrt{3}} \sqrt{|d|}, \sqrt{|d|} \right) \). In this case, \(|d| < 3r^2\) so that

\[ |k + \sqrt{d}| < \sqrt{r^2 + 3r^2} = 2r. \]

Hence, the element \( \frac{k + \sqrt{d}}{2r} \) has height equal to \( r \) which is less than \( \sqrt{|d|} \). This implies that, when such an integer exists, the minimal height of a generator is less than \( \sqrt{|d|} \). In this case, when looking for height-reduced elements \( \alpha \) with minimal height and \( e = c \), it suffices to further assume that \( b = 1 \) and \( a \geq 0 \). Now suppose that \( r \in \left( \frac{\sqrt{|d|}}{2}, \frac{\sqrt{|d|}}{\sqrt{3}} \right) \). If it happens to be the case that \(|k + \sqrt{d}| \leq 2r\), then, as above, the element \( \frac{k + \sqrt{d}}{2r} \) has height equal to \( r \) which is less than \( \sqrt{|d|} \). If, instead, \(|k + \sqrt{d}| > 2r\), then \( \frac{k + \sqrt{d}}{2r} \) has height \( \frac{m}{4} > |k + \sqrt{d}| \) and \( \frac{m}{4} \leq \frac{5r}{4} < \frac{5}{\sqrt{3}} \sqrt{|d|} < \sqrt{|d|} \) because dividing the equation \( k^2 + |d| = rm \) through by \( 4r^2 \) and using the constraints on \( k \) and \( r \) shows that

\[ \frac{m}{4r} = \left( \frac{k}{2r} \right)^2 + \frac{|d|}{4r^2} \leq \frac{1}{4} + 1 = 5 \frac{4}{4}. \]

Hence, in this case as well, when looking for elements satisfying the same conditions as \( \alpha \), it suffices to further assume that \( b = 1 \) and \( a \geq 0 \).

As in the proof of Theorem 2.5.2, Theorem 2.4.2 shows that there is such an element \( r \in \left( \frac{\sqrt{|d|}}{2}, \sqrt{|d|} \right) \) for all \(|d| > N_0\). Assuming the Generalized Riemann Hypothesis, for \(|d| \geq 3609419832785\), Lemma 2.5.1 shows that there is a prime \( p \in \left( \frac{\sqrt{|d|}}{2}, \sqrt{|d|} \right) \) such that \( d \) is a square modulo \( p \). Direct computation ([OSC]) shows that the only values of \( d \) that are negative, squarefree, congruent to 1 modulo 4, and have absolute value less than 3609419832785 such that there is no element with height less than \( \sqrt{|d|} \) are \(-19, -43, -67, -163, -267, -499\) and \(-955\). An element of minimal height in each of these cases is \( \frac{1 + \sqrt{-19}}{2}, \frac{1 + \sqrt{-43}}{2}, \frac{1 + \sqrt{-67}}{2}, \frac{1 + \sqrt{-163}}{2}, \frac{3 + \sqrt{-267}}{40}, \frac{1 + \sqrt{-499}}{90}, \) and \( \frac{5 + \sqrt{-955}}{70} \),
respectively. Hence, for all $|d| > N_0$, or for all $|d|$ assuming the Generalized Riemann Hypothesis, it is always possible to choose $\alpha$ with height $c$ such that $c = c'$ and $b = 1$. This proves (3) and the rest of (4).

The results of (5) and (6) will now follow from the previous paragraph and Theorem 2.3.1. There is an element of smallest height of the form $\frac{a + \frac{1 + \sqrt{d}}{2}}{c}$ where $c \mid N\left((a + \frac{1 + \sqrt{d}}{2})\right)$ and $c \geq \frac{\sqrt{a^2 - d}}{2}$, for all $|d| > N_0$, or for all $|d|$ assuming the Generalized Riemann Hypothesis; when this holds, this implies that there is some integer $\ell$ such that $\frac{a^2 - d}{4} = c\ell$, i.e. such that $a^2 = (2c)(2\ell) + d$.\footnote{It is interesting to note that $d$ is a square modulo $c$.} Suppose that this condition holds. If $a \geq 2c$, then by subtracting the appropriate multiple of $2c$ from both sides shows that there is an element of smallest height of the form $\frac{a + \frac{1 + \sqrt{d}}{2}}{c}$ where $c \mid N\left((a + \frac{1 + \sqrt{d}}{2})\right)$, $a < 2c$, and $c \geq \frac{\sqrt{a^2 - d}}{2}$ (use the division algorithm to write $a = 2cq + a'$ for some $0 \leq a' < 2c$). If $a > c$, then replacing $a$ by $2c - a$ and changing $\ell$ to $\ell + c - a$ shows that there is an element of smallest height of the form $\frac{a + \frac{1 + \sqrt{d}}{2}}{c}$ where $c \mid N\left((a + \frac{1 + \sqrt{d}}{2})\right)$, $a < c$, and $c \geq \frac{\sqrt{a^2 - d}}{2}$. Now, in the equation $a^2 = (2c)(2\ell) + d$, if $\ell > c$, then $\ell > \frac{\sqrt{a^2 - d}}{2}$ so that $c\ell > \left(\frac{\sqrt{a^2 - d}}{2}\right)^2 = \frac{a^2 - d}{4}$. Since this contradicts the definition of $\ell$, $\ell$ is at most $c$. Conversely, any solution of the equation $z^2 = (2x)(2y) + d$ with $x \geq y$ and $z \leq x$ gives an element $\frac{z + \frac{1 + \sqrt{d}}{2}}{x} \in \mathbb{Q}(\sqrt{d})$ with height $x$. This completes the proof.

Corollary 2.5.5. Let $d \equiv 1 \pmod{4}$ be a negative, squarefree integer. The minimal height value of a generator of $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$ is never attained by an algebraic integer for $|d|$ sufficiently large. Assuming the Generalized Riemann Hypothesis, the minimal
height value of a generator of $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$ is attained by an algebraic integer if and only if $d \in \{-3, -7, -11, -19, -43, -67, -163\}$.

Proof. \(\frac{|d|+1}{4} \leq \sqrt{|d|}\) if and only if $0 \neq |d| < (2 + \sqrt{3})^2 < 15$. Checking the small values of $d \in \{-3, -7, -11\}$ directly shows that elements of minimal height in these cases are $\frac{1+\sqrt{-3}}{2}$, $\frac{1+\sqrt{-7}}{2}$, and $\frac{1+\sqrt{-11}}{2}$, respectively. Now, given the theorem and its proof (which lists the instances where the minimal height is greater than $\sqrt{|d|}$ under the Generalized Riemann Hypothesis), along with Theorem 2.2.3 the only possibilities are those listed above. Elements of minimal height are given in the proof of the theorem for $d \in \{-19, -43, -67, -163\}$. The unconditional statement follows directly from the current theorem and Theorem 2.2.3.

It is interesting to note that, unlike in the case of an integral generator of smallest height, it is possible for two elements that are not related by inversion, negation, or Galois conjugation to share the same minimal height. Here are a few examples.

**Example 4.** In $\mathbb{Q}(\sqrt{-33})$, $\frac{3+\sqrt{-33}}{6}$ and $\frac{4+\sqrt{-33}}{7}$ each have height 7, which is minimal in this field among generators. These elements are not related by inversion, negation, or Galois conjugation and the element

$$\left(\frac{3+\sqrt{-33}}{6}\right)\left(\frac{4+\sqrt{-33}}{7}\right) = \frac{-3 + \sqrt{-33}}{6}$$

also has height 7 since it is the negative of the Galois conjugate of the first element! In fact, a relationship between the two elements on the left-hand side of this equation is given in Theorem 2.5.2, part (6), as explained below.

For this field, the element of minimal height found in the theorem, $\frac{3+\sqrt{-33}}{7}$, is found via the equation $3^2 + 33 = 7 \cdot 6$. Its inverse is the first element listed above.
\[-3 \equiv 4 \pmod{7}, \text{ so since it happens to be the case that } \sqrt{4^2 + 33} = 7 \leq \frac{4 + \sqrt{-33}}{7} \text{ also has minimal height. This follows from the very same argument given in the proof of the theorem, or just by direct computation. It also happens to be the case that } 3 \text{ is half of } 6, \text{ so, using the notation of the theorem, Equation 2.3 is an instance of the identity } \left(\frac{z+\sqrt{-d}}{y}\right)\left(\frac{x-\sqrt{-d}}{x}\right) = \frac{z-y+\sqrt{-d}}{y} \text{ that coincidentally has this extra equal-height property.}

**Example 5.** In \(\mathbb{Q}(\sqrt{-22})\), the elements \(\sqrt{-22}_{11}\) and \(\sqrt{-22}_4\) each have the smallest height among generators of \(\mathbb{Q}(\sqrt{-22})\) over \(\mathbb{Q}\). The reason for this is given in Theorem 2.3.3. (Note that \(\sqrt{-22}_{11}\) is the negative of the inverse of \(\sqrt{-22}_2\), that \(\sqrt{-22}_4 = \frac{\sqrt{-22}}{2}\), and that \(N\left(\frac{\sqrt{-22}}{2}\right) = \frac{11}{2}\).)

The following three corollaries are really corollaries of the joint results of Theorems 2.5.2 and 2.5.4, in conjunction with Theorem 2.4.2. Note that the polynomial-height and the height of a generator, even in the imaginary quadratic case, need not be the same. For example, the polynomial \(33x^2 + 42x + 20\) has polynomial-height 42; but the (non-real) roots of this polynomial have absolute value less than 0.7785 so that their height is equal to 33.

**Definition.** For a negative fundamental discriminant \(D\), \(H_{\min}(D)\) will denote the minimal height of a generator of \(\mathbb{Q}(\sqrt{D})\) over \(\mathbb{Q}\).

**Corollary 2.5.6.** For negative, squarefree \(d\) with \(|d| > N_0\), \(\hat{H}_{\min}(D) = H_{\min}(D)\). This is always true if one assumes that the Generalized Riemann Hypothesis holds.

**Proof.** This follows directly from Theorems 2.4.2, 2.5.2, and 2.5.4. \(\square\)
Corollary 2.5.7. As $D$ ranges over negative fundamental discriminants,

$$\lim_{D \to -\infty} \frac{H_{\min}(D)}{\frac{1}{2} \sqrt{|D|}} = 1.$$  

Proof. This follows directly from the previous corollary and Ruppert’s Theorem 2.4.1. \qed

Further, recall Ruppert’s Conjecture 1.3.7: $\hat{H}_{\min}(D) \leq \frac{41}{\sqrt{163}} \sqrt{|D|}$. His method of proof for Theorem 2.4.1 is ineffective, but assuming the Generalized Riemann Hypothesis this conjecture does indeed hold.

Corollary 2.5.8. Let $D$ be a negative fundamental discriminant. Assuming that the Generalized Riemann Hypothesis holds,

$$\hat{H}_{\min}(D) = H_{\min}(D) \leq \frac{41}{\sqrt{163}} \sqrt{|D|} < 3.22 \sqrt{|D|}.$$  

Proof. The proofs of Theorems 2.5.2 and 2.5.4 show that $H_{\min}(D) \leq \sqrt{|D|}$ for all $D$ except $-19, -43, -67, -88, -148, -163, -232, -267, -499, -708,$ and $-955$. In each of these cases, $\frac{H_{\min}(D)}{\sqrt{|D|}}$ is equal to\(\frac{5}{\sqrt{19}}, \frac{11}{\sqrt{43}}, \frac{17}{\sqrt{67}}, \frac{11}{\sqrt{88}}, \frac{19}{\sqrt{148}}, \frac{41}{\sqrt{163}}, \frac{29}{\sqrt{232}}, \frac{23}{\sqrt{267}}, \frac{25}{\sqrt{499}}, \frac{31}{\sqrt{708}},\) and $\frac{35}{\sqrt{955}}$. The largest of these is $\frac{41}{\sqrt{163}}$. \qed

Finally, recall Theorem 1.3.3 of Roy and Thunder. Here is an equivalent formulation of that result:

Theorem 2.5.9. For any number field $K$, let $i(K)$ be the smallest natural number such that every ideal class of $K$ contains an ideal with norm not exceeding $i(K)$. If $K$ is an imaginary quadratic number field, then

$$3i(K) \leq \frac{|D|}{H_{\min}(D)} \leq 4i(K).$$
It is clear that a number field $K$ has class number 1 if and only if $i(K) = 1$. Theorem 2.5.9 paired with Corollary 2.5.7 and Theorems 2.5.2 and 2.5.4 gives a proof of the following well-known result:

**Theorem 2.5.10.** There are only finitely many imaginary quadratic fields with class number 1. Moreover, assuming the Generalized Riemann Hypothesis, only $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, and $\mathbb{Q}(\sqrt{-163})$ have class number 1.

**Proof.** By Corollary 2.5.7, $H_{\min}(\mathcal{D}) < \sqrt{|\mathcal{D}|}$ for $|\mathcal{D}| > 4N_0$. Hence, for such $\mathcal{D}$, $\sqrt{|D|} = \frac{|\mathcal{D}|}{\sqrt{|D|}} < \frac{|\mathcal{D}|}{H_{\min}(\mathcal{D})} \leq 4i(\mathbb{Q}(\sqrt{D}))$. Since the class index of a number field $K$ is 1 if and only if $K$ has class number 1, this shows that there are only finitely many imaginary quadratic fields with class number 1. Assuming the Generalized Riemann Hypothesis, Theorems 2.5.2 and 2.5.4 give a bound for “sufficiently large”, so direct computation completes the proof. \qed

Further, this theorem, paired with Corollaries 2.5.3 and 2.5.5, gives a characterization of imaginary quadratic fields with class number 1 in terms of heights of generators:

**Corollary 2.5.11.** Assuming the Generalized Riemann Hypothesis, the minimal height of a generator of $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$, where $d$ is a negative, squarefree integer, is achieved by an algebraic integer if and only if $\mathbb{Q}(\sqrt{d})$ has class number 1.
2.6 Generators of Smallest Height in Real Quadratic Extensions of $\mathbb{Q}$.

Corollary 2.3.2 puts one restriction on looking for generators $\alpha = \frac{a+b\sqrt{d}}{c}$ of smallest height in $\mathbb{Q}(\sqrt{d})$. Pairing this result with Theorems 2.2.1 and 2.2.2 helps puts additional restrictions as well in the relevant cases. This highlights the difference between the real and imaginary quadratic field cases.

**Theorem 2.6.1.** Let $d \not\equiv 1 \pmod{4}$ be a positive, squarefree integer. Suppose that $\alpha = \frac{a+b\sqrt{d}}{c}$ is height-reduced. If $\alpha$ has minimal height among all generators of $\mathbb{Q} (\sqrt{d})$, then $b = 1$ and $a < \sqrt{d}$. There exists an element $\frac{a'+\sqrt{d}}{c'}$ with minimal height among all generators such that $c' < \sqrt{d}$.

**Proof.** As in the proof of Theorem 2.5.2, the leading coefficient of the minimal polynomial of $\alpha$ is $c$.

If $c \geq a+b\sqrt{d}$, then, by the formula for height in terms of Mahler measure (Theorem 1.1.6),

$$H(\alpha) = c \max \left( 1, \left| \frac{a+b\sqrt{d}}{c} \right| \right) \cdot \max \left( 1, \left| \frac{a-b\sqrt{d}}{c} \right| \right)$$

$$= c \geq a+b\sqrt{d}$$

$$\geq b\sqrt{d}$$

since $|a-b\sqrt{d}| \leq |a| + |b\sqrt{d}| = a+b\sqrt{d} \leq c$. Since $H(\alpha) < 2\sqrt{d}$, by Theorem 2.2.1, it follows that $b$ must equal 1.

If $c < a+b\sqrt{d}$, then $H(\alpha) = c \max \left( 1, \left| \frac{a+b\sqrt{d}}{c} \right| \right) \cdot \max \left( 1, \left| \frac{a-b\sqrt{d}}{c} \right| \right) \geq c \frac{a+b\sqrt{d}}{c} = a+b\sqrt{d}$. As before, Theorem 2.2.1 shows that $b$ must equal 1.
The above calculations show that \( H(\alpha) \geq a + \sqrt{d} \). Theorem 2.2.1 again shows that \( a \) must be less than \( \sqrt{d} \). Hence, \( N((a + \sqrt{d})) = d - a^2 = c\ell \) for some integer \( \ell > 0 \). Either \( c < \sqrt{d} \) or \( \ell < \sqrt{d} \) (otherwise, \( d - a^2 = c\ell > d \), which is impossible). \( H(\alpha) = H\left(\frac{a + \sqrt{d}}{\ell}\right) \) since \( \alpha \) and \( \frac{a + \sqrt{d}}{\ell} \) are negative Galois conjugates of each other. This completes the proof.

\[ \square \]

**Corollary 2.6.2.** Let \( d \not\equiv 1 \pmod{4} \) be a positive, squarefree integer. The minimal height value for a generator of \( \mathbb{Q}(\sqrt{d}) \) over \( \mathbb{Q} \) is either a natural number greater than \( \sqrt{d} \) or a natural number plus \( \sqrt{d} \).

**Theorem 2.6.3.** Let \( d \not\equiv 1, d \equiv 1 \pmod{4} \) be a positive, squarefree integer. Suppose that \( \alpha = \frac{a + b\sqrt{d}}{c} \) is height-reduced. If \( \alpha \) has minimal height among all generators of \( \mathbb{Q}(\sqrt{d}) \), then \( b = 1 \) and \( a \geq 0 \).

**Proof.** As in the proof of Theorem 2.6.1, if \( a \geq 0 \), then

\[
H(\alpha) \geq a + b\frac{1 + \sqrt{d}}{2} \geq \frac{b}{2}(1 + \sqrt{d})
\]

so that \( b = 1 \) by Theorem 2.2.2. If \( a < 0 \), then note that \( a + b \geq 1 \). The argument is now similar to the others:

\[
H(\alpha) \geq \left| a + \frac{b + 1 + \sqrt{d}}{2} \right| \\
= a + b + b\frac{\sqrt{d} - 1}{2} \\
\geq 1 + b\frac{\sqrt{d} - 1}{2};
\]

since this is at least \( \sqrt{d} \) if \( b > 1 \), Theorem 2.2.2 again completes the argument. The fact that \( a \geq 0 \) is now trivial since \( a < 0 \) implies that \( b \geq 2 \).
Corollary 2.6.4. Let \( d \neq 1, d \equiv 1 \pmod{4} \) be a positive, squarefree integer. The minimal height value for a generator of \( \mathbb{Q}(\sqrt{d}) \) over \( \mathbb{Q} \) is either a natural number greater than \( \frac{1 + \sqrt{d}}{2} \) or a non-negative integer plus \( \frac{1 + \sqrt{d}}{2} \).

There are some cases where it is easy to find a generator of minimal height. This ease evidently arises from the ordering of the real numbers.

Example 6. When \( d > 0, d \not\equiv 1 \pmod{4} \), there is a generator of height \( \lceil \sqrt{d} \rceil \) if and only if \( \lceil \sqrt{d} \rceil \mid d \): If \( \lceil \sqrt{d} \rceil \mid d \), then \( \frac{\sqrt{d}}{\lceil \sqrt{d} \rceil} \) has height \( \lceil \sqrt{d} \rceil \). If \( \lceil \sqrt{d} \rceil \) is the height of some element \( a + \sqrt{d} \) with \( a \geq 0 \) and \( c \geq 1 \), then as in the proof of Theorem 2.6.1, \( \lceil \sqrt{d} \rceil \geq a + \sqrt{d} \) so that \( a = 0 \) and either \( \lceil \sqrt{d} \rceil = c \mid d \) or \( \lceil \sqrt{d} \rceil = \frac{d}{c} \mid d \).

Incidentally, there are infinitely many such \( d \). \( d = n(n + 1) \) for some integer \( n \) if and only if \( \lceil \sqrt{d} \rceil \mid d \). To show that there are infinitely many squarefree \( d \) with \( \lceil \sqrt{d} \rceil \mid d \), it therefore suffices to show (actually, it is equivalent to the statement) that there are infinitely many pairs of consecutive squarefree integers. This, however, follows easily from the fact that the density of the set of squarefree integers is \( \frac{6}{\pi^2} > \frac{1}{2} \).

Example 7. When \( d > 0, d \not\equiv 1 \pmod{4} \), if \( d - 1 \) is a square, then there is a generator of height \( \sqrt{d} + 1 \): \( \frac{1 + \sqrt{d}}{\sqrt{d} - 1} \) has height \( \sqrt{d} + 1 \). By Corollary 2.6.2 and Example 6, this is the smallest possible height value of a generator. More generally, when \( d \not\equiv 1 \pmod{4} \), if \( d - n^2 \) is a square, then there is a generator of height \( \sqrt{d} + n \); however, this need not be the minimal height: take \( d = 34, n = 3 \), and compare with \( H \left( \frac{2 + \sqrt{34}}{8} \right) = 2 + \sqrt{34} \).

Incidentally, there are infinitely many squarefree \( d \) such that \( d = n^2 + 1 \) for some integer \( n \). For example, see [Na] where it is shown that a polynomial of degree 2 with
integer coefficients that is primitive, has no repeated roots, and such that the greatest common divisor of \( \{ f(n) : n \in \mathbb{N} \} \) is squarefree has infinitely many squarefree values. Note that this result guarantees infinitely many squarefree \( d = n^2 + 1 \) that are either congruent to 1 or 2 modulo 4. In the 1 modulo 4 case, there is a generator of height \( \frac{1 + \sqrt{d}}{2} \), namely \( \frac{1 + \sqrt{d}}{2} \) itself. By Corollary 2.6.4, this is the minimal height of a generator in \( \mathbb{Q}(\sqrt{d}) \). However, replacing \( n \) by \( 2n + 1 \) (or \( 2n \)) and using the Nagell result on the resulting polynomial shows that there are infinitely many squarefree \( d = n^2 + 1 \) congruent to 2 (and 1) modulo 4.

Example 6 shows that in the case discussed there, the integers are not a good source of generators of minimal height in \( \mathbb{Q}(\sqrt{d}) \) even in the real quadratic case. The following two conjectures show this point. They remain conjectures solely because the required computations have not yet been done, although they are eminently doable.

**Conjecture 2.6.5.** Let \( d \not\equiv 1 \pmod{4} \) be a positive, squarefree integer. Assume the Generalized Riemann Hypothesis. The minimal height value of a generator of \( \mathbb{Q}(\sqrt{d}) \) over \( \mathbb{Q} \) is attained by an algebraic integer if and only if \( d = 2 \) or \( d = 3 \).

**Proof.** (Sketch) If \( d = 2 \), then \( \sqrt{2} \) has height 2 = \( \lceil \sqrt{2} \rceil \). If \( d = 3 \), then \( 1 + \sqrt{3} \) has height equal to itself. As explained in Example 6 and Corollary 2.6.2, this is the smallest height value of a generator. Conversely, it suffices to construct an element whose height is smaller than either \( 2\lceil \sqrt{d} \rceil \) or \( \sqrt{d} + \lfloor \sqrt{d} \rfloor \) when \( d - 1 \) is either a square or not, respectively. In the former case, \( d \) must be equal to 2 or be at least 10 so that either \( d = 2 \) or \( \lfloor \sqrt{d} \rfloor \geq 3 \) and \( \frac{\sqrt{d} + 1}{\sqrt{d} - 1} \) has height \( \sqrt{d} + 1 \). Constructing elements in the latter case is seemingly not as easy. Instead, invoking Lemma 2.5.1 for
Conjecture 2.6.6. Let \( d \neq 1, d \equiv 1 \pmod{4} \) be a positive, squarefree integer. Assume the Generalized Riemann Hypothesis. The minimal height value of a generator of \( \mathbb{Q}(\sqrt{d}) \) over \( \mathbb{Q} \) is attained by an algebraic integer if and only if \( d \in \{5, 13, 21, 29, 53, 77, 173, 293, 437\} \).

Proof. (Sketch) If \( d \) equals 5, 13, 21, 29, 53, 77, 173, 293, or 437, then \( \mathbb{Q}(\sqrt{d}) \) has elements \( \frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{13}}{2}, \frac{3+\sqrt{21}}{2}, \frac{3+\sqrt{29}}{2}, \frac{5+\sqrt{53}}{2}, \frac{7+\sqrt{77}}{2}, \frac{11+\sqrt{173}}{2}, \frac{15+\sqrt{293}}{2}, \) or \( \frac{19+\sqrt{437}}{2} \) with heights \( \frac{1+\sqrt{5}}{2}, 3, \frac{3+\sqrt{21}}{2}, 7, \frac{7+\sqrt{77}}{2}, 13, 17, \) or \( \frac{19+\sqrt{437}}{2} \), respectively. Direct computation shows that these are elements of minimal heights in these cases. Conversely, it suffices to construct an element whose height is smaller than \( \frac{\sqrt{d}+\lfloor\sqrt{d}\rfloor-1}{2} \). Invoking Lemma 2.5.1 for \( d > 3609445221315 \) gives an element \( \alpha = \frac{a+\sqrt{d}}{p} \in \mathbb{Q}(\sqrt{d}) \) such that \( \frac{\sqrt{d}}{2} \leq p < \frac{\sqrt{d}+\lfloor\sqrt{d}\rfloor-3}{2} \) and \( 0 \leq a \leq p < \frac{\sqrt{d}+\lfloor\sqrt{d}\rfloor-3}{2} \) so that \( H(\alpha) \) is either equal to \( p \) or \( \frac{a+\sqrt{d}}{2} \), both of which are strictly smaller than \( \frac{\sqrt{d}+\lfloor\sqrt{d}\rfloor-1}{2} \). For smaller values of \( d \), direct computation should complete the proof. □

It is interesting to point out, in light of Corollary 2.5.11, that all (conjecturally) of the real quadratic fields with minimal height attained by an integer have class number 1. Of course, there are many other real quadratic fields that have class number 1. However, the fundamental units in these cases, when written in either the form \( a+b\sqrt{d} \) or \( a+b\frac{1+\sqrt{d}}{2} \), have \( b = 1 \). It would be very interesting if this condition
on the fundamental unit together with the class number 1 condition is equivalent to having the minimal height attained by an integer.

Finally, here is one further conjecture that is similar to Conjecture 1.3.9. It too is based on numeric evidence, but there are no larger-$|d|$ results to help prove it.

**Conjecture 2.6.7.** Recalling that

\[ H_{\min}(D) = \min \{ H(\alpha) : \mathbb{Q}(\alpha) \text{ is a quadratic extension of } \mathbb{Q} \text{ with discriminant } D \}, \]

\[ \lim_{D \to \infty} \frac{H_{\min}(D)}{\frac{1}{2} \sqrt{|D|}} = 1. \]
3.1 The Real Quadratic Case and More

The most obvious avenue for continuation is resolving Conjecture 2.6.7 and the comment in the paragraph preceding it. The numeric evidence for this conjecture, namely doing a brute-force search for elements of smallest height in real quadratic extensions and then looking at trends, is compelling. A first attack was to mimic the argument given in the imaginary quadratic case. Unfortunately, while that works for small $d$, there are cases where it fails to work. Attempts at making slight modifications in the statements of Theorems 2.5.2 and 2.5.4 (part (6)) appear to resolve some of these cases, but there are always new cases that are not resolved. The lack of an apparent general relationship (let alone equality) with the minimal polynomial-height makes this case more challenging. It does appear, however, that when the minimal height of a generator of a given real quadratic field is equal to an integer, then that value is equal to the value of the minimal polynomial-height of such a generator. Unfortunately, even this has resisted proof so far. As usual with real quadratic fields, however, these apparently elementary observations may have their proofs (or disproofs) lying quite deep.
Beyond the real quadratic case, theorems like Theorem 1.3.10 show that imposing certain conditions on $\mathbb{Q}(\alpha)$ may lead to results. The totally real condition and the prime degree condition seem possibly problematic, however, as exhibited in the real quadratic case. Perhaps totally imaginary extensions are a possibility, but this too is unclear.

### 3.2 Relative Heights

In 1989, Bergé and Martinet [BeMa] introduced relative heights. Given a number field $K$, a point $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$, and a number field $L$ such that $P \in \mathbb{P}^n(L)$, they define the height of $\alpha$ relative to $K$ as

$$H_L(K; \alpha) = \inf_{i \in \mathbb{Z}, \epsilon_j \in \mathcal{O}_K^\times} \left( H\left( \left[ \epsilon_0^{1/i} x_0, \ldots, \epsilon_n^{1/i} x_n \right] \right) \right)^{[L:Q]} ,$$

where now the function $H(P) = \exp(h(P))$ is the non-logarithmic absolute Weil height (“Weil height”, for the purposes of this section). This reduces to the Weil height when $K = \mathbb{Q}$. de la Maza [De] shows that the relative height behaves much like the Weil height on other occasions though. In particular, when $L = K$ or $K$ is a totally real extension and $L$ is a totally complex quadratic extension of $K$,

$$H_L(K; \theta) = \max (N(c), N(b)) ,$$

where $(\theta) = \frac{1}{n}$ for relatively prime integral ideals $\mathfrak{b}$ and $\mathfrak{c}$. Perhaps the relative height functions in these cases are close enough to the Weil height function to enable the statements, and even the proofs, of the main results of this work to remain valid when one uses the relative height functions instead of the height functions used here.
Relative height functions appear to have gone largely unnoticed. It would be interesting to see which results can directly translate and which ones cannot, as well as reasons why they can or cannot translate.
Appendix A
PARi/GP CODE

In order to do the computations in Chapter 2, the number theory computing package PARi/GP [PARI2] was used. There are two distinct programs that were used to examine the “small” values of $|d|$, one for the $d \not\equiv 4 \pmod{4}$ case and one for the $d \equiv 1 \pmod{4}$ case where $d$ is a negative, squarefree integer. They are listed below in that order.

The first code is fairly straightforward, it simply checks if $d$ is a square modulo $x$ for some $x$ in a certain range. The second code is slightly more complicated because $x$ is required to be odd. As noted in the proof of Theorem 2.5.4, this restriction is what allows one to apply the Chebotarev Density Theorem argument.

```plaintext
for(d=<start value>,<end value>,
   if(d%4<>1 && issquarefree(d),
      x=ceil(sqrt(-d));
      while(!issquare(Mod(d,x)) && x<2*sqrt(-d),
         x=x+1
      );
   if(x>2*sqrt(-d),
      print("d=",d," is bad!")
   )
```

79
In order to find minimal heights within any \textit{fixed} real quadratic extension when \( d \) is not congruent to 1 modulo 4, the following code was used. The code for the other quadratic cases was similar. It uses the relationship between the polynomial-height and the height in conjunction with a (hopefully) good initial guess at an element with minimal height in order to bound the possible coefficients of minimal polynomials for elements with small height. As exhibited in the theorems concerning minimal heights of algebraic integers versus general field elements, the guesses coming from
the algebraic integers were always pretty good in the real case but quickly became very bad in the imaginary case.

\[
\text{for}(d=\text{<start value>}, \text{<end value>}, \\
\hspace{1cm} \text{if}(d\%4\neq1 \&\& \text{issquarefree}(d), \\
\hspace{2cm} srootd=\text{sqrt}(d); \\
\hspace{2cm} target=srootd+\text{floor}(srootd); \\
\hspace{2cm} bound=\text{floor}(4*\text{target}); \\
\hspace{2cm} \text{minht}=[\text{target},1,-2*\text{floor}(srootd),-d+\text{floor}(srootd)^2]; \\
\hspace{2cm} \text{for}(n=1,\text{floor}(\text{target}), \\
\hspace{3cm} \text{for}(m=0,\text{bound}, \\
\hspace{4cm} \text{if}(m\%2==0, \\
\hspace{5cm} \text{for}(k=-1*\text{bound},n, \\
\hspace{6cm} \text{disc}=m^2-4*n*k; \\
\hspace{6cm} \text{if}((\text{disc}>0) \&\& ((k<0 \&\& n<-k)|| (k>0)) \&\& \\
\hspace{7cm} (\text{gcd}(n,\text{gcd}(m,k))==1) \&\& \\
\hspace{7cm} ((\text{disc} \% d)==0) \&\& \text{issquare}(\text{disc}/d) \&\& \\
\hspace{7cm} (n*\text{max}(1,\text{abs}((-m+\text{sqrt}(\text{disc}))/(2*n)))* \\
\hspace{8cm} \text{max}(1,\text{abs}((-m-\text{sqrt}(\text{disc}))/(2*n)))<=\text{minht}[1]), \\
\hspace{8cm} \text{minht}=[n*\text{max}(1,\text{abs}((-m+\text{sqrt}(\text{disc}))/(2*n)))* \\
\hspace{8cm} \text{max}(1,\text{abs}((-m-\text{sqrt}(\text{disc}))/(2*n))),n,m,k] \\
\hspace{5cm}) \\
\hspace{4cm}) \\
\hspace{3cm}) \\
\hspace{2cm}) \\
\hspace{1cm}) \\
\text{minht} \\
\text{81}
BIBLIOGRAPHY


[OSC] Ohio Supercomputer Center.

[RoTh] Damien Roy; Jeffrey Thunder, Bases of Number Fields with Small Height, Rocky Mountain J. Math. 26 (1996), 1089-1098.


