Local Computations for Global Problems: Class Number Formula

Claus Fieker

MPI-Leipzig, September 2, 2021

Intro/ Basics

We will discuss applications and problems in class group computation.
This is completely different in flavour, here we are computing the p-valuation of the class number - using p-adic analytic techniques.

Intro

(mainly work of Yinan Zhang, based on Iwasawa and Cohen)
Let K be a (totally real abelian) number field, then this has a ζ-function:

$$\zeta_K(s) = \sum N(\mathfrak{a})^{-s}$$

where the sum runs over all integral ideals of $\mathcal{O}$. It is well known (and non-trivial) that ζ_K is meromorphic in $\mathbb{C}$ with a simple pole in 1, furthermore, we have the class number formula:

$$\mathrm{Res}_{s=1}\,\zeta_K = \frac{2^{r_1}(2\pi)^{r_2}\,\mathrm{Reg}_K\,h_K}{\omega_K\sqrt{|D_K|}}$$

Where Reg_K is the regulator, h_K the class number, ω_K the number of torsion units.
This is extensively used to compute h_K and Reg_K, but...

p-adic version

... it also has a p-adic version! Here we need the totally real and abelian bit.
It looks the "same", but now the regulator is p-adic.
Furthermore, the residue can be explicitly computed using L-series (p-adic ones).
OK: there is more to it:

- we need to embed K into a cyclotomic field
- then need the characters that define K
- compute the residue
- compute the regulator

Definitions and more definitions

Let $n \in \mathbb{N}$, a *character* χ modulo n is a homomorphism

$$\chi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$$

It is easy to see that the the character values are actually only $\phi(n)$-th roots of unity, so we can replace $\mathbb{C}$ here by any field containing a primitive $\phi(n)$-th root.
(In reality, a character is a map $\chi : ((\mathbb{Z}/n\mathbb{Z})^*, *) \to (\mathbb{Z}/\phi(n)\mathbb{Z}, +)$.
If a character needs evaluation, we compose it with the map $1 \bmod \phi(n) \mapsto x$ where x is a primitive $\phi(n)$-th root, somewhere)
The multiplicative group of a p-adic field has a canonical decomposition:

$$K^* = \mathbb{Z} \times \mathbb{F}_q^* \times (1 + \pi\mathcal{O})$$

where $\mathbb{F}_q$ is the (finite) residue field of K, $\mathbb{Z}$ is generated by π, a uniformiser and $\mathcal{O}$ is the valuation ring.

... and more: Hurwitz

$$\zeta_p(s,x) := \frac{1}{s-1}\int_{\mathbb{Z}_p} \langle x+t\rangle^{1-s} dt$$

(for $1 \neq s \in \mathbb{C}_p$ and $x \in \mathbb{Q}_p$ small enough (in $|.|_p$)) This can actually be evaluated as a series:

$$\zeta_p(s,x) = \frac{\langle x\rangle^{1-s}}{s-1}\sum_{j=0}^{\infty}\binom{1-s}{j}B_j x^{-j}$$

where B_j are Bernoulli numbers.
and $\langle x\rangle$ is the projection onto the 1-units.

L_p-functions

If we now also have a (primitive) character, we can define L-functions:

$$L_p(s,\chi) := \frac{1}{\omega(f)}\frac{1}{\langle f\rangle^s}\sum_{0\le a<f}\chi(a)\zeta_p(s,\frac{a}{f})$$

Where f is the conductor of χ and ω the Teichmüller character, extended to $\mathbb{Q}_p^*$:
For $x\in\mathbb{Z}_p$, $v_p(x)=0$, define $\omega(x)$ to be the unique $p-1$st root of unity s.th. $x\equiv\omega(x) \bmod p$. For $x\in\mathbb{Q}_p^*$ we define

$$\omega(x) := p^{v_p(x)}\omega(xp^{-v_p(x)})$$

If χ is non-trivial, we have closed, explicit, formulae for $L_p(1,\chi)$
A finite one, by Iwasawa:

$$L_p(1,\chi) = -\left(1-\frac{\chi(p)}{p}\right)\frac{\sum_{a=1}^{f}\chi(a)\zeta^a}{f}\sum_{a=1}^{f}\bar{\chi}(a)\log_p(1-\zeta^{-a})$$

By Cohen: $p>2$, $m := \mathrm{lcm}(p,f)$

$$L_p(1,\chi) = \sum_{0\le a<m,\gcd(a,p)=1}\chi(a)\left(-\frac{\log_p(a)}{m}+\sum_{j=1}^{\infty}(-1)^j\frac{m^j}{a^j}\frac{B_j}{j}\right)$$

(In finite precision this too is a finite sum)

The statement

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

(For totally real abelian fields and the p-adic regulator R_p)
Using the precising explicit formulae, this can be computed.
Both methods have their pros and cons.

- Iwasawa needs a large number of (expensive) logarithms
- Cohen needs a larger field $\mathrm{lcm}(p, f)$ and the Bernoulli numbers

In either case, *the* problem is the need to work with roots of unity of large order. In contrast to $\mathbb{C}$, they live in fields of large degree.

... there is more

So far, all "our" computations work with fields explicitly given via some polynomial:

$$K = \mathbb{Q}[t]/\mu$$

Assume we know the field to be totally real and abelian (Galois group?), how do we get

- the conductor (of the field this time)
- the characters "defining" the field?

If K is of prime degree, step 1 is easy $f = \sqrt[d-1]{D}$, but in general?

Norm group

We need to start with, a *multiple* d of the conductor. Baring better ideas: the discriminant will do. (badly)
We want

$$U := \langle N(\mathfrak{P}) | \mathfrak{P} \text{ prime in } K, \text{ coprime to } d \rangle < (\mathbb{Z}/d\mathbb{Z})^* =: G$$

We know we're done if $|G/U| = (K : \mathbb{Q})$. We simply run over all primes until done. (if the field happens to be wrong, ie. non-abelian, the quotient will become too small)
Under GRH we have (useful) upper bounds for the $\mathfrak{P}$ we need,
Without GRH we ave (useless) upper bounds.
We ignore both.

Conductor

For any $b|d$ we have the natural projection:

$$\pi_{d,b} : \mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z} : x \mapsto x$$

The conductor of U (and thus of K) is the smallest $f|d$ s.th.

$$G/U = (\mathbb{Z}/f\mathbb{Z})^*/\pi_{d,f}(U)$$

We systematically try the divisors of d, one prime at a time. Incidentally, f is also the minimal integer s.th. K can be embedded into the f-th cyclotomic field.

Characters

The characters we need have to satisfy two properties:

- $\chi(U) = 1$, ie. $U \leq \ker \chi$
- χ has to be primitive, ie. the conductor of $\ker \chi$ has to be f as well

Good news: we need only half of them: if χ is odd, then $L_p(1, \chi) = 0$, so we don't need them.

Roots of 1

Given p and f, we need a primitive f-th root of 1 in a (minimal) extension of $\mathbb{Q}_p$. Easy part $f = p^r g$ with $\gcd(g, p) = 1$, then

- ζ_g is unramified
- ζ_{p^r} is totally ramified

In fact $\mathbb{Q}_p(\zeta_g) : \mathbb{Q}_p$ is the order of p modulo g and is easily findable. For $\mathbb{Q}_p(\zeta_p)$ we have two canonical possibilities:

- define the field by a factor of the cyclotomic polynomial
- use a small polynomial (ie. the one from the finite field)

Ramified Part

Easy: let g be the p^r-th cyclotomic polynomial. By construction this is

- irreducible (p-adically)
- totally ramified
- defines the root of 1
- is definitely not Eisenstein.

However, $g(x+1)$ is...
Finally we need to compose, ie. stack.

Problem

The fields are large

The logarithm

Here we need to define $\log_p$ on $\mathbb{C}_p$, not only on $1+p\mathbb{Z}_p$, this is the Iwasawa logarithm. Lets do it algorithmically. Wanted $\log_p x$ for x in some (ramified) extension K.

- $k := v_\pi(x)$ for "the" uniformiser in K
- We have $\pi^e = \epsilon p$ for some unit ϵ
- $y := \pi^{-k}x = (\epsilon p)^{-k/e}x$
- y^{q-1} is now a 1-unit, so $\log_p(y) = 1/(q-1)\log_p(y^{q-1})$ (possibly need to power by powers of p to make valuations large enough)
- $\log_p \epsilon^{-k/e} = -k/e \log_p \epsilon$
- $\log_p(p) = 0$
- so we can assemble $\log_p x$

Note: $\log_p$ and Frobenius commute...

Residue

Looking at the explicit formulae that give the p-adic data.
However:

- the conductor of K is potentially large, thus the p-adic field will be large and *general*, ie. ramified
- while we have good (polynomial runtime) complex approximations to the residue, we don't have them p-adically
- we need the slightly modified p-adic logarithm, extended to $\mathbb{C}_p$, evaluated on many elements in large fields. Even in low precision this is expensive.

Regulator

The regulator is easy:

- compute the units normally
- compute the p-adic conjugates
- ... and their logarithm
- ... and the determinant

Why???

It's cool.

To compute a GRH-free class or unit group requires (current knowledge) algorithms that have a runtime at least linear in $\sqrt{|D_L|}$. (slow slow really slow)

However, to get the size of the p-part of the class group ($v_p(h_K)$) is feasible:

- compute units believing any conjectures you want
- saturate the units at p, so they are p-maximal
- compute the p-adic residue (linear in the *conductor*)
- read off $v_p(h_K)$

For cyclic field (say of prime degree l), the trick is that $|D| = f^{l-1}$, hence the total time is *much* better than $\sqrt{|D|}$ - but still exponential.

...

(Part) of the theory extends to CM-fields as well, but they are, so far, not constructive.
For abelian fields, Leopoldt's conjecture is known, so no nasty surprises with the regulator.
In general, part of the problem is a consistent definition of a p-adic regulator. They all(?) agree on either being zero or not, but otherwise ...