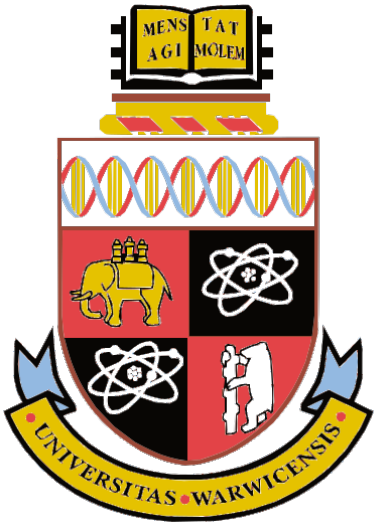


Discriminant Bounds and Class Numbers

by

Elvira Lupoian

MA4K8 Scholarly Report

Submitted to The University of Warwick

Mathematics Institute

April, 2020

Contents

Introduction

This dissertation will present some general results on the class number and ideal class group of a number field, which will be applied to class numbers of layers of cyclotomic $\mathbb{Z}_p$-extensions in the last section of this report. The first section will give a series of results which bound the class number. We will pay close attention to the results of Odlyzko [13], who uses bounds on the discriminant of a number field to bound the class number. In addition, we will also look at Miller's [7] for more advanced methods of bounding the class number.

In Section 2, we will present some of Masley's general results [6] on the class numbers of extensions of number fields. These results are described in detail and their proofs are further explained using additional results.

In Section 3, we will focus on the class number of layers of $\mathbb{Z}_p$-extensions. An overview of $\mathbb{Z}_p$-extensions will be provided, followed by more recent results and a description of how results from the previous two sections may be used to calculate the class number of layers of the cyclotomic $\mathbb{Z}_p$-extension of the rationals. The following theorem will be the main results of this section.

Theorem 0.1. *(Miller) The fields* $\mathbb{B}_{13,1}$,$\mathbb{B}_{17,1}$ *and* $\mathbb{B}_{19,1}$ *have class number 1.*

Here, $\mathbb{B}_{p,n}$ denotes the nth layer of the cyclotomic $\mathbb{Z}_p$-extension of the rationals.

1 Class Number Bounds

There are various approaches to bounding the class numbers and this section will focus on the work of Odlyzko [13], Masley [6] and Miller [7].

In [13], Odlyzko derived bounds for the absolute value of the discriminant of a number field and used this result to bound the class number. Although the results of [13] are not as good as other estimates derived by Odlyzko for number fields of large degree (over $\mathbb{Q}$), they are easy to prove and applicable to number fields of small degrees.

Masley used the results of Odlyzko to define class number bound functions, which he used to bound the class number of fields with small root discriminant.

In [7], Miller uses some of his more complex, analytically derived bounds on class numbers of fields with larger root discriminant. The results of Miller will not be proved, but we will focus on their applications.

Odlyzko's main results

Let K be an algebraic number field of degree n, with r_1 real and $2r_2$ complex embeddings. Denote by $D = D_K$ the absolute value of the discriminant of K.

In his paper [13], Odlyzko obtained some very simple, but rather powerful estimates for

D.
Define

$$\psi(s) = \frac{\Gamma'}{\Gamma}(s)$$
$$Z(s) = -\frac{\zeta_K'}{\zeta_K}(s)$$
$$Z_1(s) = -\frac{d}{ds}(Z(s))$$

where $\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx$ is the usual Gamma function defined for all s with $Re(s) > 0$ and $\zeta_K(s) = \sum_I \frac{1}{(N(I))^s}$ denotes the Dedekind zeta function defined for all s with $Re(s) > 1$, the sum runs through all the non-zero ideals I of O_K (N is the usual ideal norm).

Note. Equivalently, ζ_K is defined by the Euler product

$$\zeta_K(s) = \prod_P \frac{1}{1 - N(P)^{-s}}$$

where P runs through the non-zero prime ideal of O_K. Taking logarithm and differentiating, it is clear that

$$Z(s) = \sum_P \frac{\log(N(P))}{N(P)^s - 1}$$

where P runs through the non-zero prime ideals of O_K.
Thus $Z(\sigma) > 0$ for $\sigma > 1$.A similar calculation shows $Z_1(\sigma) > 0$ for $\sigma > 1$.

In his paper [13], Odlyzko obtained some very simple, but rather powerful estimates for D.

Theorem 1.1. *(Discriminant bound) Let $\sigma > 1$, and $\tilde{\sigma}$ satisfying $\tilde{\sigma} \geq \frac{5+\sqrt{12\sigma^2-5}}{6}$ and $\tilde{\sigma} \geq 1 + \alpha\sigma$, where $\alpha = \sqrt{\frac{14-\sqrt{128}}{34}} < 0.3$ is a constant. Then:*

$$\begin{aligned} log(D) \geq\ & r_1\left(log(\pi) - \psi\left(\tfrac{\sigma}{2}\right)\right) + 2r_2(\log(2\pi) - \psi(\sigma)) \\ & + (2\sigma - 1)\left(\tfrac{r_1}{4}\psi'\left(\tfrac{\tilde{\sigma}}{2}\right) + r_2\psi'(\tilde{\sigma})\right) + 2Z(\sigma) \\ & + (2\sigma - 1)Z_1(\tilde{\sigma}) - \tfrac{2}{\sigma} - \tfrac{2}{\sigma-1} - \tfrac{2\sigma-1}{\tilde{\sigma}^2} - \tfrac{2\sigma-1}{(\tilde{\sigma}-1)^2} \end{aligned}$$

Note. By assuming the Generalized Riemann Hypothesis, Odlyzko showed that the same bound can be obtained with the less strict conditions on σ and $\tilde{\sigma}$

$$\sigma > 1,\ \tilde{\sigma} > 1 \text{ and } \sigma \leqslant \tfrac{1}{2} + \sqrt{3}(\tilde{\sigma} - \tfrac{1}{2})$$

We will follow Section 3 of [13] to prove Theorem 1.1. Odlyzko starts with the following relation obtained by Stark in [15].

$$\begin{aligned} log(D) =& r_1\left(\log(\pi) - \psi\left(\frac{s}{2}\right)\right) + 2r_2(\log(2\pi) + \psi(s)) + \\ & 2Z(s) + 2{\sum_\rho}' \frac{1}{s-\rho} - \frac{2}{s} - \frac{2}{s-1} \end{aligned} \tag{1}$$

and this holds for all $s \in \mathbb{C}$, where ρ runs through all the non-trivial zeros of ζ_K and $\sum'$ indicates ρ and $\bar{\rho}$ terms are to be summed together.
Note. A zero $\rho = \beta + i\gamma$ of ζ_K is non-trivial if $0 < \beta < \frac{1}{2}$.

Taking $s = \sigma > 1$ in the above gives

$$\begin{aligned} log\,(D) =& r_1 \left(log\,(\pi) - \psi\left(\frac{\sigma}{2}\right)\right) + 2r_2\,(log(2\pi) + \psi(\sigma)) + 2Z\,(\sigma) + \\ & 2\sum_{\rho} Re\left(\frac{1}{\sigma - \rho}\right) - \frac{2}{\sigma} - \frac{2}{\sigma - 1} \end{aligned} \tag{2}$$

The main idea of the proof is to obtain an estimate for the sum over the zeros of ζ_K, which is independent of the discriminant.
Differentiating (1) and setting $s = \tilde{\sigma} > 1$ gives

$$2\sum_{\rho} Re\frac{-1}{(\tilde{\sigma} - \rho)^2} = \frac{r_1}{2}\psi'\left(\frac{\tilde{\sigma}}{2}\right) + 2r_2\psi'(\tilde{\sigma}) + 2Z_1\,(\tilde{\sigma}) - \frac{2}{\tilde{\sigma}^2} - \frac{2}{(\tilde{\sigma} - \rho)^2} \tag{3}$$

Using (2) and (3), proving Theorem 1.1 reduces to showing

$$2\sum_{\rho} Re\frac{1}{\sigma - \rho} \geq (2\sigma - 1)\sum_{\rho} Re\frac{-1}{(\tilde{\sigma} - \rho)^2} \tag{4}$$

subject to the conditions of Theorem 1.1.
The following elementary results are used in the proof.
Lemma 1.2. *Let $\sigma > 1$, $\tilde{\sigma} > 1$. If $\sigma \leq \frac{1}{2} + \sqrt{3}(\tilde{\sigma} - \frac{1}{2})$ then*

$$2\frac{\sigma - \frac{1}{2}}{(\sigma - \frac{1}{2})^2 + y^2} \geq (2\sigma - 1)\frac{y^2 - (\tilde{\sigma} - \frac{1}{2})^2}{(y^2 + (\tilde{\sigma} - \frac{1}{2})^2)^2} \tag{5}$$

for all $y \in \mathbb{R}$

Proof. Observe that $2\sigma - 1 > 0$ and thus proving (5) reduces to proving

$$\frac{1}{(\sigma - \frac{1}{2})^2 + y^2} \geq \frac{y^2 - (\tilde{\sigma}^2 - \frac{1}{2})^2}{(y^2 + (\tilde{\sigma} - \frac{1}{2})^2)^2}$$

multiplying both sides by the respective denominators (since they are positive), expanding and rearranging, the above is equivalent to

$$\left(3\left(\tilde{\sigma} - \frac{1}{2}\right)^2 - \left(\sigma - \frac{1}{2}\right)^2\right)y^2 + \left(\tilde{\sigma} - \frac{1}{2}\right)^2\left[\left(\tilde{\sigma} - \frac{1}{2}\right)^2 + \left(\sigma - \frac{1}{2}\right)^2\right] \geq 0$$

By our choice of σ,$\tilde{\sigma}$: $\left(3\left(\tilde{\sigma} - \frac{1}{2}\right)^2 - \left(\sigma - \frac{1}{2}\right)^2\right) \geq 0$, and as $y, \sigma, \tilde{\sigma} \in \mathbb{R}$: y^2, $\left(\tilde{\sigma} - \frac{1}{2}\right)^2$ and $\left(\sigma - \frac{1}{2}\right)^2$ are also positive. Thus the inequality follows under the assumptions of our

hypothesis. □

Lemma 1.3. *Let* $\sigma > 1$, $\tilde{\sigma} \geq \frac{5}{6} + \frac{1}{6}\sqrt{12\tilde{\sigma} - 5}$ *and* $\tilde{\sigma} \geq 1 + \alpha\sigma$ *where* $\alpha = \sqrt{\frac{14-\sqrt{128}}{34}} < 0.3$. *Then*

$$\frac{\sigma - x}{(\sigma - x)^2 + y^2} + \frac{\sigma - 1 + x}{(\sigma - 1 + x)^2 + y^2} \geq \left(\sigma - \frac{1}{2}\right) \left\{ \frac{y^2 - (\tilde{\sigma} - x)^2}{\left[y^2 + (\tilde{\sigma} - x)^2\right]^2} + \frac{y^2 - (\tilde{\sigma} - 1 + x)^2}{\left[y^2 + (\tilde{\sigma} - 1 + x)^2\right]^2} \right\} \tag{6}$$

for all real x, $0 \leq x \leq 1$ *and real* y.

Proof. Observe that both side of (6) are invariant under the transformations $x \mapsto 1 - x$ and $y \mapsto -y$, and so it is sufficient to prove the inequality for $\frac{1}{2} \leq x \leq 1$ and $y \geq 0$. If $\frac{1}{2} \leq x \leq 1$

$$\frac{\sigma - x}{(\sigma - x)^2 + y^2} + \frac{\sigma - 1 + x}{(\sigma - 1 + x)^2 + y^2} \geq \frac{2\left(\sigma - \frac{1}{2}\right)}{(\sigma - 1 + x)^2 + y^2}$$

and so it suffices to prove that

$$\frac{2}{(\sigma - 1 + x)^2 + y^2} \geq \frac{y^2 - (\tilde{\sigma} - x)^2}{\left[y^2 + (\tilde{\sigma} - x)^2\right]^2} + \frac{y^2 - (\tilde{\sigma} - 1 + x)^2}{\left[y^2 + (\tilde{\sigma} - 1 + x)^2\right]^2} \tag{7}$$

for all $\frac{1}{2} \leq x \leq 1$ and $y \geq 0$.
Observe that for $y \leq \tilde{\sigma} - x$, both summands on the right hand side of (7) are non positive, so the inequality holds trivially.
Suppose $y \geq \tilde{\sigma} - 1 + x$. Then

$$\frac{y^2 - (\tilde{\sigma} - x)^2}{\left[y^2 + (\tilde{\sigma} - x)^2\right]^2} + \frac{y^2 - (\tilde{\sigma} - 1 + x)^2}{\left[y^2 + (\tilde{\sigma} - 1 + x)^2\right]^2} \leq \frac{2y^2 - (\tilde{\sigma} - x)^2 - (\tilde{\sigma} - 1 + x)^2}{\left[y^2 + (\tilde{\sigma} - x)^2\right]^2}$$

and

$$\frac{2}{(\sigma - 1 + x)^2 + y^2} - \frac{2y^2 - (\tilde{\sigma} - x)^2 - (\tilde{\sigma} - 1 + x)^2}{[y^2 + (\tilde{\sigma} - x)^2]^2} = \frac{F(x, y, \sigma, \tilde{\sigma})}{[(\sigma - 1 + x)^2 + y^2][y^2 + (\tilde{\sigma} - x)^2]^2} \tag{8}$$

where

$$F(x, y, \sigma, \tilde{\sigma}) = 5y^2(\tilde{\sigma} - x)^2 + 2(\tilde{\sigma} - x)^4 - 2y^2(\sigma - 1 + x)^2 + (\tilde{\sigma} - x)^2(\sigma - 1 + x)^2 + (\tilde{\sigma} - 1 + x)^2(\sigma - 1 + x)^2 + y^2(\tilde{\sigma} - 1 + x)^2$$

For $y \geq \tilde{\sigma} - 1 + x$

$$F(x, y, \sigma, \tilde{\sigma}) \geq y^2[5(\tilde{\sigma} - x)^2 + (\tilde{\sigma} - 1 + x)^2 - 2(\sigma - 1 + x)^2]$$

The derivative of $f(x) = 5(\tilde{\sigma} - x)^2 + (\tilde{\sigma} - 1 + x)^2 - 2(\sigma - 1 + x)^2$ is non-positive for $\frac{1}{2} \leq x \leq 1$, and so

$$f(x) \geq f(1) = 5(\tilde{\sigma} - 1)^2 + \tilde{\sigma}^2 - 2\sigma^2$$

Since $\tilde{\sigma} \geq \frac{5}{6} + \frac{1}{6}\sqrt{12\sigma^2 - 5}$

$$\begin{aligned} 5(\tilde{\sigma} - 1)^2 + \tilde{\sigma}^2 - 2\sigma^2 &\geq 6(12\sigma^2 - 5) + 30 - 2\sigma^2 \\ &= 70\sigma^2 \end{aligned}$$

and $70\sigma^2$ is non-negative as $\sigma \in \mathbb{R}$.
Hence (8) is non-negative for $y \geq \tilde{\sigma} - 1 + x$ and the lemma holds in this case.
Suppose $\tilde{\sigma} - x < y < \tilde{\sigma} - 1 + x$.
The second summand in the right hand side of (7) is negative, so it suffices to prove

$$\frac{2}{(\sigma - 1 + x)^2 + y^2} \geq \frac{y^2 - (\tilde{\sigma} - x)^2}{[y^2 + (\tilde{\sigma} - x)^2]^2}$$

Consider

$$\frac{2}{(\sigma - 1 + x)^2 + y^2} - \frac{y^2 - (\tilde{\sigma} - x)^2}{[y^2 + (\tilde{\sigma} - x)^2]^2} = \frac{G(x, y, \sigma, \tilde{\sigma})}{((\sigma - 1 + x)^2 + y^2)[y^2 + (\tilde{\sigma} - x)^2]^2}$$

where

$$G(x, y, \sigma, \tilde{\sigma}) = y^4 - y^2((\sigma - 1 + x)^2 - 5(\tilde{\sigma} - x)^2) + (\tilde{\sigma} - x)^2(\sigma - 1 + x)^2 + 2(\tilde{\sigma} - x)^4 \quad (9)$$

Note that $(\sigma - 1 + x)^2 - 5(\tilde{\sigma} - x)^2 \geq 0$ implies

$$(\tilde{\sigma} - x)^2 \leq \tfrac{1}{5}(\sigma - 1 + x)^2 \leq \alpha(\sigma - 1 + x)^2$$

and this contradicts our initial assumption.
Therefore all summands of (9) are positive, and so subject to our assumptions $G(x, y, \sigma, \tilde{\sigma}) \geq 0$, proving the remaining case of the lemma. □

Proof. (of Theorem 1.1) Recall that under our hypothesis, Theorem 1.1 follows from (4). If $\rho = \beta + i\gamma$ is a non-trivial zero then so is $1 - \beta + i\gamma$, and so we can group the ρ and

$1-\bar{\rho}$ terms in (4), to obtain the equivalent inequality

$$\sum_{\rho} Re\left\{\frac{1}{\sigma-\beta-i\gamma}+\frac{1}{\sigma-1+\beta-i\gamma}\right\} \geq$$
$$\left(\sigma-\frac{1}{2}\right)\sum_{\rho} Re\left\{\frac{-1}{(\tilde{\sigma}-\beta-i\gamma)^2}+\frac{-1}{(\tilde{\sigma}-1+\beta-i\gamma)^2}\right\}$$

To prove (4) it will suffice to show that for all non-trivial zeros $\rho=\beta+i\gamma$

$$\begin{aligned}\frac{\sigma-\beta}{(\sigma-\beta)^2+\gamma^2}+\frac{\sigma-1+\beta}{(\sigma-1+\beta)^2+\gamma^2} \geq \\ \left(\sigma-\frac{1}{2}\right)\left\{\frac{\gamma^2-(\tilde{\sigma}-\beta)^2}{(\gamma^2+(\tilde{\sigma}-\beta)^2)^2}+\frac{\gamma^2-(\tilde{\sigma}-1+\beta)^2}{(\gamma^2+(\tilde{\sigma}-1+\beta)^2)^2}\right\}\end{aligned} \tag{10}$$

This follows from Lemma (6) when $\tilde{\sigma} \geq 1+\alpha\sigma$ and $\tilde{\sigma} \geq \frac{5}{6}+\frac{1}{6}\sqrt{12\sigma^2-5}$.
This completes the proof of Theorem 1.1. □

Note. If we assume the GRH for ζ_K, then all the non-trivial zeros of ζ_K are of the form $\rho=\frac{1}{2}+i\gamma$.
Then for any σ and $\tilde{\sigma}$, the inequality (4) will clearly follow if we can show that

$$2Re\left(\tfrac{1}{\sigma-\rho}\right) \geq (2\sigma-1)\,Re\left(\tfrac{-1}{(\tilde{\sigma}-\rho)^2}\right)$$

for all non-trivial zeros ρ

$$Re\left(\tfrac{1}{\sigma-\rho}\right)=\tfrac{\sigma-\frac{1}{2}}{(\sigma-\frac{1}{2})^2+\gamma^2}$$
$$Re\left(\tfrac{-1}{(\tilde{\sigma}-\rho)^2}\right)=\tfrac{\gamma^2-(\tilde{\sigma}-\frac{1}{2})^2}{((\tilde{\sigma}-\frac{1}{2})^2+\gamma^2)^2}$$

Therefore one can apply (5) directly and deduce that if $\sigma \leq \frac{1}{2}+\sqrt{3}(\tilde{\sigma}-\frac{1}{2})$, then

$$2Re\left(\tfrac{1}{\sigma-\rho}\right) \geq (2\sigma-1)\,Re\left(\tfrac{-1}{(\tilde{\sigma}-\rho)^2}\right)$$

holds for any non-trivial zero ρ.

There are various ways of using the bound given in Theorem 1.1.
I will proceed with calculating the simplest possible bound, obtained from some basic estimates.
Remark. Recall that $Z(\sigma)>0$ and $Z_1(\sigma)>0$. No lower bound for $Z(\sigma)$ and $Z_1(\sigma)$ which are valid in the general is known, and in the simplest case their contribution to the bound in Theorem 1.1 can be disregarded.

Observe that the best estimate for large values of n is obtained when σ is close to 1. Taking $\sigma=1+\frac{1}{\sqrt{n}}$ and $\tilde{\sigma}=1+\alpha\sigma$, one can use elementary facts about the gamma function to show

$$\psi\left(\tfrac{\sigma}{2}\right) \longrightarrow -\gamma-2\log 2$$
$$\psi\left(\sigma\right) \longrightarrow -\gamma$$

$$\psi'\left(\tfrac{\sigma}{2}\right) \longrightarrow 2.714$$
$$\psi'(\sigma) \longrightarrow 1.329$$

as $n \to \infty$.
Using this with the inequality of Theorem 1.1 gives

$$\begin{aligned}\log D \geq\ & r_1(\log\pi + \gamma + 2\log 2\ ) + 2r_2(\log 2\pi + \gamma\ ) \\ & + (2\sigma - 1\ )\left(\frac{r_1}{4}2.714 + r_2 1.329\ \right) - \frac{2}{\sigma} - \frac{2}{\sigma - 1} \\ & + \frac{2\sigma - 1}{\tilde{\sigma}^2} - \frac{2\sigma - 1}{(\tilde{\sigma} - 1)^2}\end{aligned} \tag{11}$$

Since $2\sigma - 1 \geq 1$

$$\begin{aligned}D &\geq \left(\pi \exp\left(\gamma + 2\log 2 + \frac{2.714}{4}\right)\right)^{r_1}\left(2\pi \exp\left(\gamma + \frac{1.329}{2}\right)\right)^{2r_2} + O(1) \\ &= (\ 44.112)^{r_1}(\ 21.749)^{2r_2} + O(1)\end{aligned} \tag{12}$$

Taking nth root of both sides, the basic estimate is obtained

$$\boxed{D^{1/n} \geq (44.112)^{\frac{r_1}{n}}(21.749)^{\frac{2r_2}{n}} + O(1)} \tag{13}$$

Remark. The other estimate of $D^{1/n}$ can be derived by defining $\tilde{\sigma}$ as a function of σ, and taking $\tilde{\sigma}$ to be the smallest possible value which satisfies the hypothesis of Theorem 1.1. This value of $\tilde{\sigma}$ can be used to find σ, and then the inequality given in Theorem 1.1 can be used to bound $D^{1/n}$.
This is one of the methods used by Odlyzko, alongside other results of Stark, to construct tables presenting close to optimal values of σ, and the resulting estimates of $D^{1/n}$ for several degrees. These tables can be found in [13].

The main application of Odlyzko's bounds of $D^{1/n}$ is to class numbers of complex quadratic extensions of totally real fields.
Prior to Odlyzko, Stark proved a number of results which showed that for any fixed $m > 2$ and $h \geq 1$, there exist only finitely many totally complex number fields K of degree $2m$, $h(K) = h$ and such that K contains a totally real subfield of index 2. Moreover, he showed that all such fields can be determined effectively.
Stark conjectured that even more is true, namely that for any $h \geq 1$, there exist only finitely many totally complex fields K of all degree with $h(K) = h$, which contain totally real subfields of index 2. This conjectured results was proved by Odlyzko by combining Theorem 1.1 and some of the previous results of Stark.
Notation. Denote by $\mathcal{N}$ the set of number fields k for which there exists a sequence of fields $\mathbb{Q} = k_0 \subseteq k_1 \subseteq ... \subseteq k_l = k$, each extensions normal over the preceding one.

Theorem 1.4. *(Odlyzko) There exist effectively computable positive constants c and δ*

such that if K is a totally complex number field of degree $2m$ containing a totally real subfield k of degree m then

$$h(K) > c[mg(m)]^{-1}(1+\delta)^m \tag{14}$$

where $g(m) = 1$ if $k \in \mathcal{N}$ and $g(m) = m!$ if $k \notin \mathcal{N}$.
Moreover, if the Generalized Riemann Hypothesis holds for k, then we may replace $g(m) = m!$ by $g(m) = m$ when $k \notin \mathcal{N}$.

This theorem shows that for each h there is an effectively computable bound $m_0(h)$ such that if K is a totally complex number filed of degree $2m$, with $h(K) = h$, which contains a totally real subfield k with $|K : k| = 2$ and $k \in \mathcal{N}$, then $m \leq m_0(h)$. Moreover, if the General Riemann Hypothesis holds for k, then the requirement $k \in \mathcal{N}$ can be discarded.

In particular, this proves Stark's conjecture under the assumption of the General Riemann Hypothesis, since for each fixed $m \leq m_0(h)$, there are only finitely many fields to consider by Stark's results.
If we do not assume the GRH, then we can still say that there are only finitely many totally complex number fields K with $h(K) = h$, which contain totally real subfields $k \in \mathcal{N}$ with $|K : k| = 2$.

To prove Theorem 1.4 we will follow Section 4 of [13]. Odlyzko's proof relies heavily on previous results of Stark, which can be found in [15].

Let K denote a totally complex number field of degree $2n$ and k a totally real subfield of K of degree n.
Define

$$g(n) = \begin{cases} 1 & \text{if } k \in \mathcal{N} \\ n & \text{assuming GRH and } k \notin \mathcal{N} \\ n! & \text{without assuming GRH and with } k \notin \mathcal{N} \end{cases}$$

For the rest of this subsection C_i, $I \in \mathbb{N}$ will denote effectively computable positive constants.

Odlyzko's proof uses the following bound of $h(K)$, which can be derived from a number of results of Stark (details can be found in [13] and [15]).

$$\boxed{h((K) \geq \frac{C_1}{ng(n)} f^{\frac{1}{2}-\frac{1}{2n}} \frac{D_k^{\frac{1}{2}-\frac{1}{2}(\sigma_1-1)\frac{1}{n}}}{\zeta_k(\sigma_1)(2\pi)^n}} \tag{15}$$

for $\sigma_0 \leq \sigma_1 \leq 2$, $\sigma_0 = 1 + [4\log(D_K)]^{-1}$.

Note. Using the relative class number formula $D_K = D_k^2 f$, for some positive integer $f = N(d(K/k))$ (see [1, p.79] for details).

To obtain a non-trivial result, we need to estimate the factor

$$\frac{D_k^{\frac{1}{2}-\frac{1}{2}(\sigma_1-1)\frac{1}{n}}}{\zeta_k(\sigma_1)(2\pi)^n}$$

The basic idea of the proof is to use Theorem 1.1 to bound this factor from below, with $Z(\sigma)$ term cancelling out the ζ_k and ψ, ψ' terms cancelling the 2π.
The proof will require the following auxiliary results.

Lemma 1.5. *There exists a constant $C_2 > 0$ such that for $\sigma > 1$*

$$Z(\sigma) \geq \log(\zeta_k(\sigma)) - C_2(\sigma - 1)n$$

Proof. If $x \geq 3$ and $\sigma > 1$

$$\frac{\log x}{x^\sigma - 1} = \sum_{r \geq 1} (\log x) x^{-r\sigma} \geq \sum r \geq 1 \frac{1}{r} x^{-r\sigma} = \log(1 - x^{-\sigma})^{-1}$$

and

$$\frac{\log 2}{2^\sigma - 1} \geq \log(1 - 2^{-\sigma})^{-1} - C_2(\sigma - 1)$$

hence for $\sigma > 1$

$$\begin{aligned} Z(\sigma) &= \sum P \frac{\log N(P)}{N(P)^\sigma - 1} \\ &\geq \sum P \log(1 - N(P)^{-\sigma})^{-1} - C_2(\sigma - 1)n \\ &= \log(\zeta_k(\sigma) - C_2(\sigma - 1)n \end{aligned}$$

□

Lemma 1.6. *There exist constants C_3 and C_4 such that for $1 < \sigma < \sigma' \leq 1 + C_4^{-1}$*

$$Z(\sigma) \geq (1 + (1 + C_3^{-1})(\sigma' - \sigma))Z(\sigma')$$

Proof. For $x \geq 3$ and $1 < \sigma < \sigma' \leq 2$

$$\log\left(\frac{x^{\sigma'} - 1}{x^\sigma - 1}\right) = \log x \int_\sigma^{\sigma'} \frac{x^u}{x^u - 1} du \geq \log(x)(\sigma' - \sigma)$$

and

$$\log\left(\frac{2^{\sigma'} - 1}{2^\sigma - 1}\right) = \int_{\sigma'}^{\sigma} \frac{2^u \log 2}{2^u - 1} du \geq 2^\sigma \ \log 2 \ \frac{\sigma' - \sigma}{2^{\sigma'} - 1} \tag{16}$$

so it follows that there exist positive constants C_3,C_4 such that

$$\frac{1}{N(P)^{\sigma}-1} \geq (1+(1+C_3^{-1})(\sigma'-\sigma))\frac{1}{N(P)^{\sigma'}-1} \tag{17}$$

for $1<\sigma<\sigma' \leq 1+C_4^{-1}$.
The lemma follows from the definition of $Z(\sigma)$. □

We now proceed with the proof of Theorem 1.4.

Proof. (of Theorem 1.4) As $C_3>0$ in (17), there exists C_5, C_6, C_7 such that

$$\left[1-(\sigma_1-1)\frac{2}{n}\right](1+(1+C_3^{-1})(\sigma_1-\sigma)) \geq 1 \tag{18}$$

for $1<\sigma<\sigma_1 \leq 1+C_5^{-1}$, $\sigma \leq 1+C_6^{-1}(\sigma_1-1)$ and $n \geq C_7(\sigma_1-1)^{-1}$.
Applying theorem (1.1) to estimate D_K with $\tilde{\sigma}=1+\alpha\sigma$ (which satisfies the required conditions for $\tilde{\sigma}$ for $\sigma-1$ sufficiently small). Thus

$$\begin{aligned}\log D_k^{\frac{1}{2}-\frac{1}{2}(\sigma_1-1)-\frac{1}{n}} \geq \frac{n}{2}\left(\log\pi-\psi\left(\frac{1}{2}\right)\right)+\frac{n}{8}\psi'\left(\frac{1+\alpha}{2}\right)-C_8(\sigma_1-1)n \\ -C_9(\sigma-1)^{-1}+Z(\sigma)\left[1-(\sigma_1-1)-\frac{2}{n}\right]\end{aligned} \tag{19}$$

for $1<\sigma<\sigma_1 \leq 1+C_{10}^{-1}$.
Using lemma 1.5 and (18)

$$Z(\sigma)\left[1-(\sigma_1-1)-\frac{2}{n}\right] \geq \log\zeta_k(\sigma_1)-C_2(\sigma_1-1)n$$

for $1<\sigma<\sigma_1 \leq 1+C_5^{-1}$, $\sigma \leq 1+C_6^{-1}(\sigma_1-1)$ and $n \geq C_7(\sigma_1-1)^{-1}$.
Combining these inequalities with (15)

$$h(K) \geq \frac{C_1}{ng(n)} f^{\frac{1}{2}-\frac{1}{2n}} exp(-C_{11}(\sigma_1-1)n-C_9(\sigma-1)^{-1})\left(\frac{50}{2\pi}\right)^{\frac{n}{2}}$$

for $1<\sigma<\sigma_1 \leq 1+C_5^{-1}$, $\sigma \leq 1+C_6^{-1}(\sigma_1-1)$, $n \geq C_7(\sigma_1-1)^{-1}$ and $\sigma_0 \leq \sigma_1$
It's sufficient to choose σ, σ_1 satisfying: $1<\sigma<\sigma_1 \leq 1+C_5^{-1}$, $\sigma \leq 1+C_6^{-1}(\sigma_1-1)$ and in this case

$$\exp\left(-C_{11}(\sigma_1-1)n-C_9(\sigma-1)^{-1}\right)\left(\frac{50}{2\pi}\right)^{\frac{n}{2}} \geq C_{12}^{-1}(1+C_{13}^{-1})^n$$

Taking n large enough with $n \geq C_7(\sigma_1-1)^{-1}$ and $\sigma_0 \leq \sigma_1$, gives

$$h(K) \geq \frac{C_1 C_{12}^{-1}}{ng(n)} f^{\frac{1}{2}-\frac{1}{2n}}(1+C_{13}^{-1})^n$$

which proves the theorem. □

Masley's application of Odlyzko's discriminant bounds

There is a more simplistic application of Theorem 1.1 by Masley in [6]. Masley used Odlyzko's results in his development of the theory of the root-discriminant and illustrated its application to class number problems.

Definition. Let K denote a number field of degree n over $\mathbb{Q}$. Let $d(K)$ denote its discriminant. The root discriminant $rd(K)$ of K is defined to be

$$rd(K) = |d(K)|^{\frac{1}{n}}$$

Proposition 1.7. *Let L/K be an extension of number fields. Then*

$$rd(K) \leq rd(L)$$

with equality if and only if L/K is unramified at all finite primes.

Proof. The discriminants of K and L are related by the formula (see [1, p.79] for details)

$$|d(L)| = N(d(L/K))|d(K)|^{[L:K]}$$

where $d(L/K)$ denoted the relative discriminant ideal and N denotes the absolute norm of the ideal, from which the first statement follows.
A prime of K ramifies in L if and only if the prime divides the relative discriminant $d(L/K)$. Thus L/K is unramified at all finite primes if and only if $d(L/K)$ is the unit ideal, proving the second statement. □

Definition. Let K be an algebraic number field. The narrow Hilbert class field of K, denoted $N(K)$, is the maximal abelian extension of K unramified at all finite primes of K.

Corollary 1.8. *Let K be an algebraic number field, and let L be any intermediate field between K and the narrow Hilbert class field of K, $N(K)$. Then $rd(K) = rd(L)$.*
In particular, the Hilbert class field of K has the same root discriminant as K.

Proof. By Proposition 1.7 and the definition of $N(K)$

$$rd(N(K)) \geq rd(L) \geq rd(K) = rd(N(K))$$

Thus $rd(N(K)) = rd(L) = rd(K)$.
Furthermore, $N(K)$ contains the Hilbert class field of K, and so their root discriminants must be equal. □

Notation. Let $rd(m) = rd(\mathbb{Q}(\zeta_m))$ and $rd'(m) = rd(\mathbb{Q}(\zeta_m)^+)$, where ζ_m is a primitive mth root of unity and $\mathbb{Q}(\zeta_m)^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is the maximal real subfield of $\mathbb{Q}(\zeta_m)$.

Corollary 1.9. *If at least two distinct primes p, q ramify in $\mathbb{Q}(\zeta_m)$, then $rd(m) = rd'(m)$.*

Proof. In such case, we have the following

$$\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_m)^+\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_m)^+\mathbb{Q}(\zeta_q)$$

As $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_m)^+\mathbb{Q}(\zeta_p)$, at most primes above p ramify in $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)^+$. Similarly, at most primes above q ramify in $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)^+$.

By Proposition 1.7, $rd'(m) \leq rd(m)$, with $rd'(m) = rd(m)$ if and only if no prime of $\mathbb{Q}(\zeta_m)^+$ ramifies in $\mathbb{Q}(\zeta_m)$.

If $\mathfrak{a}$ is any prime ideal of $C'(m)$ which ramifies in $C(m)$, then $\mathfrak{a}$ must lie above both p and q, but this is impossible since p, q are distinct.
Therefore, the equality must hold, $rd'(m) = rd(m)$. □

Proposition 1.10. *Let K and F be algebraic number fields with relatively prime discriminants, and let $L = KF$ be the compositum of F and K. Then*

$$\boxed{rd(L) = rd(K)rd(F)}$$

Proof. As proved in Washington [17, p.11]

$$d(L) = d(F)^{[K:\mathbb{Q}]}d(K)^{[F:\mathbb{Q}]}$$

Taking $[L : \mathbb{Q}] = [F : \mathbb{Q}][K : \mathbb{Q}]$th roots gives the result. □

Proposition 1.11. *The root discriminant $rd(m)$ of $\mathbb{Q}(\zeta_m)$ and $rd'(m)$ of $\mathbb{Q}(\zeta_m)^+$ are given by*
- $rd(p^a) = p^{(a-\frac{1}{p-1})}$, $rd'(p^a) = p^{\left(a-\frac{1}{p-1}-\frac{1}{\varphi(p^a)}\right)}$
- $rd(m) = rd'(m) = \prod_{p^a|m} rd(p^a)$ *when at least two primes ramify in $\mathbb{Q}(\zeta_m)$*

Proof. As calculated in [12]
$d(p^a) = p^{\varphi(p^a)\left(a-\frac{1}{p-1}\right)}$ and $d'(p^a) = p^{\frac{1}{2}\left[\varphi(p^a)\left(a+1-\frac{p}{p-1}\right)-1\right]}$

Taking $\varphi(p^a)$ and $\frac{1}{2}\varphi(p^a)$th roots, the results for $rd(p^a)$ and $rd'(p^a)$ follow.

When $m = \prod_{i=1}^{t} p_i^{a_i}$, note that $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{p_1^{a_1}}) \dots \mathbb{Q}(\zeta_{p_t^{a_t}})$ and the results follows by Proposition 1.10. □

To connect the root discriminant and class number bounds, we'll need the following.

Definition. An increasing function $g : \mathbb{N} \longrightarrow \{x \in \mathbb{R} | x > 0\}$ is called a class number bound function if for all positive integers n

$$g(n) \leq \inf rd(K)$$

where the infimum is taken over all number fields of degree n.

Some class number bound functions can be constructed using Theorem 1.4.

Theorem 1.12. *There are explicit ordered pairs of positive real numbers (A, E) for which $g_{(A,E)}(x) = Ae^{-E/x}$ is a class number bound function.*
The function $G(x) = \sup_{(A,E)} g_{(A,E)}(x)$ is also a class number bound function.

Proof. (Sketch) These functions are constructed using Theorem 1.1. We will give an example of how such a function can be constructed (for details of the general case see [6]). We will denote computable real constants by a_i, $i \in I$, for some index set I.
Let K be a number field of degree n and discriminant D. As shows in (12), using the simplest estimates of factors in Theorem 1.1

$$\begin{aligned} D &\geq \left(\pi \exp\left(\gamma + 2\log 2 + \frac{2.714}{4}\right)\right)^{r_1} \left(2\pi \exp\left(\gamma + \frac{1.329}{2}\right)\right)^{2r_2} + O(1) \\ &= \pi^{r_1}(2\pi)^{2r_2} \exp\left((r_1 + 2r_2\gamma + r_1 a_1 + 2r_2 a_2) + O(1)\right. \end{aligned}$$

Define

$$A = \max(\pi^{r_1/n}(2\pi)^{2r_2/n}) \text{ and } E = -\min\left(n\left((r_1 + 2r_2\gamma + r_1 a_1 + 2r_2 a_2)\right)\right.$$

where the maximum and minimum is taken over all non-negative integers r_1, r_2 with $r_1 + 2r_2 = n$, and ensure that these constants are big enough such that

$$D^{1/n} \geq Ae^{-E/n}$$

for any number field of degree n. Thus $g_{(A,E)} = Ae^{-E/n}$ is class number bound function. Better class number bound functions (that is, closer to the value of the infimum) may be obtained using better estimates of Z, Z_1 and ψ in Theorem 1.1. □

The main result of Masley is the following.

Theorem 1.13. *Let K be a number field and let $g(x)$ be a class number bound function. The $g(x) > rd(K)$ implies*

$$\boxed{h(K) < \frac{x}{[F : \mathbb{Q}]}}$$

Proof. Let $H(K)$ be the Hilbert Class Field of K. Then

$$\begin{aligned} g(x) > rd(K) = rd(H(K)) &\geq g([H(K) : \mathbb{Q}]) \\ &= g(h(K)[K : \mathbb{Q}]) \end{aligned}$$

Thus $g(x) > g(h(K)[K : \mathbb{Q}])$.
As g is increasing, $h(K)[K : \mathbb{Q}] < x$ and so

$$h(K) < \frac{x}{[K : \mathbb{Q}]}$$

□

Remark. Since $g(x)$ is necessarily bounded, Theorem 1.13 is only useful for fields with small root discriminant.

The results of Odlyzko, more specifically Theorem 1.12, can be applied directly. Suppose K is a number field of degree n. By Theorem 1.12 a pair (A, E) can be explicitly constructed, with

$$|d(K)| > A^n e^{-E}$$

Applying this to the Hilbert class field, the corollary above gives

$$\log(rd(K)) > \log A - \frac{E}{hn}$$

If $rd(K) < A$, then we obtain an upper bound for the class number h

$$\boxed{h < \frac{E}{n(\log A - \log rd(K))}}$$

However, if the root discriminant of K is larger 60.7 (the largest value of root discriminant in Odlyzko's table and hence the largest value of root discriminant for which a pair (A, E) can be effectively computable, see [13]), the above method cannot be applied. Therefore, this method is very much limited.

Miller's Upper Bounds for Class Numbers

In [7], Miller was able to obtain an upper bound for class numbers of number fields of root discriminant larger than 60.7 by establishing lower bounds for sums over prime ideals of the Hilbert class field. Miller gives the following important lemma, which he proved in an earlier paper [8].

Lemma 1.14. *Let K be a totally real field of degree n, and let*

$$F(x) = \frac{e^{-\left(\frac{x}{c}\right)^2}}{\cosh\left(\frac{x}{2}\right)}$$

for a positive constant c. Suppose S is a subset of the prime integers which totally split into principal ideals of K. Let

$$B = \frac{\pi}{2} + \gamma + \log 8\pi - \log rd(K) - \int_0^\infty \frac{1 - F(x)}{2}\left(\frac{1}{\sinh\frac{x}{2}} + \frac{1}{\cosh\frac{x}{2}}\right)dx + 2\sum_{p\in S}\sum_{m=1}^{\infty}\frac{\log p}{p^{\frac{m}{2}}}F(m\log p)$$

If $B > 0$ then we have an upper bound for the class number h of K

$$\boxed{h < \frac{2c\sqrt{\pi}}{nB}}$$

There is a slightly stronger version of this lemma if one assumes the Generalized Riemann Hypothesis.

Lemma 1.15. *Let K be a totally real field of degree n, and let*

$$F(x) = e^{-\left(\frac{x}{c}\right)^2}$$

for a positive constant c. Suppose S is a subset of the prime integers which totally split into principal ideals of K. Let

$$B = \frac{\pi}{2} + \gamma + \log 8\pi - \log rd(K) - \int_0^\infty \frac{1 - F(x)}{2}\left(\frac{1}{\sinh\frac{x}{2}} + \frac{1}{\cosh\frac{x}{2}}\right)dx + 2\sum_{p\in S}\sum_{m=1}^{\infty}\frac{\log p}{p^{\frac{m}{2}}}F(m\log p)$$

If $B > 0$ then we have, under the generalized Riemann hypothesis, an upper bound for the class number h of K

$$\boxed{h < \frac{2c\sqrt{\pi}\ e^{\left(\frac{c}{4}\right)^2}}{nB}}$$

Note. Using this result, to find an upper bound of h it suffices to take the set S large enough and then pick an appropriate constant $c > 0$, to have $B > 0$.

There is an efficient ways of choosing S and it begins with the following observation.

Observation. Given an element x of a Galois number field K, we define its norm to be

$$N(x) = \left| \prod_{\sigma\in Gal(K/\mathbb{Q})} \sigma(x) \right|$$

Note that if x is in the ring of integers of K, and if its norm is a prime integer p, which is

unramified in K, then p totally splits into principal ideals and we can take p to be in the set S.

Once sufficiently many such prime integers which totally spit into principal ideals are found, upper bound for the class number can be established.

After an upper bound is established, various "push up" and "push down" results (some of which can be found in the next section) can be used to determine the exact class number.

In [7], Miller uses this method to prove the following.

Theorem 1.16. *(Miller) Let p be a prime integer, and let $\mathbb{Q}\left(\zeta_p + \zeta_p^{-1}\right)$ denote the maximal real subfield of the pth cyclotomic field $\mathbb{Q}\left(\zeta_p\right)$. Then the class number of $\mathbb{Q}\left(\zeta_p + \zeta_p^{-1}\right)$ is 1 for $p \leq 151$.*
Furthermore, under the assumption of the generalized Riemann hypothesis, the class number of $\mathbb{Q}\left(\zeta_p + \zeta_p^{-1}\right)$ is 1 for $p \leq 241$ and $p \neq 163, 191, 229$, with $h\left(\mathbb{Q}\left(\zeta_{163} + \zeta_{163}^{-1}\right)\right) = 4$, $h\left(\mathbb{Q}\left(\zeta_{191} + \zeta_{191}^{-1}\right)\right) = 11$ and $h\left(\mathbb{Q}\left(\zeta_{229} + \zeta_{229}^{-1}\right)\right) = 3$.

The basic ideas of Miller's methodology are presented in the following proposition.

Proposition 1.17. *The class number of $\mathbb{Q}(\zeta_{71} + \zeta_{71}^{-1})$ is 1*

Proof. (Sketch) Using the integral basis $\{b_0, b_1 \ldots b_{34}\}$ where $b_0 = 1$ and $b_j = 2\cos\frac{2\pi j}{p}$ for $1 \leq j \leq 34$, searching over the elements of the form

$$\sum_{i=0}^{34} a_i b_i$$

where $a_i \in \{-1, 0, 1\}$, one finds algebraic integers (of this form) with prime norms

283 , 569, 709, 853 , 1277, 1279, 1847, 1987, 2129 and 2131

With these forming S and $c = 15$, Lemma 1.14 gives

$$h\left(\mathbb{Q}(\zeta_{71} + \zeta_{71}^{-1})\right) < 9$$

Using Schoof's table, the class number is 1 (see [14]).

Note. In [14], for each prime conductor less than 10000, Schoof gives a number $\tilde{h}$ which is either equal to the class number h, or $h > 8000\tilde{h}$. In particular, if the upper bound of h is less than 8000, then $h = \tilde{h}$.

□

2 Some General Results

This section will include some general results on the class numbers and the ideal class groups of extensions of number fields. These will be used alongside the bounds of the previous section to determine some class numbers. The results are stated in full generality, even through we will apply them to specific types of extensions.
We will follow section 2 of Masley's paper [6].

Notation. Throughout this section $d(m)$ and $h(m)$ will denote the discriminant and class number of $\mathbb{Q}(\zeta_m)$, where ζ_m is a primitive mth root of unity. Similarly, $d'(m)$ and $h'(m)$ will denote the discriminant and class number of $\mathbb{Q}\left(\zeta_m + \zeta_m^{-1}\right) = \mathbb{Q}(\zeta_m)^+$.

The following series of results are fundamental in the proof of the first significant theorem of this section, the 'Pushing up' theorem.

Theorem 2.1. *Let E/F be an extension of number fields. The following are equivalent:*
1. For any unramified abelian extension H of F, $H \cap E = F$
2. The norm map $N : Cl(E) \longrightarrow Cl(F)$ is surjective.
If (1) and (2) are satisfied, then $Cl(F)$ is isomorphic to a subgroup of $Cl(E)$.
In particular $h(F)$ divides $h(E)$ and the order of the kernel of N is $\frac{h(E)}{h(F)}$

Remark. The norm map referred to above is defined as $N([I]) = \left[N_{E/F}(I)\right]$, where $N_{E/F}$ denotes the usual ideal norm in the extensions E/F

Proof. From Class Field theory there exists an inclusion reversing bijection ϕ between $U = \{H \,|F \subseteq H \subseteq E,\ H/F \text{ is unramified and abelian}\}$ and $C = \{G \leqslant ClF) \mid N(Cl(E)) \subseteq G\}$ (this is a corollary of the Artin Reciprocity theorem for Hilbert Class Field, often referred to as Class Field Theory for unramified abelian extensions, for details see [2, p.98])

Claim. $\phi(F) = Cl(F)$

Suppose $\phi(F) = G \lneqq Cl(F)$ for some $G \in C$. Since $Cl(F) \in C$, there exists $H \in U$ such that $\phi(H) = Cl(F)$. Then $\phi(F) \lneqq \phi(H)$ and as ϕ is an inclusion reversing bijection, $H \subsetneq F$ which contradicts $H \in U$. Thus $\phi(F) = Cl(F)$ proving the claim.
Suppose that (1) holds.
Let $G = N(Cl(E)) \leqslant Cl(F)$. As $G \in C$, $G = \phi(H)$ for some $H \in U$. To prove that $G = Cl(F)$ (and so N is surjective), by the claim it suffices to show $H = F$. As H is an unramified abelian extension of F , by assumption $E \cap H = F$. Also $H \subseteq E$ so $E \cap H = H$, and thus $F = E \cap H = H$.
Suppose that (2) holds, so $N(Cl(E)) = Cl(F)$.
Let H be any unramified, abelian extension of F. Then $F \subseteq H \cap E \subseteq E$, with $H \cap E$ unramified and abelian, so $H \cap E \in U$, and hence $\phi(H \cap E) = G \in C$.
As $G \in C$, $G \leq Cl(F)$ and by assumption $N(Cl(E)) = Cl(F) \leq G$, it follows that

$G = Cl(F)$, and hence $\phi(H \cap E) = Cl(F) = \phi(F)$, so $H \cap E = F$.
This concludes the proof of the two conditions being equivalent.
If (2) holds (or equivalently (1)), by the first isomorphism theorem

$$Cl(F) = N(Cl(E)) \simeq Cl(E)/Ker(N).$$

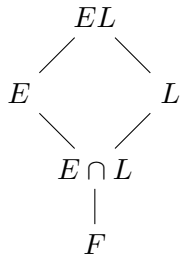
and $Cl(E)/Ker(N)$ is isomorphic to a subgroups of $Cl(E)$. Therefore $h(F) = |Cl(F)| = |Cl(E)/Ker(N)| = \frac{|Cl(E)|}{|Ker(N)|}$ and so: $h(F) | h(E)$ and $|Ker(N)| = \frac{h(E)}{h(F)}$ □

The equivalence given in Theorem 2.1 plays an important role in checking the hypothesis condition of the 'Pushing up theorem' in [6]. In order to prove the 'Pushing up' theorem we will use some preliminary results which are implied in [6], but not stated or proved.

Lemma 2.2. *Let E and L be field extensions of a number field F. If E/F is a Galois extension then EL/L and $E/E \cap L$ are both Galois extensions , and $Gal(EL/L) \cong Gal(E/E \cap L)$.*
In particular $[EL : L] = [E : E \cap L]$

This Lemma is adapted from [10]

Proof. Note the we have the following picture



As E/F is a Galois extension, E must be the splitting filed of some separable polynomial $f \in F[x]$.
Notably, $f \in L[x]$ so EL is the splitting field of f over L , and $f \in (E \cap L)[x]$ so E is the splitting field of f over $E \cap L$. Thus EL/L and $E/E \cap L$ are both Galois extensions.
Consider the map

$$\psi : Gal(EL/L) \longrightarrow Gal(E/E \cap L)$$
$$\sigma \longmapsto \sigma|_E$$

Observe that this is well defined, since $E \subseteq EL$ and any $\sigma \in Gal(EL/L)$ permutes the roots of f, so $\sigma(E) = E$. Clearly, ψ is homomorphism.

If $\sigma \in Gal\,(EL/L)$ is such that $\sigma|_E = 1$ (in $Gal\,(E/E \cap L)$), then σ fixes all elements of E and so it fixes all elements of EL, and thus $\sigma = 1$ (in $Gal\,(EL/L)$) so ψ is injective. If $\alpha \in E$ is fixed by all $\sigma \in Gal(EL/L)$, then $\sigma \in E \cap L$. Then $E^{\psi(Gal(EL/L))} = E \cap L$ and so by the Fundamental theorem of Galois Theory

$$\psi(Gal(EL/L)) = Gal(E/E \cap L)$$

and hence ψ is also surjective. □

We will need the following version of Abhyankar's Lemma.

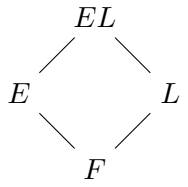
Lemma 2.3. *(Abhyankar's Lemma) Let E and L be field extensions of a number field F and EL their compositum. Let $\mathfrak{p}_E$, $\mathfrak{p}_L$ be primes of E,L respectively with the same restriction $\mathfrak{p}$ to F, and $\mathfrak{P}$ a prime of EL lying above both. Then*

$$e(\mathfrak{P}/\mathfrak{p}_L) = e(\mathfrak{p}_E/\mathfrak{p})/\gcd(e(\mathfrak{p}_E/\mathfrak{p}), e(\mathfrak{p}_L/\mathfrak{p}))$$

Proof. See [5]. □

Lemma 2.4. *Let E/F and L/F be two number field extensions. If E/F is unramified, then EL/L is unramified.*

Proof. Recall that EL/L is unramified if no prime of L, finite or infinite. ramifies in EL.



Let $\mathfrak{p}_L$ be any finite prime of L. To show $\mathfrak{p}_L$ does not ramify in EL, one must show that for any prime $\mathfrak{P}$ of EL with $\mathfrak{P} \mid \mathfrak{p}_L O_L$, $e\,(\mathfrak{P}/\mathfrak{p}_L) = 1$.
Take $\mathfrak{p}$ of F with $\mathfrak{p}_L|\mathfrak{p}O_L$, and $\mathfrak{p}_E$ a prime of E with $\mathfrak{p}_E\,|\mathfrak{p}O_E$ and $\mathfrak{P} \mid \mathfrak{p}_E O_{EL}$.
By Abhyankar's lemma

$$e\,(\mathfrak{P}/\mathfrak{p}_L) = e\,(\mathfrak{p}_E/\mathfrak{p})\,/\,\gcd\,(e\,(\mathfrak{p}_E/\mathfrak{p})\,, e\,(\mathfrak{p}_L/\mathfrak{p}))$$

Since E/F is unramified, $e\,(\mathfrak{p}_E/\mathfrak{p}) = 1$ and hence $e\,(\mathfrak{P}/\mathfrak{p}_L) = 1$ as required.
Let σ be an infinite prime of L, and suppose that it ramifies in EL.
Now, σ is real, but has complex extensions σ_{EL} and $\sigma_{\bar{E}L}$, with $\sigma_{EL} \neq \sigma_{\bar{E}L}$ and $\sigma_{EL}|_L = \sigma = \sigma_{\bar{E}L}|_L$ (this is the definition of σ ramifying in EL).
Note $\sigma|_F$ is real. Also $\sigma|_F$ is extended by $\sigma_{EL}|_E$ and $\sigma_{\bar{E}L}|_E$, which are not equal and not real (else $\sigma_{EL} = \sigma_{\bar{E}L}$). This is contradiction, as E/F is unramified.
Therefore, no infinite prime of L ramifies in EL, and this completes the proof. □

If the equivalent conditions of Theorem 2.1 are satisfied for the extension E/F, then one sees directly that $h(F) = |H(F) : F| = |EH(F) : E|$ divides $h(E) = |H(E) : E|$ since $EH(F) \subseteq H(E)$ by Lemmas 2.2 and 2.4.
This can also be deduced from the stronger result of the 'Pushing up' theorem.

Theorem 2.5. *(Pushing up) Let E/F be an extension of number fields.*
Then $|H(F) : H(F) \cap E|$ divides $h(E)$ and $h(F)$ divides $|E : F|h(E)$.
In particular, if for any any unramified abelian extension H of F, $E \cap H = F$ then $h(F)$ divides $h(E)$.

Proof. By Lemmas 2.2 and 2.4 $|H(F) : H(F) \cap E| = |EH(F) : E$ divides $h(E) = |H(E) : E|$, and $h(F) = |H(F) : F| = |EH(F) : E|$ divides $h(E)|E : F| = |H(E) : E||E : F| = |H(E) : F|$.

$$\begin{array}{c} H(E) \\ | \\ EH(F) \\ | \\ E \\ | \\ F \end{array}$$

If for any unramified abelian extension H of F, $E \cap H = F$, then $|H(F) : H(F) \cap E| = |H(F) : F| = h(F)$ divides $h(E)$. □

This theorem is particularly powerful in the case of 'totally ramified' extensions.

Definition. An extension E/F is totally ramified if no subextension of E/F, except F itself is unramified over F.
Corollary 2.6. *Suppose E/F is totally ramified. Then $h(F)$ divides $h(E)$.*

Proof. Let H be any unramified abelian extension of F. Then $H \cap E$ is an unramified abelian extension of F, contained in E, thus $H \cap E = F$ as E/F is totally ramified.
By Theorem 2.5 $h(F)|h(E)$. □

Example. If $F \subseteq E \subseteq C(p^a)$ then $h(F)|h(E)$.

Corollary 2.7. *For the cyclotomic fields: $h'(m)|h(m)$, $h'(m)|h'(km)$ and $h(m)|h(km)$ for any positive integer k.*

Proof. The cyclotomic extensions $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)^+$, $\mathbb{Q}(\zeta_{km})^+/\mathbb{Q}(\zeta_m)^+$ and $\mathbb{Q}(\zeta_{km})/\mathbb{Q}(\zeta_m)$ are totally ramified. □

Information on the class groups of number fields can also be 'pushed down', as will be shown in the subsequent results.

Definition. Let p be a prime and F a number field. A p-extension E of F, is a Galois extension, whose Galois group is a p-group. In other words, $|Gal\,(E/F)\,| = [E : F] = p^n$ for some $n \in \mathbb{N}$.

The following lemma is fundamental.

Lemma 2.8. *Let E/F be a non-trivial p-extension , which is unramified outside the (possibly empty) finite set S of prime divisors of F.*
If S is empty, F has an unramified cyclic extension of degree p.
If S is non empty, then for any $v \in S$, if p divides $h\,(E)$, then F has a cyclic extension of degree p , which is unramified outside $S - \{v\}$

Proof. The proof will make use of the well known fact that any proper subgroup of a p group is contained in a normal subgroup of index p
Suppose $S = \emptyset$.
Then $Gal(E/F)$ contains a normal subgroup A of index p.
Set $K = E^A$, the subfield of E fixed by A. This is an extension of F and
• K/F is unramified (since S is empty)
• $[K : F] = |Gal(E/F)/A| = p$ (by the Fundamental theorem of Galois Theory).

Suppose $S \neq \emptyset$ and $v \in S$.
Let $P(E)$ be the maximal unramified abelian p extension of E. As p divides $h(E)$, $P(E)$ is a proper extension of E. Suppose s is any embedding of $P(E)$ into an algebraic closure of F which restricts to the identity on F. Then $s(E) = E$ (since E/F is normal and $s(P(E))/s(E)$ is an unramified abelian p-extension). By maximality of $P(E)$, $s(P(E)) = P(E)$ so $P(E)/F$ is a Galois extension .
Let $G = Gal(P(E)/F)$ and T be the inertia group for a prime w of $P(E)$ lying above v. Since $P(E)/E$ is a proper extension, and $P(E)/E$ is unramified, T is a proper subgroup of G.
Let N be a normal subgroup of G containing T, with $|G : N| = p$.
Let $K = P(E)^N$, the subfield of $P(E)$ fixed by N.
The inertia group $T^{'}$ of any prime of $P(E)$ lying above v is conjugate in G to T, hence it is contained in N. It follows that K/F is unramified at v. Since $P(E)/F$ is unramified outside S, K/F is unramified outside $S^{'} = S - \{v\}$. □

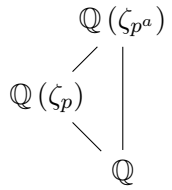
An important consequence of this is the following.

Theorem 2.9. *(Pushing down) Suppose E/F is a p-extension with at most one ramified prime divisor of F ramified in E. Then $p|\ h(E)$ implies $p|\ h(F)$. Moreover, if E/F is totally ramified, then $p|\ h(E)$ if and only if $|\ h(F)$.*

Proof. By Theorem 2.8, since p divides $h(E)$, $H(F)$ the Hilbert class field of F contains

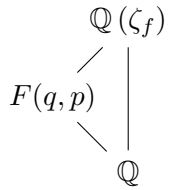
a cyclic extension of degree p (over F). Hence $p\,|h(F) = \ |H(F) : F|$.
Suppose E/F is totally ramified. By Corollary 2.6, $h(F)$ divides $h(E)$ and thus if $p|\ h(F)$, then $p|\ h(E)$. □

Example. If $p\ |h(p^a)$ then $p\ |h(p)$, as $[\mathbb{Q}\,(\zeta_{p^a}) : \mathbb{Q}\,(\zeta_p)] = p^{a-1}$ so Theorem 2.9 applies directly.



Notation. Let $f \in \mathbb{N}$ and n a positive integer with $n|\ \phi(f) = |\mathbb{Q}(\zeta_f : \mathbb{Q}|$. Let $F\,(n, f)$ be a degree n cyclic extension of $\mathbb{Q}$, with conductor f. In general this is not unique, but we will distinguish between the extensions determined by n and f when necessary or consider all fields such fields if unspecified.

Example. Let p,q be primes with $p \equiv 1 \mod 2q$. Then q does not divide $h(F(q,p))$, since otherwise by Theorem 2.9, $q|\ h\,(\mathbb{Q}) = 1$



Studying the structure of the ideal class group can also be useful in determining the class number. Important information on the rank of the ideal class group is given by the 'Structure theorem'. We begin with some preliminaries.
Let G be a finite abelian group and p a prime number.
Definition. The p-rank of G, denoted by $r(p)$, is the dimension of the vector space $\mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} G \simeq G/p\ G$ over the field $\mathbb{F}_p$.
Equivalently, the p-rank of G is the number of cyclic factors in an elementary divisor decomposition of the p-Sylow group of G.

Remark. G is a finite abelian group and so it may be decomposed into a product of primary cyclic subgroups:

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_k\mathbb{Z}$$

with $d_i|d_{i+1}$ for all $1 \leq i < k$, and thus:

$$r\,(p) = |\{i : p \mid d_i\}|$$

Definition. Let $q = p^a$, for some positive integer a. The q-rank of G, denoted by $r(q) = r(p^a)$, is the number of cyclic factors in an elementary divisor decomposition of the p-Sylow subgroup of G, whose order is divisible by q.

Remark. If $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_k\mathbb{Z}$, then

$$r(p^a) = |\{i : q \mid d_i\}|$$

Let $B(p^n) = G/G_{p^n}$, where $G_{p^n} = \{g^{p^n} : g \in G\}$.
We begin by proving the following purely algebraic lemma. This is result implied in Masley's proof of the Rank Theorem, but it is not stated or proved.
Lemma 2.10. *For any* $n \geq 1$

$$\boxed{B(p^n) \simeq (\mathbb{Z}/p^n\mathbb{Z})^{r(p^n)} \times \prod_{i=1}^{n-1} \left(\mathbb{Z}/p^i\mathbb{Z}\right)^{r\left(p^i\right)-r\left(p^{i+1}\right)}}$$

In particular, $\mid B(p^n) \mid = p^{s(n)}$ *where* $s(n) = \sum_{i=1}^{n} r\left(p^i\right)$

Proof. Observe that $G \simeq \prod_{i=1}^{k} \mathbb{Z}/d_i\mathbb{Z}$ and $G_{p^n} \simeq \prod_{i=1}^{k} p^n(\mathbb{Z}/d_i\mathbb{Z})$.
Consider the natural homomorphism

$$\phi : G \longrightarrow \prod_{i=1}^{k} \frac{\mathbb{Z}/d_i\mathbb{Z}}{p^n(\mathbb{Z}/d_i\mathbb{Z})}$$

Then ϕ is a surjective homomorphism with kernel G_{p^n}, and thus:

$$G/G_{p^n} \simeq \prod_{i=1}^{k} \frac{\mathbb{Z}/d_i\mathbb{Z}}{p^n(\mathbb{Z}/d_i\mathbb{Z})}$$

If $n = 1$, then for any i, either $p \nmid d_i$ or $p \mid d_i$.
Case 1. If $p \nmid d_i$, then $p(\mathbb{Z}/d_i\mathbb{Z}) \simeq \mathbb{Z}/d_i\mathbb{Z}$ and so $\frac{\mathbb{Z}/d_i\mathbb{Z}}{p(\mathbb{Z}/d_i\mathbb{Z})} \simeq 1$
Case 2. If $p \mid d_i$, then the natural homomorphism

$$\varphi : \mathbb{Z}/d_i\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

is surjective, its kernel is $p(\mathbb{Z}/d_i\mathbb{Z})$ and hence:

$$\frac{\mathbb{Z}/d_i\mathbb{Z}}{p(\mathbb{Z}/d_i\mathbb{Z})} \simeq \mathbb{Z}/p\mathbb{Z}$$

Therefore:

$$G/G_p \simeq (\mathbb{Z}/p\mathbb{Z})^{r(p)}$$

since $r(p) = |\{i : p \mid d_i\}|$.
For $n > 1$ and $1 \leqslant i \leqslant k$, either $p \nmid d_i$ or d_i is divisible by some power of p.

Case 3. If $p \nmid d_i$, arguing as before $\frac{\mathbb{Z}/d_i\mathbb{Z}}{p^n(\mathbb{Z}/d_i\mathbb{Z})} \simeq 1$

Case 4. If $p^m \mid d_i$ for $0 < m < n$ and $p^{m+1} \nmid d_i$, then: $p^n(\mathbb{Z}/d_i\mathbb{Z}) = p^{n-m}(p^m(\mathbb{Z}/d_i\mathbb{Z})) \simeq p^m(\mathbb{Z}/d_i\mathbb{Z})$

$$\frac{\mathbb{Z}/d_i\mathbb{Z}}{p^n(\mathbb{Z}/d_i\mathbb{Z})} \simeq \mathbb{Z}/p^m\mathbb{Z}$$

where the isomorphism is induced by the natural homomorphism:

$$\varphi_{(m,d_i)} : \mathbb{Z}/d_i\mathbb{Z} \longrightarrow \mathbb{Z}/p^m\mathbb{Z}$$

Note that : $|\{i : p^m \mid d_i, p^{m+1} \nmid d_i\}| = r(p^m) - r\left(p^{m+1}\right)$, and hence combining all such term in the quotient G/G_{p^n} we get:

$$(\mathbb{Z}/p^m\mathbb{Z})^{r(p^m)-r\left(p^{m+1}\right)}$$

Case 5. If $p^n \mid d_i$ then as argued previously: $\frac{\mathbb{Z}/d_i\mathbb{Z}}{p^n(\mathbb{Z}/d_i\mathbb{Z})} \simeq \mathbb{Z}/p^n\mathbb{Z}$, and hence combing all these terms in the quotient, we get:

$$(\mathbb{Z}/p^n\mathbb{Z})^{r(p^n)}$$

The result follows from the 3 cases above.
With notation as above, $|B(p^n)| = p^{nr(p^n)} \prod_{i=1}^{n-1} p^{i(r(p^i)-r(p^{i+1}))}$. Thus

$$|B| = p^{s((n)}$$

with $s(n) = nr(n) + \sum_{i=1}^{n-1} i(r(p^i) - r(p^{i+1}))$.

$$\begin{aligned} s(n) &= nr(p^n) + \sum_{i=1}^{n-1} ir(p^i) + \sum_{i=1}^{n-1} ir(p^{i+1}) && (20)\\ &= nr(p^n) - (n-1)r(p^n) + \sum_{i=1}^{n-1} ir(p^i) + \sum_{i=2}^{n-1}(i-1)r(p^i) && (21)\\ &= r(p^n) + r(p) + \sum_{i=2}^{n-1}(i-(i-1))r(p^i) && (22)\\ &= \sum_{i=1}^{n} r(p^i) && (23) \end{aligned}$$

□

This lemma is used in the proof of the following result.

Theorem 2.11. *(Structure theorem) Let E/F be cyclic extension of degree n and p a prime number which divides neither n nor $h\left(\tilde{E}\right)$ for $F \subseteq \tilde{E} \subsetneq E$. Let $q = p^a$, where a is any positive integer. Then the q-rank of $Cl(E)$ is divisible by f, the order of p modulo n.*

Proof. The proof consists of two main steps:
1.The group $G = Gal(E/F)$ acts on $B(q) = Cl(E)/Cl(E)_q$, where as above $Cl(E)_q = \{c^q : c \in Cl(E)\}$.
2. The action of G on $B(q) - \{1\}$ is faithful.
Assuming these two results: the orbits of any generator of G will have n elements, and so $|B(q)| \equiv 1 \bmod n$. If $q = p$, $|B(p)| = p^{r(p)}$ by the lemma. Thus:

$$p^{r(p)} \equiv 1 \bmod n \text{ and so } f \mid r(p), \text{ since } f \text{ is the order of } p \text{ modulo } n.$$

Assume that $f \mid r(p^n)$ for all $1 \leq n < a$. Then, by the lemma :

$$|B(q)| = |B(p^a)| = p^{\sum_{i=1}^{a} r\left(p^i\right)}$$

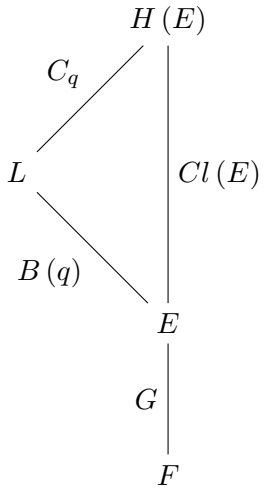
and hence: $f \mid \sum_{i=1}^{a} r\left(p^i\right)$ and so using the induction hypothesis: $f \mid r(q) = r(p^a)$, which is the required results.

Step 1. Recall that $Cl(E) \simeq Gal(H(E)/E)$, where $H(E)$ is the Hilbert class field of E. This follows from Artin's reciprocity law (see [2, p.97]) and the isomorphisms is given by:

$$\psi : [\mathfrak{a}] \longmapsto \left(\frac{H(E)/E}{\mathfrak{a}}\right)$$

Let $L = H(E)^{C_q}$, the subfield of $H(E)$ fixed by $C_q = \psi\left(Cl(E)_q\right)$. Note that $G = Gal(E/F)$ acts on $Cl(E)$, by the natural action $(\sigma, [\mathfrak{a}]) = [\sigma(\mathfrak{a})]$.
This is equivalent to G acting on $Gal(H(E)/E)$ by conjugation (by the properties of the Artin symbol, see [2, p.95] for details).

Since C_q is G-invariant, it is a normal subgroup of $Gal(H(E)/F)$. Also L/F is Galois and G acts on: $Gal(L/E) \simeq Cl(E)/Cl(E)_q = B(q)$.



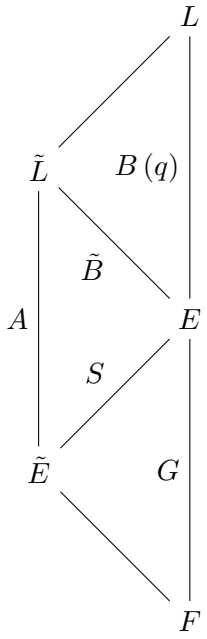
Step 2. Take $g \in G$ and let $S = \langle g \rangle$.
For $b \in B(q)$, denote by gb the result of the action of g on b. This can be extended by additivity and so $B(q)$ may be viewed as a $\mathbb{Z}[G]$ module.
Suppose $g \neq 1$. Observe that it is sufficient to prove $(g-1)B(q) = B(q)$, since if this were the case, then the map:

$$\phi_g : B(q) \longrightarrow B(q)$$
$$\phi_g : b \longmapsto (g-1)b$$

is surjective.

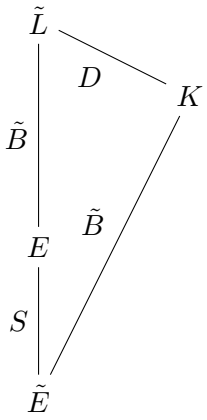
Also, as $B(q)$ is finite, ϕ_g is injective (and this is for any $g \in G, g \neq 1$).

The action is necessarily faithful, as otherwise, there exists an $f \in Gal(E/F)$ with $f \neq 1$ and $fx = x$ for all $x \in B(q) - \{1\}$, then $\phi_f(x) = (f-1)(x) = fx - x = x - x = 0$ for all $x \in B(q)$, contradicting the fact that ϕ_f is injective.
Let $\tilde{E} = E^S$. Note that $(g-1)B(q) < B(q)$, S acts on $(g-1)B(q)$, and thus $(g-1)B(q)$ is a normal subgroup of $Gal\left(L/\tilde{E}\right)$ (since the action is by conjugation). Then $\tilde{L} = L^{(g-1)B(q)}$ is a normal extension of $\tilde{E}$.
Let $A = Gal\left(\tilde{L}/\tilde{E}\right)$, then $\tilde{B} = B(q)/(g-1)B(q) = Gal\left(\tilde{L}/E\right)$.



Note that $|\tilde{B}| = p^m$ for some $m \in \mathbb{N}$, and $|S|$ divides n, so since $p \nmid n$, $|\tilde{B}|$ and $|S|$ are coprime, and therefore: $A \simeq \tilde{B} \times D$, with $D \simeq S$ (complements of groups).

Let K be the field fixed by D, such that $Gal\left(\tilde{L}/K\right) = D$ and $Gal\left(K/\tilde{E}\right) = A/D \simeq \tilde{B}$.



Suppose $\tilde{B}$ is not trivial. Let P be any prime divisor of $L\tilde{L}$, and T its inertial group in $\tilde{L}/\tilde{E}$. Since $\tilde{L}/E$ is unramified (as $\tilde{L}$ is a subfield of $H(E)$), $T \cap \tilde{B} = 1$.
Also $|\tilde{B}|$ and $|D|$ are coprime, so $T \subseteq D$. Therefore, $K/\tilde{E}$ is unramified, so $K \subseteq H\left(\tilde{E}\right)$ and consequently, $p \mid h\left(\tilde{E}\right)$. As $F \subseteq \tilde{E} \subsetneq E$, this contradicts our hypothesis, so $\tilde{B}$ must be trivial, and this completes the proof of step 2.

□

Theorem 2.12. *(Rank Theorem) Suppose E/F is a cyclic extension of degree n. Let p be a prime which does not divide $h\left(\tilde{E}\right)$ for any $F \subseteq \tilde{E} \subsetneq E$ and which does not divide*

n. If $p \mid h(E)$ then the p-rank of $Cl(E)$ is a multiple of f, the order of p module n, and $p^f \mid h(E)$

Proof. Since $Cl(E) \simeq \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_k\mathbb{Z}$, it follows that $h(E) = |Cl(E)| = \prod_{i=1}^{k} d_i$. Recall that $r(p) = |\{i : p \mid d_i\}|$, and $f \mid r(p)$ by Theorem 2.11, so p divides f of the d_i's and hence $p^f \mid h(E)$. □

This is a very useful consequence of the Structure theorem, as it can be use alongside bounds on the class number (see tables of [13]) to calculate the class number, as will be demonstrated in the examples below.

Example. Recall that $h'(59)$ denotes the class number of $\mathbb{Q}(\zeta_{59})^+$. Using discriminant bounds, we can deduce that $h'(59) \leq \frac{340}{29} < 12$ As $\mathbb{Q}(\zeta_{59})^+/\mathbb{Q}$ is a cyclic extension of degree 29, by Theorem 2.12 for all primes $p < 12$, if $p|\ h'(59)$, then p^{f_p} also divides $h'(59)$, where f_p is the order of p modulo 29.
But for all $p < 12$, $p^{f_p} > 12$ and so $h'(59) = 1$

Example. As 11 divides $66 = \phi(67)$, $F(11, 67)$ exists and is a cyclic extension of $\mathbb{Q}$, of degree 11. Using Odlyzko's class number bound functions, we can deduce $h(F(11, 67) \leq 13$.
By Theorem 2.9, 11 does not divide $h(F(11, 67))$.
Also if $p \neq 11$, $p \leq 13$ divides $h(F(11, 67))$, then so does $p^{f_p} \geq 13$ by Theorem 2.12, where f_p is the order of p modulo 11. For any $p \leq 13$ and $p \neq 11$, $p^{f_p} > 13$ and hence $h(F(11, 67)) = 1$.

Another important results proved in [6] is the 'Kummer Criterion'. Before stating this result, we will discuss some of the background material as presented in [6].

Recall that for any $m \in \mathbb{N}$, $h'(m)$ divides $h(m)$, and so one can write

$$h(m) = h^*(m)h'(m)$$

for some $h^*(m) \in \mathbb{N}$, called the relative class number. There are explicit ways of calculating $h^*(m)$.
When $m = p$

$$h^*(p) = 2p \prod_{\chi} (-2f(\chi))^{-1} \sum_{a=1}^{f(\chi)} a\chi(a)$$

where the product is over all the primitive, odd Dirichlet characters χ of conductor $f(\chi)$.

This was known to Kummer and he called it 'the formula for the first factor $h_1(p)$' of the cyclotomic class number of the p-th roots of unity .

Kummer also had a general formula for the first factor $h_1(m)$ of the cyclotomic class number of the mth roots of unity

$$h_1(m) = \begin{cases} 2m \prod_{\chi} (-2f(\chi))^{-1} \sum_{a=1}^{f(\chi)} a\chi(a) & \text{if m is odd and } m \not\equiv 2 \ mod 4 \\ m \prod_{\chi} (-2f(\chi))^{-1} \sum_{a=1}^{f(\chi)} a\chi(a) & \text{if m is odd and } m \equiv 0 \ mod 4 \end{cases}$$

For Kummer, the second factor of the cyclotomic class number of the mth roots of unity was $h_2(m) = \frac{h(m)}{h_1(m)}$.

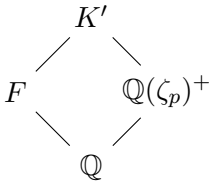
If $m = p^a$, $h_1(p^a) = h^*(p^a)$ and so $h_2(p^a)$ is the class number of $\mathbb{Q}(\zeta_{p^a})$.
When more than one prime ramifies in $\mathbb{Q}(\zeta_m)$, $h^*(m) = 2h_1(m)$ and so $h_2(m)$ is twice the class number of $\mathbb{Q}(\zeta_m)^+$.

Note. Kummer considered the second factor to be the class number of $\mathbb{Q}(\zeta_m)^+$ because his class group was the group of ideals modulo the subgroup of ideals generated by an element of positive norm.

Kummer proved that if p divides $h_2(p) = h'(p)$, then p divides $h^*(p)$. Using this he was able to use the first factor $h_1(p)$, to determine whether a prime is regular ($p \nmid h(p)$) or irregular ($p \mid h(p)$). This generalizes as follows.

Theorem 2.13. *(Kummer Criterion) Let F be a totally real algebraic number field and let p be an odd prime. Suppose that adjoining a pth root of unity of a root of unity in $F\mathbb{Q}(\zeta_p)$ to $F\mathbb{Q}(\zeta_p)$ never gives an unramified extension of $F\mathbb{Q}(\zeta_p)$ of degree p.*
If p divides $h(F)$, then p also divides $h(F\mathbb{Q}(\zeta_p))/h(F\mathbb{Q}(\zeta_p)^+)$.

Proof. Let $K = F\mathbb{Q}(\zeta_p)$ and $K' = F\mathbb{Q}(\zeta_p)^+$.
By Theorem 2.5, $h(F)$ divides $h(K')\,|K' : F|$ so if p divides $h(F)$, then p divides $h(K')$ or $|K' : F|$.



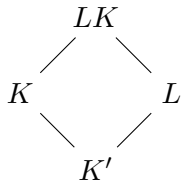
Suppose $p \mid |K' : F|$, then by the Tower Law,

$$|K' : F||F : \mathbb{Q}| = \tfrac{1}{2}(p-1)|K' : \mathbb{Q}(\zeta_p)^+|$$

so p must divide $|K' : \mathbb{Q}(\zeta_p)|/|F : \mathbb{Q}|$ and hence $p|F : \mathbb{Q}|$ must divide $|K' : \mathbb{Q}(\zeta_p)^+|$.
This is a contradiction as $|K' : \mathbb{Q}(\zeta_p)^+| = |F\mathbb{Q}(\zeta_p)^+ : \mathbb{Q}(\zeta_p)^+| = |F : \mathbb{Q}(\zeta_p)^+ \cap F|$ and $|F : \mathbb{Q}(\zeta_p)^+ \cap F| \leq |F : \mathbb{Q}|$. Thus $p \nmid |K' : F|$ and so $p \mid h(K')$.
Now K' has a cyclic, unramified (totally real) extension L of degree p.

Note. Clearly $K = F\mathbb{Q}(\zeta_p) = K'(\zeta_p)$, and since ζ_p satisfies $x^2 - \left(\zeta_p + \zeta_p^{-1}\right) x + 1 \in K'[x]$ and $\zeta_p \notin K'$. It follows that $|K : K'| = 2$.

Observe that L and K are both abelian extensions of K', and $L \cap K = K'$ since $K' \subseteq L \cap K \subseteq L$ and so $|L \cap K : K'| = 1$ or p. If $|L \cap K : K'| = p$ then $L \cap K = L$ and so $L \subseteq K$. Thus $K' \subseteq L \subseteq K$ and $|L : K'| = p$ divides $|K : K'| = 2$, which contradicts p being an odd prime.



It follows that LK/K' is a cyclic extension of degree $2p$.
By the Fundamental theorem of Galois theory, LK/L is Galois of degree p.

Let s be a generator of $Gal(LK/K)$ and J an automorphism of LK induced by complex conjugation, so $sJ = Js$ and this generates $Gal(LK/K')$. As LK/K is a Galois extension, $Gal(LK/K) \simeq \mathbb{Z}/p\mathbb{Z}$ and $\zeta_p \in K$, by results Kummer theory (see [4, p.58] for details) $LK = K\left(a^{1/p}\right)$ with $(a^{1/p})^p = a \in K$.

Let $\alpha = a^{1/p}$ be a fixed pth root of a. Let $(Ja)^{1/p} = J\alpha$. Now $s(\alpha) = \zeta_1\alpha$ and $s(J\alpha) = \zeta_2(J\alpha)$, where ζ_1, ζ_2 are primitive p-th roots of unity.(since s generates the Galois group of LK/K and hence it permutes the roots of $x^p - a \in K[x]$).
Then $\zeta_2(J\alpha) = s(J\alpha) = J(s\alpha) = J(\zeta_1\alpha) = \bar{\zeta_1}(J\alpha)$, so it follows

$$s(\alpha J\alpha) = (s\alpha)(sJ\alpha) = (\zeta_1\alpha)\left(\bar{\zeta_1}J\alpha\right) = \alpha J\alpha$$

so $a(Ja)$ is a pth power in K.
Let $b = a/Ja = a^2/aJa$. Then

$$LK = K(\alpha) = K\left(\alpha^2\right) = K\left(b^{1/p}\right)$$

Consider the ideal (b) generated by b in K. Then

$$(b) = \mathfrak{b}^p$$

for some fractional ideal $\mathfrak{b}$ of K, since LK/K is unramified. Also $bJb = 1$ so $J\mathfrak{b} = \mathfrak{b}^{-1}$. The ideal class $[\mathfrak{b}]$ of $\mathfrak{b}$ is in the kernel of the norm map $N : C(K) \longrightarrow C(K')$.

Remark. The norm map is surjective in this case, since by Theorem 2.1 the surjectivity of N is equivalent to proving that

$$\text{for any unramified abelian extension } H \text{ of } K',\ H \cap K = K'$$

In this case, since $[K : K'] = 2$, for any unramified abelian extension H of K', either $K \cap H = K'$ or $K \cap H = K$. In the second case, $K \subset H$, so $K/K^{'}$ must be unramified, which is a contradiction since the infinite primes of K' ramify in K (as K' is totally real, but K is not)

If $\mathfrak{b}$ is not a principal ideal, then p will divide the order of the kernel of N, which by Theorem 2.1 is $h(K)/h(K')$, (since the norm map is surjective Theorem 2.1 applies) which is the required result.

If we had $\mathfrak{b} = (d)$ with $d \in K$, then

$$\mathfrak{b}^{2p} = \mathfrak{b}^p/(J\mathfrak{b})^p = (d/Jd)^p = (u)^p$$

where $u = d/Jd$.
Then $(b^2) = (u^p)$ so $v = u^p/b^2 = (d^p/a^2)/J(d^p/a^2)$ is a unit of K, all of whose conjugates have absolute value one. But then the unramified extension LK/K is just $K(v^{1/p})/K$ with v a root of unity in K, contrary to the hypothesis. □

Definition. Let E/F be an extension of number fields. We say that E/F has no capitulation if no non-principal ideal of F become principal in E. In other words, for any non principal ideal I of O_F, IO_E is not a principal ideal of O_E.

Theorem 2.14. *(Parity Check) Let E/F be a ramified quadratic extension of number fields with no capitulation. If 2 divides $h(F)$ then 2 also divides $h(E)/h(F)$.*
In particular, if $h'(m)$ is even then $h^*(m)$ is also even.

Proof. Suppose $c \in Cl(F)$ is such that $c^2 = 1$ and $c \neq 1$.
Note that the inclusion of $Cl(F)$ into $Cl(E)$ is injective, as no ideal class of a non-principal ideal maps onto the trivial class (of principal ideal) since no non principal ideal of F becomes principal in E.
Thus one can consider $c \in Cl(E)$, with $c \neq 1$.

Consider the norm map $N : Cl(E) \longrightarrow Cl(F)$.
If H is any unramified abelian extension of F, then $F \subseteq H \cap E \subseteq E$, and since E/F is a quadratic extension, either $H \cap E = F$ or $H \cap E = E$. In the latter case, $E \subseteq H$,

and so E/F is an unramified extension. This contradicts the initial assumptions, and so $H \cap E = F$. Therefore by Theorem 2.1, N is surjective.

In particular, $N(c) = c^2 = 1$ so $c \in \ker(N)$. Thus $\ker(N)$ must have even order.
By Theorem 2.1, the order of the kernel is $h(E)/h(F)$, and so this must be even.

In particular, $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)^+$ is ramified at the infinite primes, and a theorem of Kronecker, no non-principal ideal of $'\mathbb{Q}(\zeta_m)^+$ becomes principal in $\mathbb{Q}(\zeta_m)$, so the above applies directly to this extension. □

Theorem 2.15. *(Cyclotomic spiuegelungsatz) Let p be any prime number and let M be the least common multiple of m and p. If p divided $h'(m)$, then p also divides $h^*(M)$.*

Proof. If $p = 2$, then $\mathbb{Q}(\zeta_m = \mathbb{Q}(\zeta_M)$ so by Theorem 2.14, if $p|h'(m)$ then $p|h^*(m)$.

Suppose p is an odd prime.
If $M = m$, then $h^*(M) = h^*(m)$, and so by Theorem 2.13 if p divides $h'(m) = h'(M)$ then p divides $h^*(m) = h^*(M)$.
If $m = p$, the results also follows from applying Theorem2.13 directly.
If p does not divide m, then by Corollary 2.7, $h'(m)|\ h'(M)$ and so, $p|\ h'(m)$ implies $p|\ h'(M)$. Then by Theorem 2.13 p divides $h^*(M)$. □

3 Class Numbers and $\mathbb{Z}_p$ extensions

This section will focus on the class numbers of layers of $\mathbb{Z}_p$-extensions. After a brief overview of some basic facts on these extensions, there will a discussion on some well known classical results on the class numbers as well as some more recent results.

3.1 Basic Facts

What follows is a brief introduction to the theory of $\mathbb{Z}_p$ -extensions. Many results will be stated without proof and details can found in [17, p.265] and [3].

Definition. Let K be a number field and p any rational prime. A $\mathbb{Z}_p$-extension of K is a Galois extension K_∞/K with $Gal\,(K_\infty/K) \simeq \mathbb{Z}_p$, where $\mathbb{Z}_p$ is the additive group of p-adic integers.

In general $\mathbb{Z}_p$-extensions exist.

Let U be the group of all p^nth roots of unity in $\mathbb{C}$, for all $n \geqslant 0$. Let P be the cyclotomic field of pth roots of unity when $p \neq 2$, and the cyclotomic field of 4th roots of unity if $p = 2$. Define

$$P_\infty = P(U)$$

Then P_∞/P is a $\mathbb{Z}_p$-extension.

Note. The field P_∞ has a unique subfield $\mathbb{Q}_\infty$ such that

$$P\mathbb{Q}_\infty = P_\infty \text{ and } P \cap \mathbb{Q}_\infty = \mathbb{Q}$$

Notably $\mathbb{Q}_\infty/\mathbb{Q}$ is also a $\mathbb{Z}_p$ -extension. This is known as the Cyclotomic $\mathbb{Z}_p$-extension of the rational numbers (see [3] for more details on this construction).

Moreover, any number field K has a $\mathbb{Z}_p$ extension.
Define $K_\infty = K\mathbb{Q}_\infty$. Then K_∞/K is a $\mathbb{Z}_p$-extension. This is often referred to as the Cyclotomic $\mathbb{Z}_p$-extension of K.

It is also possible to regard a $\mathbb{Z}_p$-extension as a sequence of fields. The details of this follow from the proposition below.

Proposition 3.1. *Let K_∞/K be a $\mathbb{Z}_p$-extension. Then for each $n \geqslant 0$, there exists a unique field K_n, with K_n/K an extension of degree p^n. What is more, these K_n (and K_∞) are the only intermediate fields of K_∞/K.*

Proof. By the Fundamental theorem of Galois theory (see [11, p.159] for details) there is a one to one correspondence between the intermediate fields of the extension K_∞/K and the closed subgroups of $Gal\,(K_\infty/K) \simeq \mathbb{Z}_p$. Any non-trivial closed subgroup of $\mathbb{Z}_p$ is of the form $p^n\mathbb{Z}_p$ for some $n > 0$. Taking $K_n = K_\infty^{p^n\mathbb{Z}_p}$ the result follows. □

This shows that for any $\mathbb{Z}_p$-extension K_∞/K there exists a sequence of fields

$$K = K_0 \subset K_1 \subset ... \subset K_\infty = \cup_{i=0}^{\infty} K_i$$

with $Gal\,(K_n/K) \simeq \mathbb{Z}/p^n\mathbb{Z}$ for each $n \geq 0$.

The following two results provide some information on how primes ramify in $\mathbb{Z}_p$-extensions. The notion of ramification in an infinite extension is consistent with ramification in finite extensions, more details can be found in [17, p.393]. The propositions below can be found in both [17, p.265] and [3]. The authors have different approaches to proving them. Whilst Washington uses various results from class field theory, Iwasawa has a more elementary approach and uses observations from his detailed study of the structure of $\mathbb{Z}_p$-extensions (which can also be found in [3]).

Proposition 3.2. *Let K_∞/K be a $\mathbb{Z}_p$-extension and let $\tilde{q}$ be any prime (including infinite primes) of K which does not lie above p. Then K_∞/K is unramified at $\tilde{q}$.*

More specifically, $\mathbb{Z}_p$-extensions are unramified outside of p.

Proposition 3.3. *Let K_∞/K be a $\mathbb{Z}_p$-extension. Then at least one prime ramifies in the extension. Moreover, there exists $n \geq 0$ such that every prime which ramifies in K_∞/K_n is totally ramified.*

Note. It is possible to have K_∞/K_n unramified for some $n \geq 0$.

As shown above, any number field K has at least one $\mathbb{Z}_p$-extension, namely the cyclotomic $\mathbb{Z}_p$-extension of K. However, there could be more. An interesting problem is to determine how many such extensions exist for a given number field.

Let E denote the group of units of K which are congruent to 1 modulo every prime $\tilde{q}$ of K lying above p. Let $\bar{E}$ be its closure. Then $\bar{E}$ is a $\mathbb{Z}_p$ module.
Washington proved the following.

Theorem 3.4. *Suppose that the $\mathbb{Z}_p$-rank of $\bar{E}$ is $r_1 + r_2 - 1 - \delta$ for some $\delta \geq 0$ (where (r_1, r_2) is the signature of K). Then there are $r_2 + 1 + \delta$ independent $\mathbb{Z}_p$-extensions of K.*

There is also a well-known conjecture of Leopoldt regarding the $\mathbb{Z}_p$-rank of $\bar{E}$.
Conjecture 3.5. *(Leopoldt) The $\mathbb{Z}_p$ rank of $\bar{E}$ is $r_1 + r_2 - 1$.*

In fact, this has been proved for abelian number fields.
Remark. From the two results above, it is also clear that the cyclotomic $\mathbb{Z}_p$ -extension of $\mathbb{Q}$ is the only possible $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

3.2 Class number of $\mathbb{B}_{p,n}$

Let $\mathbb{B}_{p,n}$ denote the nth layer of the cyclotomic $\mathbb{Z}_p$ extensions of $\mathbb{Q}$.

When $p \neq 2$, $\mathbb{B}_{p,n}$ is the unique real subfield of $\mathbb{Q}\left(\zeta_{p^{n+1}}\right)$ of degree p^n over $\mathbb{Q}$. For $p = 2$, $\mathbb{B}_{2,n} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{2^{n+2}}\right)\right)$.

Let $h_{p,n}$ denote the class number of $\mathbb{B}_{p,n}$.

The study of these $h_{p,n}$ began with Weber, who studied $\mathbb{Z}_2$-extensions. One of his first significant results is the following.

Theorem 3.6. *(Weber) For all positive integers n, $h_{2,n}$ is odd.*

Weber went further and conjectured that in fact all $h_{2,n}$ are trivial.

Conjecture 3.7. *(Weber's class number problem) For all positive integers n, $h_{2,n} = 1$.*

Weber's results was generalised by Iwasawa.

Theorem 3.8. *(Iwasawa) For all positive integers n and primes p, $h_{p,n}$ is not divisible by p.*

In fact, in [3] Iwasawa proved a much stronger result on the class number of the nth layer of any $\mathbb{Z}_p$-extension of a number field K for any n and p.

Theorem 3.9. *(Iwasawa) Let K_∞/K be a $\mathbb{Z}_p$-extension. Suppose that K_n is unique subfield of K_∞ with K_n/K a degree p^n extension. Let p^{e_n} be the exact power of p dividing the class number of K_n. Then there exist integers $\lambda \geq 0$, $\mu \geq 0$ and ν, all independent of n, and an integer n_0 such that*

$$e_n = \lambda n + \mu p^n + \nu \text{ for all } n \geq n_0$$

In [16] Washington proved the following deep results which applies for any prime $l \neq p$.

Theorem 3.10. *(Washington) Let k be an abelian number field and k_∞/k the cyclotomic $\mathbb{Z}_p$-extension of k. If $l \neq p$ is a prime and l^{f_n} the exact power of l dividing $h_{p,n}$.*
Then f_n is bounded independent of n. In fact, f_n is constant for large n.

Returning to our discussion of $h_{p,n}$, it is important to note that the exact class number has been calculated for very few of the $\mathbb{B}_{p,n}$s. This is mainly due to their large degree and discriminant. Notably, all the known class numbers are 1. A table summarising the known class numbers can be found in [9].

Naturally one can ask whether all $\mathbb{B}_{p,n}$ have class number 1. In fact, this is a well known conjecture.

Conjecture 3.11. *For any prime p and positive integer n, the class number of $\mathbb{B}_{p,n}$ is 1*

There are various ways of approaching this problem, one of which will be explored in the next subsection.

3.3 Class Numbers of $\mathbb{B}_{13,1}$, $\mathbb{B}_{17,1}$ and $\mathbb{B}_{19,1}$

In [9] Miller developed new a technique to calculate the class number of some $\mathbb{B}_{p,n}$'s. Miller uses a bound on the class number (similar to those developed in section 1) and some general results on the class group of the number field (similar to those seen in section 2) to determine the exact value of the class number.

In [9], Miller proves that $\mathbb{B}_{13,1}$, $\mathbb{B}_{17,1}$ and $\mathbb{B}_{19,1}$ all have class number 1. We will follow [9] to give a sketch of the proof of Miller's main result.

Theorem 3.12. *(Miller) The class number of $\mathbb{B}_{13,1}$, $\mathbb{B}_{17,1}$ and $\mathbb{B}_{19,1}$ is 1*

Recall that Miller gives the following unconditional upper bound for class numbers.

Lemma 3.13. *Let K be a totally real field of degree n, and let*

$$F(x) = \frac{e^{-\left(\frac{x}{c}\right)^2}}{cosh\left(\frac{x}{2}\right)}$$

for a positive constant c. Suppose S is a subset of the prime integers which totally split into principal ideals of K. Let

$$B = \frac{\pi}{2} + \gamma + log8\pi - logrd(K) - \int_0^\infty \frac{1-F(x)}{2}\left(\frac{1}{sinh\frac{x}{2}} + \frac{1}{cosh\frac{x}{2}}\right)dx + 2\sum_{p\in S}\sum_{m=1}^{\infty}\frac{logp}{p^{\frac{m}{2}}}F(m\ logp)$$

If $B > 0$ then we have an upper bound for the class number h of K

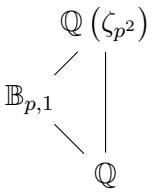
$$\boxed{h < \frac{2c\sqrt{\pi}}{nB}}$$

All the terms in the definition of B can be calculated explicitly once the set S and the constant c are specified.
Once sufficiently many primes to include in our set S are found, c can be determined analytically and the lemma is used to establish an upper bound for the class number.

After the bound is established, the following version of the Rank Theorem 2.12 can be used to determine the exact class number.

Theorem 3.14. *(A special case of the Rank theorem) Let K be a number field of prime degree p over the rationals. If a prime q, $q \neq p$ divides the class number of K, then q^f divides the class number, where f is the order of q modulo p.*

To find sufficiently many primes for the S, an integral basis is often useful, as it can be used to find elements of prime norm (as illustrated in 1.17).
The field $\mathbb{B}_{p,1}$ is the degree p subfield of the cyclotomic field of conductor p^2.



If σ generates the Galois group of the cyclotomic field, then the Galois subgroup generated by σ^p fixes the subfield $\mathbb{B}_{p,1}$.

Let $\zeta = \exp\left(\frac{2\pi i}{p^2}\right)$. Given the generator σ, define $b_0 = 1$ and $b_j = \sum_{k=0}^{p-2}\zeta^{\sigma^{kp(j-1)}}$ for $1 \leq j \leq p-1$. Then

$$\{b_0, b_1. \ldots, b_{p-1}\}$$

is an integral basis.
Note. This basis is dependent of the choice of generator σ.

Proposition 3.15. *The class number of* $\mathbb{B}_{13,1}$ *is 1.*

Proof. (Sketch) The root discriminant of $\mathbb{B}_{13,1}$ is approximately 113.9, which is too large for Odlyzko's unconditional discriminant bounds to be used.
The Galois group of the cyclotomic field of conductor 169 is generated by σ, where $\sigma(\zeta) = \zeta^2$ with $\zeta = \exp\left(\frac{2\pi i}{169}\right)$. Using this, an integral basis $\{b_0, b_1, \ldots, b_{12}\}$ can be defined.

Searching over the sparse vectors of the integral basis, the elements

$$b_0 - b_1 - b_2 - b_3 - b_6 - b_7 - b_8 \text{ and } b_0 - b_1 - b_2 - b_4 + b_{12}$$

have norms 19 and 23 respectively.

Thus primes 19 and 23 totally split into principal ideals.
Taking $S = \{19, 23\}$ and $c = 10$, an upper bound for the class number can be calculated.

$$h(\mathbb{B}_{13,1}) \leq 7$$

Notably 2^{f_2}, 3^{f_3}, 5^{f_5} and 7^{f_7} (where f_q is the order of q modulo 13) are all greater than 7.
Using the Rank Theorem 3.14, $h(\mathbb{B}_{13,1}) = 1$ □

Proposition 3.16. *The class number of* $\mathbb{B}_{17,1}$ *is 1.*

Proof. (Sketch) Let b_i be integral basis vectors as before.
Let T be the set of elements of the form

$$x = a_1 b_{j_1} + ... + a_{12} b_{j_{12}}$$

where $0 \leq j_1 < ... < j_{12} \leq 17$ and $a_j \in \{-1, 0, 1\}$ for all $1 \leq j \leq 12$.
Let U be the set of their norm up to 10^{12}.

$$U = \{N(x) \mid x \in T, N(x) < 10^{12}\}$$

Let S_1 be the set of prime norms

$$S_1 = \{p \mid p \in U, p \text{ prime}\}$$

Define S_2 to be

$$S_2 = \{p \mid pq \in U, p \text{ prime}, p \notin S_1, q \in S_1\}$$

Note. If $N(x) = pq$, $N(y) = q$ for $x, y \in O_K$, then: $\frac{x}{y^\sigma} \in O_K$ with norm p, for some Galois automorphism σ

Taking $S = S_1 \cup S_2 \setminus \{17\}$ and $c = 22$ in (3.13), the class number is bounded by 5

$$h(\mathbb{B}_{17,1}) \leq 5$$

Since 2^{f_2}, 3^{f_3} and 5^{f_5} (where f_q is the order of q modulo 17) are all greater than 5, by the Rank Theorem 3.14 the class number is 1. □

Proposition 3.17. *The class number of* $\mathbb{B}_{19,1}$ *is 1.*

Proof. (Sketch) A similar method as in the previous proposition is used to generate S. Taking $c = 40$, the class number can be bounded by 38.

$$h(\mathbb{B}_{19,1}) \leq 38$$

By Theorem 3.8, 19 does not divide $h(\mathbb{B}_{19,1})$.
For the any other prime $q < 38$, the Rank theorem shows that $q \nmid h(\mathbb{B}_{19,1})$.
Thus $h(\mathbb{B}_{19,1}) = 1$. □

References

[1] Henri Cohen. *Advanced topics in computational number theory*, volume 193. Springer Science & Business Media, 2012.

[2] David A Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[3] Kenkichi Iwasawa. On zl-extensions of algebraic number fields. *Annals of Mathematics*, pages 246–326, 1973.

[4] Helmut Koch. *Algebraic number theory*, volume 62. Springer Science & Business Media, 2012.

[5] Joachim König, Danny Neftin, and Jack Sonn. Unramified extensions over low degree number fields. *Journal of Number Theory*, 2019.

[6] John Myron Masley. Class numbers of real cyclic number fields with small conductor. *Compositio Mathematica*, 37(3):297–319, 1978.

[7] John Miller. Real cyclotomic fields of prime conductor and their class numbers. *Mathematics of Computation*, 84(295):2459–2469, 2015.

[8] John C Miller. Class numbers of totally real fields and applications to the weber class number problem. *arXiv preprint arXiv:1405.1094*, 2014.

[9] John C Miller. Class numbers in cyclotomic zp-extensions. *Journal of Number Theory*, 150:47–73, 2015.

[10] James S Milne. Fields and galois theory. *Courses Notes, Version*, 4, 2003.

[11] Patrick Morandi. Galois theory. In *Field and Galois Theory*. Springer, 1996.

[12] Trajano Pires da Nóbrega Neto, J Carmelo Interlando, and José Othon Dantas Lopes. On computing discriminants of subfields of (ζp r). *Journal of Number Theory*, pages 319–325, 2002.

[13] Andrew M Odlyzko. Some analytic estimates of class numbers and discriminants. *Inventiones mathematicae*, 29(3):275–286, 1975.

[14] René Schoof. Class numbers of real cyclotomic fields of prime conductor. *Mathematics of computation*, 72(242):913–937, 2003.

[15] Harold M Stark. Some effective cases of the brauer-siegel theorem. *Inventiones mathematicae*, 23(2):135–152, 1974.

[16] Lawrence Washington. The non-p-part of the class number in a cyclotomic zp-extension. *Invent. math*, 49(1):87–97, 1978.

[17] Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science & Business Media, 1997.