Some Typical Examples of Calculating the Class Number h_K with Using Minkowski Bound

$L^{I}G_{U}O$

September 28, 2024

For a number field K, the Minkowski bound $M_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|\Delta_K|}$ where r_2 is the number of pairs of complex embeddings of K, n is the degree of K over $\mathbb{Q}$ and Δ_K is the discriminant of K, is a useful tool to estimate the class number h_K of K.[1] In this note, we will give some typical examples of calculating the class number h_K using Minkowski bound.

The importance of Minkowski bound lies in that for arbitrary ideal class $[\mathfrak{b}]$ of K, there exists an integral ideal $\mathfrak{a}$ s.t. $[\mathfrak{a}] = [\mathfrak{b}]$ and $\mathrm{N}(\mathfrak{a}) \leq M_K$. We can even use a weaker conclusion which says $\mathrm{Cl}(K) = \{[\mathfrak{p}] \mid \mathfrak{p} \cap \mathbb{Z} =: p \leq M_K\}$.[2]

The calculation process

$$\xrightarrow[\text{Choose a suitable integral basis}]{} \text{Calculate} \Delta_K \text{ and } M_K$$

$$\xrightarrow[\substack{\text{Use Some Facts}\\ \text{Inspect } (\alpha) \text{ for small } \alpha \in \mathcal{O}_K}]{} \text{Consider ideal decomposition of all prime numbers } p \leq M_K$$

$$\xrightarrow[\text{Get all orders and relations of } [\mathfrak{p}]]{} \text{Get the structure of } \mathrm{Cl}(K) \text{ and } h_K$$

1 Examples

During the calculation, we will use the following facts:

(i) If $K = \mathbb{Q}(\sqrt{d})$ with d squarefree, then $\Delta_K = \begin{cases} d & \text{if } d \equiv 1 \bmod 4 \\ 4d & \text{if } d \equiv 2, 3 \bmod 4 \end{cases}$; If p is odd and unramified, then p splits $\iff \left(\frac{d}{p}\right) = 1$; 2 splits $\iff d \equiv 1 \bmod 8$, when $d \equiv 1 \bmod 4$.

(ii) Dedekind's theorem: $p \mid \Delta_K \iff (p)$ ramified in $\mathcal{O}_K$

(iii) Let L be a number field extension over K $L = K(\alpha)$ with $\alpha \in \mathcal{O}_L$, and $f(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of α over K. If $\mathfrak{p} \nmid |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$, denote $f(x) = f_1(x)^{e_1} \cdots f_g(x)^{e_g} \pmod{\mathfrak{p}}$

[1] The class number characterizes the degree of failure of the unique decomposability of elements in $\mathcal{O}_K$, more explicitly, $h_K = 1 \iff$ UFD $\iff$ PID in $\mathcal{O}_K$.

[2] There follows $h_{\mathbb{Q}(\sqrt{d})} = 1$ for $d = -1, \pm 2, \pm 3, 5, -7, 13$ because their Minkowski bounds are all less than 2.

with all $p_k(x)$ are moinc and pairwise different irreducible polynomials in $\mathcal{O}_K/\mathfrak{p}[x]$. Then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$, with $\mathfrak{P}_i = (\mathfrak{p}, f_i(\alpha)), e_i = e(\mathfrak{P}_i/\mathfrak{p}), f(\mathfrak{P}_i/\mathfrak{p}) = \deg f_i(x)$ for all i.[3]

1.1 Complex Quadratic Fields $K = \mathbb{Q}(\sqrt{-d})$

In this case, we have $r_2 = 1, n = 2$ and $M_K = \left(\frac{4}{\pi}\right)\frac{2!}{2^2}\sqrt{|\Delta_K|} = \frac{2}{\pi}\sqrt{|\Delta_K|}$.

Example 1: $K = \mathbb{Q}(\sqrt{-5})$.

$-5 \equiv 3 \bmod 4, \Delta_K = -20$, so $M_K = \frac{2}{\pi}\sqrt{20} \approx 2.85$.

$(2) = (2, 1+\sqrt{-5})^2 = \mathfrak{p}^2$, and $\mathfrak{p}$ is not principal because $a^2+5b^2 = 2$ has no integral solutions.

Hence $\mathfrak{p}_2$ has order 2 and $\mathrm{Cl}(K) = \mathbb{Z}/2\mathbb{Z}$ and $h_K = 2$.

Example 2: $K = \mathbb{Q}(\sqrt{-11})$.

$-11 \equiv 1 \bmod 4, \Delta_K = -11$, $M_K = \frac{2}{\pi}\sqrt{11} \approx 2.11$.

(2) is not ramified in K and $-11 \equiv 5 \bmod 8$ so (2) is inert.

Hence $\mathrm{Cl}(K) = \{e\}$ and $h_K = 1$.

Example 3: $K = \mathbb{Q}(\sqrt{-14})$.[4]

$-14 \equiv 2 \bmod 4, \Delta_K = -56$, $M_K = \frac{2}{\pi}\sqrt{56} \approx 4.76$.

$(2) = \mathfrak{p}^2$ with $\mathfrak{p} = (2, \sqrt{-14})$ and $\mathrm{N}(\mathfrak{p}) = 2$. From $a^2 + 14b^2 = 2$ has no integral solutions ,we see $\mathfrak{p}$ is not principal and order is 2; $(3) = \mathfrak{p}_3\bar{\mathfrak{p}}_3$ with $\mathfrak{p}_3 = (3, \sqrt{-14}+1)$ and $\mathfrak{p}_3$ is not principal because $a^2+14b^2 = 3$ has no integral solutions. Note that $\alpha = \sqrt{-14}+2 \in \mathcal{O}_K$ and $\mathrm{N}(\alpha) = 2\cdot 3^2$. But $\frac{\alpha}{3} \notin \mathcal{O}_K$, so we may assume $\mathfrak{p}_3 \mid (\alpha)$ and then $[\mathfrak{p}\mathfrak{p}_3^2] = [(1)]$.

Hence $\mathfrak{p}_3$ has order 4 and $\mathrm{Cl}(K) = \mathbb{Z}/4\mathbb{Z}$, $h_K = 4$.

Example 4: $K = \mathbb{Q}(\sqrt{-23})$.

$-23 \equiv 1 \bmod 4, \Delta_K = -23$, $M_K = \frac{2}{\pi}\sqrt{23} \approx 3.05$.

$(2) = (2, \frac{1+\sqrt{-23}}{2})(2, \frac{-1+\sqrt{-23}}{2}) = \mathfrak{p}\bar{\mathfrak{p}}$ and $\mathfrak{p}$ is not principal because $\frac{1}{4}(a^2+23b^2) = 2$ has no integral solutions. Let $\alpha = \frac{1}{2}(3+\sqrt{-23}) \in \mathcal{O}_K$ and $\mathrm{N}(\alpha) = 8$ implies $(\alpha) = \mathfrak{p}^3$ or $\bar{\mathfrak{p}}^3$ or $\mathfrak{p}\bar{\mathfrak{p}}^2$ or $\mathfrak{p}^2\bar{\mathfrak{p}}$. But the last two cases are impossible because $\frac{\alpha}{2} \notin \mathcal{O}_K$; $(3) = (3, \frac{1+\sqrt{-23}}{2})(3, \frac{-1+\sqrt{-23}}{2}) = \mathfrak{p}_3\bar{\mathfrak{p}}_3$ because $\left(\frac{11}{3}\right) = -1$. Note that $\beta = \frac{1}{2}(1+\sqrt{-23}) \in \mathcal{O}_K, \mathrm{N}(\beta) = 6$ implies $[\mathfrak{p}_3] = [\mathfrak{p}]$ or $[\mathfrak{p}_3] = [\mathfrak{p}]^{-1}$.

Hence $\mathrm{Cl}(K) = \langle[\mathfrak{p}]\rangle = \mathbb{Z}/3\mathbb{Z}$ and $h_K = 3$.

---

[3]That will be great for us if there always has a $\alpha \in \mathcal{O}_L$ s.t. $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Howerver, in general, this is not true. (Dedekind) Consider the irreducible polynomial $f(x) = x^3 + x^2 - 2x + 8$ and a root θ of it. For $\mathbb{Q}(\theta)$, one can show that $\Delta_K = \mathrm{disc}\{1, \theta, \frac{4}{\theta}\} = 503$ but $\mathrm{disc}\{1, \alpha, \alpha^2\}$ is even for all $\alpha \in \mathcal{O}_K$.

[4]Actually, this is the most special case when $-15 \le d \le 15$ with d squarefree, and in other cases $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))$ are either trivial (if $d = \pm1, \pm2, \pm3, 5, 6, \pm7, \pm11, 13, 14$) or $\mathbb{Z}/2\mathbb{Z}$ (if $d = -5, -6, \pm10, -13, \pm15$).

1.2 Real Quadratic Fields $K = \mathbb{Q}(\sqrt{d})$

In this case, we have $r_2 = 0, n = 2$ and $M_K = \frac{2!}{2^2}\sqrt{|\Delta_K|} = \frac{1}{2}\sqrt{|\Delta_K|}$.

Example 5: $K = \mathbb{Q}(\sqrt{10})$.

$10 \equiv 2 \bmod 4$, $\Delta_K = 40$, $M_K = \frac{1}{2}\sqrt{40} \approx 3.16$.

$(2) = (2, \sqrt{10})^2 = \mathfrak{p}^2$ and $\mathfrak{p}$ is not principal because $a^2 - 10b^2 = \pm 2$ has no integral solutions (a must be even and then mod 10); $(3) = (3, 1+\sqrt{10})(3, -1+\sqrt{10}) = \mathfrak{p}_3\bar{\mathfrak{p}}_3$ and $\alpha = 2+\sqrt{10}, \mathrm{N}(\alpha) = 6$ implies $(\alpha) = \mathfrak{p}\mathfrak{p}_3$ or $\mathfrak{p}\bar{\mathfrak{p}}_3$.

Hence $\mathrm{Cl}(K) = \langle[\mathfrak{p}]\rangle = \mathbb{Z}/2\mathbb{Z}$ and $h_K = 2$.

Example 6: $K = \mathbb{Q}(\sqrt{173})$.

$173 \equiv 1 \bmod 4$, $\Delta_K = 173$, $M_K = \frac{1}{2}\sqrt{173} \approx 6.58$.

(2) is not ramified in K and $173 \equiv 5 \bmod 8$ so (2) is inert; (3) is not ramified in K and $\left(\frac{173}{3}\right) = -1$ so (3) is inert; (5) is not ramified in K and $\left(\frac{173}{5}\right) = -1$ so (5) is inert.

Hence $\mathrm{Cl}(K) = \{e\}$ and $h_K = 1$.

1.3 Cubic Fields

Recall that $\mathrm{disc}(x^n + ax + b, \mathrm{irr}) = (-1)^{\frac{n(n-1)}{2}}\left[(-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}\right]$, and then $\mathrm{disc}(x^3 + ax + b, \mathrm{irr}) = -(4a^3 + 27b^2)$.

Example 7: $K = \mathbb{Q}(\sqrt[3]{3})$.

We have $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{3}]$, $r_2 = 1, n = 3$ and $M_K = \left(\frac{4}{\pi}\right)\frac{3!}{3^3}\sqrt{|-243|} \approx 4.41$.

$x^3 - 3 \equiv (x+1)(x^2+x+1) \bmod 2 \equiv x^3 \bmod 3$, then $(2) = \mathfrak{p}_2\mathfrak{p}_4, (3) = \mathfrak{p}_3^3$. Note that $\mathrm{N}(-1+\sqrt[3]{3}) = 2, \mathrm{N}(\sqrt[3]{3}) = 3$, then $\mathfrak{p}_2, \mathfrak{p}_3$ are all principal, so is $\mathfrak{p}_4$ (Explicitly,$\mathfrak{p}_4 = (1+\sqrt[3]{3}+\sqrt[3]{9})$).

Hence $\mathrm{Cl}(K) = \{e\}$, $h_K = 1$.

1.4 Exercises

(1) Show that for $K = \mathbb{Q}(\sqrt{-30})$, $\mathrm{Cl}(K) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $h_K = 4$.

Hint: consider $\alpha = \sqrt{-30}$*, which gives* $[\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5] = [(1)]$.

(2) Show that for $K = \mathbb{Q}(\sqrt{-65})$, $\mathrm{Cl}(K) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $h_K = 8$.

Hint: $2, 5$ *are ramified,* 7 *is inert and* 3 *splits. Consider* $a + \sqrt{-65}$*, which gives* $\mathfrak{p}_3$ *has order 4 if taking* $a = 4$ *and* $[\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_5] = [(1)]$ *if taking* $a = 5$*. Hence* $\mathrm{Cl}(K) = \langle[\mathfrak{p}_2], [\mathfrak{p}_3]\rangle$.

(3) (Gauss, 1796) Show that for $K = \mathbb{Q}(\sqrt{-d})$ with $d = 1, 2, 3, 7, 11, 19, 43, 67$ or 163, $\mathrm{Cl}(K)$ is trivial.

2 Remarks on this note

2.1 About Δ_K

The most difficult part to calculate in M_K is usually Δ_K. And there list some useful facts about Δ_K (One can use the quadratic fields to assist to memory.)

(i) If there have $\{\alpha_i\}_{i=1}^{[K:\mathbb{Q}]} \subset \mathcal{O}_K$ s.t. disc$\{\alpha_i\}$ is squarefree, then it is exactly Δ_K.

(ii) **Brill's Thm :** sgn$\Delta_K = (-1)^{r_2}$.

(iii)[5] **Stickelberger's Thm :** $\Delta_K \equiv 0$ or $1 \bmod 4$.

Generally, let $M^\vee := \{x \in L \mid xM \subset \mathcal{O}_K\}$ for a fractional ideal M of L, then the Different of L/K is denoted by $\mathrm{D}_{L/K} = (\mathcal{O}_L^\vee)^\vee \subset \mathcal{O}_L$ and the Relative Discriminant of L/K is denoted by $\Delta_{L/K} = \mathrm{N}_{L/K}(\mathrm{D}_{L/K}) \subset \mathcal{O}_K$. We have $\mathfrak{P} \subset \mathcal{O}_L$ is ramified $\iff \mathfrak{P} \mid \mathrm{D}_{L/K}$ and $\mathfrak{p} \subset \mathcal{O}_K$ is ramified $\iff \mathfrak{p} \mid \Delta_{L/K}$.

If $\alpha \in L$ s.t. $L = K(\alpha)$ and $f(x) \in K[x]$ is the minimal polynomial of α over K, then $\mathcal{O}_K[\alpha]^\vee = \frac{1}{f'(\alpha)}\mathcal{O}_K[\alpha]$ (Actually, one can show that $\left\{\frac{b_0}{f'(\alpha)}, \cdots, \frac{b_{n-1}}{f'(\alpha)}\right\}$ is the dual basis about $\mathrm{Tr}_{L/K}$ of $\{1, \alpha, \cdots, \alpha^{n-1}\}$, where $b_0 + \cdots + b_{n-1}x^{n-1} =: \frac{f(x)}{x-\alpha} \in \mathcal{O}_L[x]$), and this will be very useful to determine $\mathrm{D}_{\mathrm{L/K}}$ in many cases.

2.2 About Bound for Cl(K)

There have various bounds whose function is similar to M_K (H. Minkowski,1886)[6], and there are many improvements and optimizations for them. Here are two examples.

Kronecker bound (L. Kronecker,1882)[7] is $K_K := \prod_{j=1}^{n}(\sum_{i=1}^{n}|\sigma_j(\alpha_i)|)$ where $\{\alpha_i\}_{i=1}^n$ is an integral basis of $\mathcal{O}_K$ and $\{\sigma_j\}_{j=1}^n$ is the set of all embeddings of K into $\mathbb{C}$ and $||$ is the usual norm on $\mathbb{C}$. If one just want to prove the finiteness of ideal groups, it is much easier to use the latter as a bound; but for practical calculations, the former is obviously better, in most cases.

Bach bound (E. Bach, 1990)[8] is $B_K := 12\log^2\Delta_K$ with assuming Generalized Riemann's Hypothesis, and the bound improves up to $(4 + o(1))\log^2\Delta_K$ as Δ_K diverges, where the function in $o(1)$ is not made explicit in that paper, but has order at least $\log^{-\frac{2}{3}}\Delta_K$.

I also searched for information about the refinement work of Minkowski bound, and there are not too much. It is worth mentioning that for real quadratic field, it can be improved from $\frac{\sqrt{\Delta_K}}{2}$ to $1 + \lfloor\frac{\sqrt{\Delta_K}}{3}\rfloor$[9] and this bound is best possible for all real quadratic fields.

---

[5]One can refer to https://math.stackexchange.com/questions/394785/proof-of-stickelberger-s-theorem

[6]Minkowski, H. (Hermann). (18961910). Geometrie der Zahlen. Leipzig: B.G. Teubner.

[7]Kronecker, L. (1882). Grundzüge einer arithmetischen Theorie der algebraischen Größen. Journal für die reine und angewandte Mathematik, 92, 1–122.

[8]Eric Bach, Explicit bounds for primality testing and related problems, Math. Comp. 55 (1990), no. 191, 355–380.

[9]Srinivasan, A. (2011). An improvement of the Minkowski bound for real quadratic orders using the Markoff theorem.

2.3 About h_K of quadratic fields

Here is a table for reference:

Table 1: $h_{\mathbb{Q}(\sqrt{d})}$ with squarefree $-30 < d < 30$

d	1	2	3	5	6	7	10	11	13
h	1	1	1	1	1	1	2	1	1
d	14	15	17	19	21	22	23	26	29
h	1	2	1	1	1	1	1	2	1
d	-1	-2	-3	-5	-6	-7	-10	-11	-13
h	1	1	1	2	2	1	2	1	2
d	-14	-15	-17	-19	-21	-22	-23	-26	-29
h	4	2	4	1	4	2	3	6	6

When $0 < d < 101$ and $K = \mathbb{Q}(\sqrt{d})$, the class number h_K is almost 1 with few exceptions: $d = 10, 15, 26, 30, 34, 35, 39, 55, 58, 65, 66, 70, 74, 78, 85, 87, 91, 95$ (in these cases $h_K = 2$), $d = 79$ ($h_K = 3$) and $d = 82$ ($h_K = 4$).

For the class number of quadratic field , Gauss has two famous conjectures:

(i) class-number one problem for complex quadratic fields: $\#\{d \mid d < 0, h_{\mathbb{Q}\sqrt{d}} = 1\} < \infty$;

(ii) class-number one problem for real quadratic fields: $\#\{d \mid d > 0, h_{\mathbb{Q}\sqrt{d}} = 1\} = \infty$

in 1934, Heilbronn and Linfoot (1934) [10] proved the Gauss Conjecture (i), which says there is at most one imaginary quadratic field whose $h_K = 1$ if $d < -163$.[11]

Interestingly, Heilbronn's proof followed a remarkable work of Deuring[12] who proved that if there were infinitely many class-number one complex quadratic fields, then the Riemann Hypothesis would follow! Many authors promptly carried this over to other class-numbers, but Heilbronn realized that Deuring's method would allow one to prove the Generalized Riemann Hypothesis (GRH). Combining with Landau's earlier result which showed that GRH could deduce (i) , He proved (i). The interesting thing is that GRH is used as a springboard to complete the proof:

$$\text{(i) fails.} \overset{\text{Heilbronn}}{\Longrightarrow} \text{GRH} \overset{\text{Landau}}{\Longrightarrow} \text{(i) holds.}$$

Journal of Number Theory, 131(8), 1420–1428.

[10] H. Heilbronn, E. Linfoot, On the imaginary quadratic corpora of class-number one. Quart. J. Math. Oxford Ser. 5 (1934), pp. 293–301.

[11] Until 1967, the exceptional number field was independently proven by Baker and Stark to be non-existent, which means that there are only nine imaginary quadratic fields with class number one given by Gauss.

[12] M. Deuring – "Imaginäre quadratische Zahlkörper mit der Klassenzahl 1" , Math. Z. 37 (1933), no. 1, p. 405–415.

Also in 1934, Heilbronn[13] prove a more general theorem which says $\lim\limits_{d\to+\infty} h_{\mathbb{Q}\sqrt{-d}} = \infty$.

The problem of the class number of real quadratic field is more difficult because the fundamental units are difficult to calculate. Hua Luogeng proved that $h_{\mathbb{Q}\sqrt{d},d>0} < \sqrt{d}$ and this is essentially the best outcome.

2.4 About $x^3 - 5 = y^2$

This is the starting point of our course, and now I give a proof of this equation has no integer solutions.

Suppose there exists a solution (x, y), then $x \equiv 1 \bmod 4$ and y is even by considering mod 4. If $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are not relatively prime ideals then they are both divisible by some prime ideal $\mathfrak{p}$. Then $\mathfrak{p} \mid (2\sqrt{-5})$, $\mathrm{N}(\mathfrak{p}) \mid 20$ and $\mathrm{N}(\mathfrak{p}) \mid \mathrm{N}((y + \sqrt{-5})) = y^2 + 5$ imply $\mathrm{N}(\mathfrak{p}) = 5$. So $5 \mid y^2 + 5, 5 \mid y$, whus $x^3 \equiv 5 \bmod 25$ which is impossible. Hence $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are relatively prime ideals. By $h_{\mathbb{Q}(\sqrt{-5})} = 2$, one can get $(y+\sqrt{-5}) = \mathfrak{a}^3$, $(y-\sqrt{-5}) = \mathfrak{b}^3$ and $\mathfrak{a}, \mathfrak{b}$ are principal ideals. Because $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$, so we can assume $y + \sqrt{-5} = (m + n\sqrt{-5})^3$ for some integers m and n. Then $y = m(m^2 - 15n^2)$ and $1 = n(3m^2 - 5n^2)$, which is a contridiction.

The key point in this approach to $y^2 = x^3 - 5$ is not so much that $h_{\mathbb{Q}(\sqrt{-5})} = 2$ but rather that $\gcd(h_{\mathbb{Q}(\sqrt{-5})}, 3) = 1$. More generally, finding the integral solutions to $y^2 = x^3 + k$ when $\gcd(h_{\mathbb{Q}(\sqrt{k})}, 3) = 1$ proceeds "as if" the ideal class group were trivial.

Finally, it is worth adding that $y^2 = x^3 + n$ is usually called Mordell equation, and one can find the n values for which this equation has no integer solutions on oeis.org/A081121 (such as $n = 6, 7, 11, 13, \cdots$) and oeis.org/A081121 (such as $n = -3, -5, -6, -9, \cdots$), or just search for *Mordell equation* on https://oeis.org/.

[13] H. Heilbronn– "On the class-number in imaginary quadratic fields", Quart. J. Math. Oxford Ser. 5 (1934), p. 150–160.