Verifying $p$-valuation of class numbers

Yinan Zhang

MAGMA group, The University of Sydney

26 July 2013
<table>
<thead>
<tr>
<th>1</th>
<th>Introduction and background</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Class groups</td>
</tr>
<tr>
<td></td>
<td>Current algorithms</td>
</tr>
<tr>
<td></td>
<td>$p$-divisibility approaches</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>$p$-adic computation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Background theory</td>
</tr>
<tr>
<td></td>
<td>Implementation in Magma</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>Analysis and examples</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Complexity</td>
</tr>
<tr>
<td></td>
<td>Examples</td>
</tr>
</tbody>
</table>
If $K$ is a number field with ring of integers $O_K$, the set of fractional ideals of $O_K$ modulo principal fractional ideals, forms the (ideal) class group, $Cl_K$, of $K$.

- The class number, $h$, is the size of $Cl_K$.
- The extent of how much unique factorisation fails in $K$ is measured by $Cl_K$. 
If $K$ is a number field with ring of integers $O_K$, the set of fractional ideals of $O_K$ modulo principal fractional ideals, forms the (ideal) class group, $Cl_K$, of $K$.

The class number, $h$, is the size of $Cl_K$.

The extent of how much unique factorisation fails in $K$ is measured by $Cl_K$. 
Class groups

- If $K$ is a number field with ring of integers $O_K$, the set of fractional ideals of $O_K$ modulo principal fractional ideals, forms the (ideal) class group, $Cl_K$, of $K$.
- The class number, $h$, is the size of $Cl_K$.
- The extent of how much unique factorisation fails in $K$ is measured by $Cl_K$. 
Motivation: Is it possible to (unconditionally) compute only the \( p \)-part of the class group, or the \( p \)-valuation of the class number? We can use the existing algorithm for computing class groups, or specialised algorithms that compute only the \( p \)-valuation. However there are some issues with both of these.
Motivation: Is it possible to (unconditionally) compute only the $p$-part of the class group, or the $p$-valuation of the class number?

We can use the existing algorithm for computing class groups, or specialised algorithms that compute only the $p$-valuation. However there are some issues with both of these.
All current (classical) implementations to compute the class group are based on Buchmann’s subexponential algorithm, with some adaptations.

It makes use of the following formula:

**Theorem (Class Number Formula)**

Suppose $K$ is a number field with discriminant $D$, class number $h$, regulator $R$, and contains $w$ roots of unity, then

$$\lim_{s \to 1} (s - 1)\zeta_K(s) = \frac{2^r \cdot (2\pi)^s \cdot hR}{w \sqrt{|D|}}$$

where $\zeta_K(s)$ is the Dedekind zeta function.

An Euler product is used to compute the residue of the zeta function.
All current (classical) implementations to compute the class group are based on Buchmann’s subexponential algorithm, with some adaptations.

It makes use of the following formula:

\[
\lim_{s \to 1} (s - 1) \zeta_K(s) = \frac{2^r \cdot (2\pi)^s \cdot hR}{w \sqrt{|D|}}
\]

where \( \zeta_K(s) \) is the Dedekind zeta function.

An Euler product is used to compute the residue of the zeta function.
All current (classical) implementations to compute the class group are based on Buchmann’s subexponential algorithm, with some adaptations.

It makes use of the following formula:

**Theorem (Class Number Formula)**

*Suppose $K$ is a number field with discriminant $D$, class number $h$, regulator $R$, and contains $w$ roots of unity, then*

$$\lim_{s \to 1} (s - 1)\zeta_K(s) = \frac{2^r \cdot (2\pi)^s \cdot hR}{w \sqrt{|D|}}$$

*where $\zeta_K(s)$ is the Dedekind zeta function.*

An Euler product is used to compute the residue of the zeta function.
Current algorithms

- All current (classical) implementations to compute the class group are based on Buchmann’s subexponential algorithm, with some adaptations.
- It makes use of the following formula:

**Theorem (Class Number Formula)**

Suppose $K$ is a number field with discriminant $D$, class number $h$, regulator $R$, and contains $w$ roots of unity, then

$$\lim_{s \to 1} (s - 1)\zeta_K(s) = \frac{2^r \cdot (2\pi)^s \cdot hR}{w \sqrt{|D|}}$$

where $\zeta_K(s)$ is the Dedekind zeta function.

- An Euler product is used to compute the residue of the zeta function.
To compute $h$ and $R$, construct a set of prime ideals of norms up to $B$.

- From these ideals, generate a relation matrix $M$ from decomposing elements of $K$ into powers of ideals.
- The rows of $M$ are used to generate a subgroup of $Cl_K$ (depending on number of relations).
- The kernel vectors of $M$ provides generators for the unit group, used to compute $R$.
- $hR$ is verified with the previous formula. If not satisfied, more relations are needed.
To compute $h$ and $R$, construct a set of prime ideals of norms up to $B$.

From these ideals, generate a relation matrix $M$ from decomposing elements of $K$ into powers of ideals.

- The rows of $M$ are used to generate a subgroup of $Cl_K$ (depending on number of relations).
- The kernel vectors of $M$ provides generators for the unit group, used to compute $R$.
- $hR$ is verified with the previous formula. If not satisfied, more relations are needed.
To compute $h$ and $R$, construct a set of prime ideals of norms up to $B$.

From these ideals, generate a relation matrix $M$ from decomposing elements of $K$ into powers of ideals.

The rows of $M$ are used to generate a subgroup of $Cl_K$ (depending on number of relations).

The kernel vectors of $M$ provides generators for the unit group, used to compute $R$.

$hR$ is verified with the previous formula. If not satisfied, more relations are needed.
To compute $h$ and $R$, construct a set of prime ideals of norms up to $B$.

From these ideals, generate a relation matrix $M$ from decomposing elements of $K$ into powers of ideals.

The rows of $M$ are used to generate a subgroup of $Cl_K$ (depending on number of relations).

The kernel vectors of $M$ provides generators for the unit group, used to compute $R$.

$hR$ is verified with the previous formula. If not satisfied, more relations are needed.
Current algorithms

- To compute $h$ and $R$, construct a set of prime ideals of norms up to $B$.
- From these ideals, generate a relation matrix $M$ from decomposing elements of $K$ into powers of ideals.
- The rows of $M$ are used to generate a subgroup of $Cl_K$ (depending on number of relations).
- The kernel vectors of $M$ provides generators for the unit group, used to compute $R$.
- $hR$ is verified with the previous formula. If not satisfied, more relations are needed.
There are two main problems with this algorithm, if one wants unconditional results:

1. The product representation of the residue converges only under the assumption of the Generalised Riemann Hypothesis (GRH).

2. Choosing the value of $B$ to certify the computation.
   - If GRH is assumed, one can use the Bach bound of $B = 12 \log^2(|D|)$, yielding a subexponential result.
   - For unconditional result, a bound (eg Minkowski) of the order $\sqrt{|D|}$ needs to be used, which is impractical for larger values of $D$. 
There are two main problems with this algorithm, if one wants unconditional results:

1. The product representation of the residue converges only under the assumption of the Generalised Riemann Hypothesis (GRH).

2. Choosing the value of $B$ to certify the computation.
   - If GRH is assumed, one can use the Bach bound of $B = 12 \log^2(|D|)$, yielding a subexponential result.
   - For unconditional result, a bound (eg Minkowski) of the order $\sqrt{|D|}$ needs to be used, which is impractical for larger values of $D$. 
There are two main problems with this algorithm, if one wants unconditional results:

1. **The product representation of the residue converges only under the assumption of the Generalised Riemann Hypothesis (GRH).**

2. **Choosing the value of $B$ to certify the computation.**

   - If GRH is assumed, one can use the Bach bound of $B = 12 \log^2 (|D|)$, yielding a subexponential result.
   - For unconditional result, a bound (eg Minkowski) of the order $\sqrt{|D|}$ needs to be used, which is impractical for larger values of $D$. 
There are two main problems with this algorithm, if one wants unconditional results:

1. The product representation of the residue converges only under the assumption of the Generalised Riemann Hypothesis (GRH).

2. Choosing the value of $B$ to certify the computation.
   - If GRH is assumed, one can use the Bach bound of $B = 12 \log^2(|D|)$, yielding a subexponential result.
   - For unconditional result, a bound (eg Minkowski) of the order $\sqrt{|D|}$ needs to be used, which is impractical for larger values of $D$. 
There are two main problems with this algorithm, if one wants unconditional results:

1. The product representation of the residue converges only under the assumption of the Generalised Riemann Hypothesis (GRH).

2. Choosing the value of $B$ to certify the computation.
   - If GRH is assumed, one can use the Bach bound of $B = 12 \log^2(|D|)$, yielding a subexponential result.
   - For unconditional result, a bound (eg Minkowski) of the order $\sqrt{|D|}$ needs to be used, which is impractical for larger values of $D$. 

Yinan Zhang
Verifying $p$-valuation of class numbers

Sydney
Number theoretical methods:

- G Gras and M-N Gras: Saturates the group of cyclotomic units at $p$ ("devissage") to deduce the $p$-valuation of the class number. Applicable only to totally real abelian extensions of $\mathbb{Q}$ with prime degree.

- Hakkarainen: Compute class number by finding small prime factors. Combines “devissage” with work on cyclotomic units. Applicable to totally real abelian extensions of $\mathbb{Q}$ where $p \neq 2$ and does not divide the degree.
Number theoretical methods:

- G Gras and M-N Gras: Saturates the group of cyclotomic units at $p$ (“devissage”) to deduce the $p$-valuation of the class number. Applicable only to totally real abelian extensions of $\mathbb{Q}$ with prime degree.

- Hakkarainen: Compute class number by finding small prime factors. Combines “devissage” with work on cyclotomic units. Applicable to totally real abelian extensions of $\mathbb{Q}$ where $p \neq 2$ and does not divide the degree.
Group theoretical method:
- Aoki and Fukuda: Compute $p$-part of class group by explicitly obtaining the annihilators of some specific ideals of the number field in question. Same restrictions.
- At least for fields of degree $p$, genus theory tells us the set of fields with $h = p$ has positive measure.
- Even for simple examples like $\mathbb{Q}[\sqrt{40}]$, neither methods can show $h = 2$. 

Yinan Zhang
Verifying $p$-valuation of class numbers
Group theoretical method:

- Aoki and Fukuda: Compute $p$-part of class group by explicitly obtaining the annihilators of some specific ideals of the number field in question. Same restrictions.

- At least for fields of degree $p$, genus theory tells us the set of fields with $h = p$ has positive measure.

- Even for simple examples like $\mathbb{Q}[^{\sqrt{40}}]$, neither methods can show $h = 2$. 
- Group theoretical method:
  - Aoki and Fukuda: Compute $p$-part of class group by explicitly obtaining the annihilators of some specific ideals of the number field in question. Same restrictions.
  - At least for fields of degree $p$, genus theory tells us the set of fields with $h = p$ has positive measure.
  - Even for simple examples like $\mathbb{Q}[\sqrt{40}]$, neither methods can show $h = 2$. 

Yinan Zhang
Sydney

Verifying $p$-valuation of class numbers
We propose a new algorithm, based on the following formula (a \( p \)-adic analogy of CNF)

**Theorem**

Let \( K \) be a totally real abelian field of degree \( n \), with \( p \)-adic regulator \( R_p \) and a group of associated Dirichlet characters \( X \), then

\[
\frac{2^{n-1} h R_p}{\sqrt{D}} = \prod_{\chi \in X, \chi \neq 1} \left( 1 - \frac{\chi(p)}{p} \right)^{-1} L_p(1, \chi)
\]

There are two closed formulae that can be used to compute \( L_p(1, \chi) \).
We propose a new algorithm, based on the following formula (a $p$-adic analogy of CNF)

**Theorem**

Let $K$ be a totally real abelian field of degree $n$, with $p$-adic regulator $R_p$ and a group of associated Dirichlet characters $X$, then

$$\frac{2^{n-1}hR_p}{\sqrt{D}} = \prod_{\chi \in X, \chi \neq 1} \left(1 - \frac{\chi(p)}{p}\right)^{-1} L_p(1, \chi)$$

There are two closed formulae that can be used to compute $L_p(1, \chi)$. 

Yinan Zhang
Verifying $p$-valuation of class numbers
We propose a new algorithm, based on the following formula (a $p$-adic analogy of CNF)

**Theorem**

Let $K$ be a totally real abelian field of degree $n$, with $p$-adic regulator $R_p$ and a group of associated Dirichlet characters $X$, then

$$\frac{2^{n-1}hR_p}{\sqrt{D}} = \prod_{\chi \in X \atop \chi \neq 1} \left(1 - \frac{\chi(p)}{p}\right)^{-1} L_p(1, \chi)$$

There are two closed formulae that can be used to compute $L_p(1, \chi)$. 
Theorem (Iwasawa)

\[ L_p(1, \chi) = - \left( 1 - \frac{\chi(p)}{p} \right) \sum_{a=1}^{f_\chi} \frac{\chi(a) \zeta^a}{f_\chi} \sum_{i=1}^{f_\chi} \chi(i) \log_p(1 - \zeta^{-i}) \]

where \( \chi \) has conductor \( f_\chi \) and \( \zeta \) is a \( f_\chi \)-th root of unity.

Theorem (Cohen)

\[ L_p(1, \chi) = \sum_{0 \leq a < m \atop (a,p)=1} \chi(a) \left( - \frac{\log_p(a)}{m} + \sum_{j \geq 1} (-1)^j \frac{m^{j-1} B_j}{a^j j} \right) \]

where \( B_j \) is the \( j \)-th Bernoulli number and \( m = \text{lcm}(f_\chi, p) \) or \( \text{lcm}(f_\chi, 4) \) if \( p = 2 \).
Background theory

**Theorem (Iwasawa)**

\[
L_p(1, \chi) = - \left(1 - \frac{\chi(p)}{p}\right) \sum_{a=1}^{f_\chi} \frac{\chi(a) \zeta^a}{f_\chi} \sum_{i=1}^{f_\chi} \overline{\chi(i)} \log_p(1 - \zeta^{-i})
\]

where \(\chi\) has conductor \(f_\chi\) and \(\zeta\) is a \(f_\chi\)-th root of unity.

**Theorem (Cohen)**

\[
L_p(1, \chi) = \sum_{0 \leq a < m} \chi(a) \left( -\frac{\log_p(a)}{m} + \sum_{j \geq 1} (-1)^j \frac{m^{j-1} B_j}{a^j} \right)
\]

where \(B_j\) is the \(j\)-th Bernoulli number and \(m = \text{lcm}(f_\chi, p)\) or \(\text{lcm}(f_\chi, 4)\) if \(p = 2\).

Yinan Zhang

Verifying \(p\)-valuation of class numbers
$L_p(1, \chi)$ is computed using either formula by the following method:

1. Find conductor $f$ of $K$. Then $K \subseteq \mathbb{Q}[\zeta_f]$.
2. Construct $E_p$, an extension of $\mathbb{Q}_p$ containing $f$-th (and $n$-th) roots of unity.
4. Construct group of Dirichlet characters of conductor $f$ with order $n$, using $\zeta_n$.
5. Select the appropriate characters using class field theory.
$L_p(1, \chi)$ is computed using either formula by the following method:

1. Find conductor $f$ of $K$. Then $K \subseteq \mathbb{Q}[\zeta_f]$.

2. Construct $E_p$, an extension of $\mathbb{Q}_p$ containing $f$-th (and $n$-th) roots of unity.


4. Construct group of Dirichlet characters of conductor $f$ with order $n$, using $\zeta_n$.

5. Select the appropriate characters using class field theory.
\[ L_p(1, \chi) \] is computed using either formula by the following method:

1. Find conductor \( f \) of \( K \). Then \( K \subseteq \mathbb{Q}[\zeta_f] \).
2. Construct \( E_p \), an extension of \( \mathbb{Q}_p \) containing \( f \)-th (and \( n \)-th) roots of unity.
3. Using Hensel lifting, construct \( f \)-th (and \( n \)-th) roots of unity.
4. Construct group of Dirichlet characters of conductor \( f \) with order \( n \), using \( \zeta_n \).
5. Select the appropriate characters using class field theory.
\( L_p(1, \chi) \) is computed using either formula by the following method:

1. Find conductor \( f \) of \( K \). Then \( K \subseteq \mathbb{Q}[\zeta_f] \).
2. Construct \( E_p \), an extension of \( \mathbb{Q}_p \) containing \( f \)-th (and \( n \)-th) roots of unity.
3. Using Hensel lifting, construct \( f \)-th (and \( n \)-th) roots of unity.
4. Construct group of Dirichlet characters of conductor \( f \) with order \( n \), using \( \zeta_n \).
5. Select the appropriate characters using class field theory.
$L_p(1, \chi)$ is computed using either formula by the following method:

1. Find conductor $f$ of $K$. Then $K \subseteq \mathbb{Q}[\zeta_f]$.
2. Construct $E_p$, an extension of $\mathbb{Q}_p$ containing $f$-th (and $n$-th) roots of unity.
4. Construct group of Dirichlet characters of conductor $f$ with order $n$, using $\zeta_n$.
5. Select the appropriate characters using class field theory.
\( L_p(1, \chi) \) is computed using either formula by the following method:

1. Find conductor \( f \) of \( K \). Then \( K \subseteq \mathbb{Q}[\zeta_f] \).
2. Construct \( E_p \), an extension of \( \mathbb{Q}_p \) containing \( f \)-th (and \( n \)-th) roots of unity.
3. Using Hensel lifting, construct \( f \)-th (and \( n \)-th) roots of unity.
4. Construct group of Dirichlet characters of conductor \( f \) with order \( n \), using \( \zeta_n \).
5. Select the appropriate characters using class field theory.
The power series for logarithm only converges in 

\[ U = \{ x \in \mathbb{C}_p \mid |x - 1|_p < 1 \}. \]

We can extend it based on the fact

\[ \mathbb{C}_p^\times \cong p^\mathbb{Q} \times \Omega \times U \]

where \( \Omega \) are the roots of unity \( \zeta_m, p \nmid m \), and every element in \( \mathbb{C}_p^\times \) has a unique decomposition.

However, this only works with 1-units \((1 + \pi \mathbb{Z}_{E_p})\) and its naive use on arbitrary elements of \( E_p \) requires extending \( E_p \).

We developed an alternative \( p \)-adic logarithm to overcome this.

Other optimisations were also introduced.
The power series for logarithm only converges in $U = \{ x \in \mathbb{C}_p \mid |x - 1|_p < 1 \}$.

We can extend it based on the fact

$$\mathbb{C}_p^\times \cong p^\mathbb{Q} \times \Omega \times U$$

where $\Omega$ are the roots of unity $\zeta_m$, $p \nmid m$, and every element in $\mathbb{C}_p^\times$ has a unique decomposition.

However, this only works with 1-units $(1 + \pi \mathbb{Z}_{E_p})$ and its naive use on arbitrary elements of $E_p$ requires extending $E_p$.

We developed an alternative $p$-adic logarithm to overcome this.

Other optimisations were also introduced.
• The power series for logarithm only converges in $U = \{x \in \mathbb{C}_p \mid |x - 1|_p < 1\}$.

• We can extend it based on the fact

$$\mathbb{C}_p^\times \cong p\mathbb{Q} \times \Omega \times U$$

where $\Omega$ are the roots of unity $\zeta_m$, $p \nmid m$, and every element in $\mathbb{C}_p^\times$ has a unique decomposition.

• However, this only works with 1-units $(1 + \pi\mathbb{Z}_{E_p})$ and its naive use on arbitrary elements of $E_p$ requires extending $E_p$.

• We developed an alternative $p$-adic logarithm to overcome this.

• Other optimisations were also introduced.

Yinan Zhang
Sydney

Verifying $p$-valuation of class numbers
The power series for logarithm only converges in $U = \{ x \in \mathbb{C}_p \mid |x - 1|_p < 1 \}$.

We can extend it based on the fact

$$\mathbb{C}_p^\times \cong p^\mathbb{Q} \times \Omega \times U$$

where $\Omega$ are the roots of unity $\zeta_m$, $p \nmid m$, and every element in $\mathbb{C}_p^\times$ has a unique decomposition.

However, this only works with 1-units $(1 + \pi \mathbb{Z}_{E_p})$ and its naive use on arbitrary elements of $E_p$ requires extending $E_p$.

We developed an alternative $p$-adic logarithm to overcome this.

Other optimisations were also introduced.
The power series for logarithm only converges in $U = \{ x \in \mathbb{C}_p \mid |x - 1|_p < 1 \}$.

We can extend it based on the fact

$$\mathbb{C}_p^\times \cong p^\mathbb{Q} \times \Omega \times U$$

where $\Omega$ are the roots of unity $\zeta_m$, $p \nmid m$, and every element in $\mathbb{C}_p^\times$ has a unique decomposition.

However, this only works with 1-units $(1 + \pi \mathbb{Z}_{E_p})$ and its naive use on arbitrary elements of $E_p$ requires extending $E_p$.

We developed an alternative $p$-adic logarithm to overcome this.

Other optimisations were also introduced.
The characters required have conductor $f$ and order a factor of $[K : \mathbb{Q}]$.

Considering the projection $\phi$:

$$(\mathbb{Z}/f\mathbb{Z})^\times \cong \text{Gal}(\mathbb{Q}[\zeta_f]/\mathbb{Q}) \to \text{Gal}(K/\mathbb{Q}) \cong Cl_f/H$$

where $Cl_f$ is the ray class group modulo $f$, and $H$ the norm group of $K$.

By definition the characters associated with $K$ act trivially on $\text{Gal}(\mathbb{Q}[\zeta_f]/K)$, which is $\ker \phi \cong H$.

By calculating and testing on $H$ we can find the required characters.

Yinan Zhang

Verifying $p$-valuation of class numbers
The characters required have conductor $f$ and order a factor of $[K : \mathbb{Q}]$.

Considering the projection $\phi$:

$$(\mathbb{Z}/f\mathbb{Z})^\times \cong \text{Gal}(\mathbb{Q}[\zeta_f]/\mathbb{Q}) \rightarrow \text{Gal}(K/\mathbb{Q}) \cong Cl_f/H$$

where $Cl_f$ is the ray class group modulo $f$, and $H$ the norm group of $K$.

By definition the characters associated with $K$ act trivially on $\text{Gal}(\mathbb{Q}[\zeta_f]/K)$, which is $\ker \phi \cong H$.

By calculating and testing on $H$ we can find the required characters.
The characters required have conductor $f$ and order a factor of $[K : \mathbb{Q}]$.

Considering the projection $\phi$:

$$(\mathbb{Z}/f\mathbb{Z})^\times \cong \text{Gal}(\mathbb{Q}[\zeta_f]/\mathbb{Q}) \to \text{Gal}(K/\mathbb{Q}) \cong Cl_f/H$$

where $Cl_f$ is the ray class group modulo $f$, and $H$ the norm group of $K$.

By definition the characters associated with $K$ act trivially on $\text{Gal}(\mathbb{Q}[\zeta_f]/K)$, which is $\ker \phi \cong H$.

By calculating and testing on $H$ we can find the required characters.
The characters required have conductor $f$ and order a factor of $[K : \mathbb{Q}]$.

Considering the projection $\phi$:

$$(\mathbb{Z}/f\mathbb{Z})^\times \cong \text{Gal}(\mathbb{Q}[\zeta_f]/\mathbb{Q}) \to \text{Gal}(K/\mathbb{Q}) \cong Cl_f/H$$

where $Cl_f$ is the ray class group modulo $f$, and $H$ the norm group of $K$.

By definition the characters associated with $K$ act trivially on $\text{Gal}(\mathbb{Q}[\zeta_f]/K)$, which is $\ker \phi \cong H$.

By calculating and testing on $H$ we can find the required characters.
- $R_p$ is computed by finding a system of fundamental units, using existing methods.

- These make use of saturation techniques to find a $p$-maximal subgroup of the unit group, developed by Biasse and Fieker.

- Unlike the existing approach where this has to be done for all $p < B$, we only need to do so at a single $p$, since the units only need to have the correct valuation at $p$.

- This provides an unconditional result for the valuation of $h$ at $p$, which can then be used to compute or verify the $p$-part of $Cl_K$. 
- $R_p$ is computed by finding a system of fundamental units, using existing methods.

- These make use of saturation techniques to find a $p$-maximal subgroup of the unit group, developed by Biasse and Fieker.

- Unlike the existing approach where this has to be done for all $p < B$, we only need to do so at a single $p$, since the units only need to have the correct valuation at $p$.

- This provides an unconditional result for the valuation of $h$ at $p$, which can then be used to compute or verify the $p$-part of $\text{Cl}_K$. 

Yinan Zhang
Verifying $p$-valuation of class numbers
- $R_p$ is computed by finding a system of fundamental units, using existing methods.
- These make use of saturation techniques to find a $p$-maximal subgroup of the unit group, developed by Biasse and Fieker.
- Unlike the existing approach where this has to be done for all $p < B$, we only need to do so at a single $p$, since the units only need to have the correct valuation at $p$.
- This provides an unconditional result for the valuation of $h$ at $p$, which can then be used to compute or verify the $p$-part of $Cl_K$. 
\( R_p \) is computed by finding a system of fundamental units, using existing methods.

- These make use of saturation techniques to find a \( p \)-maximal subgroup of the unit group, developed by Biasse and Fieker.

- Unlike the existing approach where this has to be done for all \( p < B \), we only need to do so at a single \( p \), since the units only need to have the correct valuation at \( p \).

- This provides an unconditional result for the valuation of \( h \) at \( p \), which can then be used to compute or verify the \( p \)-part of \( Cl_K \).
We can estimate the complexity for computing $L_p(1, \chi)$ up to precision $\nu$:

- Iwasawa: complexity is of order $f_\chi \nu^3 d^2$, where $d = \mathbb{Q}_p[\zeta_n, \zeta_{f_\chi}] / \mathbb{Q}_p$.
- Cohen: complexity is of order $\text{lcm}(f_\chi, p) \nu^3$.

We can deduce asymptotic behaviour of the ratio $\log D / \log f$ which shows our algorithm has the advantage when field degree is higher than 4.

Actual results are somewhat interesting.
We can estimate the complexity for computing $L_p(1, \chi)$ up to precision $\nu$:

- Iwasawa: complexity is of order $f_\chi \nu^3 d^2$, where $d = \mathbb{Q}_p[\zeta_n, \zeta_{f_\chi}]/\mathbb{Q}_p$.
- Cohen: complexity is of order $\text{lcm}(f_\chi, p) \nu^3$.

We can deduce asymptotic behaviour of the ratio $\log D / \log f$ which shows our algorithm has the advantage when field degree is higher than 4.

Actual results are somewhat interesting.
We can estimate the complexity for computing $L_p(1, \chi)$ up to precision $\nu$:

- Iwasawa: complexity is of order $f_\chi \nu^3 d^2$, where $d = \mathbb{Q}_p[\zeta_n, \zeta_{f_\chi}]/\mathbb{Q}_p$.
- Cohen: complexity is of order $\text{lcm}(f_\chi, p) \nu^3$.

We can deduce asymptotic behaviour of the ratio $\log D/\log f$ which shows our algorithm has the advantage when field degree is higher than 4.

Actual results are somewhat interesting.
We can estimate the complexity for computing $L_p(1, \chi)$ up to precision $\nu$:

- Iwasawa: complexity is of order $f_\chi \nu^3 d^2$, where $d = \mathbb{Q}_p[\zeta_n, \zeta_{f_\chi}]/\mathbb{Q}_p$.
- Cohen: complexity is of order $\text{lcm}(f_\chi, p) \nu^3$.

We can deduce asymptotic behaviour of the ratio $\log D / \log f$ which shows our algorithm has the advantage when field degree is higher than 4.

Actual results are somewhat interesting.
We can estimate the complexity for computing $L_p(1, \chi)$ up to precision $\nu$:

- Iwasawa: complexity is of order $f_\chi \nu^3 d^2$, where $d = \mathbb{Q}_p[\zeta_n, \zeta_{f_\chi}]/\mathbb{Q}_p$.
- Cohen: complexity is of order $\text{lcm}(f_\chi, p) \nu^3$.

We can deduce asymptotic behaviour of the ratio $\log D / \log f$ which shows our algorithm has the advantage when field degree is higher than 4.

Actual results are somewhat interesting.
$C_4$: conductor vs $\log |D|/\log f$
Verifying $p$-valuation of class numbers
Example ($p$-adic approach faster than classical)

$\mathbb{Q}$ adjoined by root of

$$x^7 - x^6 - 354x^5 - 979x^4 + 30030x^3 + 111552x^2 - 715705x - 2921075$$

Conductor: 827
Class group: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
Minkowski bound: 3461471
Classical method: <1 second for conditional class group, 160 seconds for verification
2-adic verification: 1.5 seconds
Example (\(p\)-adic approach faster than classical)

\(\mathbb{Q}\) adjoined by root of
\[x^7 - x^6 - 354x^5 - 979x^4 + 30030x^3 + 111552x^2 - 715705x - 2921075\]

Conductor: 827

Class group: \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\)

Minkowski bound: 3461471

Classical method: <1 second for conditional class group, 160 seconds for verification

\(2\)-adic verification: 1.5 seconds

Yinan Zhang

Verifying \(p\)-valuation of class numbers

Sydney
Example ($p$-adic approach faster than classical)

$\mathbb{Q}$ adjoined by root of

$$x^7 - x^6 - 354x^5 - 979x^4 + 30030x^3 + 111552x^2 - 715705x - 2921075$$

Conductor: 827

Class group: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Minkowski bound: 3461471

Classical method: <1 second for conditional class group, 160 seconds for verification

2-adic verification: 1.5 seconds
Example \((p\text{-adic approach faster than classical})\)

\(\mathbb{Q}\) adjoined by root of 
\[x^7 - x^6 - 354x^5 - 979x^4 + 30030x^3 + 111552x^2 - 715705x - 2921075\]

Conductor: 827  
Class group: \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\)  
Minkowski bound: 3461471

Classical method: < 1 second for conditional class group, 160 seconds for verification  
2-adic verification: 1.5 seconds
Example \((p\text{-adic approach faster than classical})\)

\[ \mathbb{Q} \text{ adjoined by root of} \]
\[ x^7 - x^6 - 354x^5 - 979x^4 + 30030x^3 + 111552x^2 - 715705x - 2921075 \]

Conductor: 827
Class group: \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\)
Minkowski bound: 3461471
Classical method: <1 second for conditional class group, 160 seconds for verification

2-adic verification: 1.5 seconds
Example ($p$-adic approach faster than classical)

$\mathbb{Q}$ adjoined by root of

$$x^7 - x^6 - 354x^5 - 979x^4 + 30030x^3 + 111552x^2 - 715705x - 2921075$$

Conductor: 827
Class group: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
Minkowski bound: 3461471
Classical method: $<1$ second for conditional class group, 160 seconds for verification
2-adic verification: 1.5 seconds
Example (classical approach impractical)

\( \mathbb{Q} \) adjoined by root of \( x^{11} - x^{10} - 930x^9 + 3045x^8 + 254577x^7 - 1429869x^6 - 20686141x^5 + 161668576x^4 + 22066074x^3 - 2332641960x^2 + 5139613620x - 2955818871 \)

Conductor: 2047
Class group: \( \mathbb{Z}/11\mathbb{Z} \)
Minkowski bound: 5028348788074 (13 digits)
Classical approach (Bach bound): 6.6 seconds for conditional class group, 48 seconds to verify with Bach bound (69752)
11-adic verification: 25 seconds
Example (classical approach impractical)

\( \mathbb{Q} \) adjoined by root of \( x^{11} - x^{10} - 930x^9 + 3045x^8 + 254577x^7 - 1429869x^6 - 20686141x^5 + 161668576x^4 + 22066074x^3 - 2332641960x^2 + 5139613620x - 2955818871 \)

Conductor: 2047

Class group: \( \mathbb{Z}/11\mathbb{Z} \)

Minkowski bound: 5028348788074 (13 digits)

Classical approach (Bach bound): 6.6 seconds for conditional class group, 48 seconds to verify with Bach bound (69752)

11-adic verification: 25 seconds
Example (classical approach impractical)

$\mathbb{Q}$ adjoined by root of $x^{11} - x^{10} - 930x^9 + 3045x^8 + 254577x^7 - 1429869x^6 - 20686141x^5 + 161668576x^4 + 22066074x^3 - 2332641960x^2 + 5139613620x - 2955818871$

Conductor: 2047

Class group: $\mathbb{Z}/11\mathbb{Z}$

Minkowski bound: 5028348788074 (13 digits)

Classical approach (Bach bound): 6.6 seconds for conditional class group, 48 seconds to verify with Bach bound (69752)

$11$-adic verification: 25 seconds
Example (classical approach impractical)

\( \mathbb{Q} \) adjoined by root of \( x^{11} - x^{10} - 930x^9 + 3045x^8 + 254577x^7 - 1429869x^6 - 20686141x^5 + 161668576x^4 + 22066074x^3 - 2332641960x^2 + 5139613620x - 2955818871 \)

Conductor: 2047
Class group: \( \mathbb{Z}/11\mathbb{Z} \)
Minkowski bound: 5028348788074 (13 digits)

Classical approach (Bach bound): 6.6 seconds for conditional class group, 48 seconds to verify with Bach bound (69752)

11-adic verification: 25 seconds
Example (classical approach impractical)

\( \mathbb{Q} \) adjoined by root of \( x^{11} - x^{10} - 930x^9 + 3045x^8 + 254577x^7 - 1429869x^6 - 20686141x^5 + 161668576x^4 + 22066074x^3 - 2332641960x^2 + 5139613620x - 2955818871 \)

Conductor: 2047

Class group: \( \mathbb{Z}/11\mathbb{Z} \)

Minkowski bound: 5028348788074 (13 digits)

Classical approach (Bach bound): 6.6 seconds for conditional class group, 48 seconds to verify with Bach bound (69752)

11-adic verification: 25 seconds
Example (classical approach impractical)

\[ \mathbb{Q} \text{ adjoined by root of } x^{11} - x^{10} - 930x^9 + 3045x^8 + 254577x^7 - 1429869x^6 - 20686141x^5 + 161668576x^4 + 22066074x^3 - 2332641960x^2 + 5139613620x - 2955818871 \]

Conductor: 2047
Class group: \( \mathbb{Z}/11\mathbb{Z} \)
Minkowski bound: 5028348788074 (13 digits)
Classical approach (Bach bound): 6.6 seconds for conditional class group, 48 seconds to verify with Bach bound (69752)
11-adic verification: 25 seconds

Yinan Zhang
Verifying \( p \)-valuation of class numbers
Jean-François Biasse and Claus Fieker, *New techniques for computing the ideal class group and a system of fundamental units in number theory*. To appear in ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium.
