CIMPA school **Class field theory computations**
University of the Philippines Diliman **9-20 January 2023**
Teachers: Jared Asuncion and Francesco Campagna

Exercises for CFT computations

CHALLENGE PROBLEM

You can hand-in the solutions to the challenge problem until Thursday at 6.30.

Here is the challenge:

- Choose you favourite $N \in \mathbf{Z}_{>0}$ (*e.g.* 250519).
- Compute the first 5 primes of the form $x^2 + Ny^2$ with $x, y \in \mathbf{Z}$ and give us the corresponding x and y.
- What is the density of the set of primes of the form $x^2 + Ny^2$?
- By which splitting condition are the primes of the form $x^2 + Ny^2$ characterised?

In some points of the following exercises you may want to use PARI/GP to perform your computations.

Exercise 1

Consider the set S_2 of primes $p \in \mathbf{Z}$ such that $p = x^2 + 2y^2$ for some $x, y \in \mathbf{Z}$.

1. Compute the ratio
$$\delta_n := \frac{\#\{p \leq n : p \in S_2\}}{\#\{p \leq n : p \text{ prime}\}}$$
for $n = 10^5, 10^6$.
2. Prove that $p \in S_2$ if and only if there exists an irreducible element $\pi \in \mathbf{Z}[\sqrt{-2}]$ such that $p = \pi\overline{\pi}$ (here $\bar{\cdot}$ denotes complex conjugation).
3. Prove that if p is an odd prime, then $p \in S_2$ if and only if $p \equiv 1, 3 \bmod 8$. Deduce that S_2 has density 1/2.

Exercise 2

Let G be a finite group and consider the weighted lattice diagram L_G whose vertexes v correspond to subgroups G_v of G and there is an arrow from a vertex v to a vertex w if $G_v \subseteq G_w$. Each arrow from v to w is weighted by the index $|G_w : G_v|$.

1. Let L'_G be the weighted lattice obtained by reversing the arrows in L_G and keeping the same weights. Draw L_G and L'_G for all finite groups of order 8
2. Show that, if G is abelian, then L'_G is isomorphic to L_G. Does this statement hold if G is not abelian?
3. Can you find an interpretation of L'_G?

Exercise 3

Show that the norm is multiplicative in towers of number fields *i.e.* if $K \subseteq F \subseteq L$ are number fields, then for every $\alpha \in L$ we have

$$N_{L/K}(\alpha) = N_{F/K}(N_{L/F}(\alpha)).$$

Exercise 4

What is your opinion: is the set of primes whose first digit is a 1 (*e.g.* $10^{35} + 69$) characterised by a splitting condition? Does it have a density?

Exercise 5

Consider the set S_{15} of primes $p \in \mathbf{Z}$ such that $p = x^2 + 15y^2$ for some $x, y \in \mathbf{Z}$.

1. Show that $p \in S_{15}$ if and only if there exists an irreducible element $\pi \in \mathbf{Z}\left[\frac{1+\sqrt{-15}}{2}\right]$ such that $p = \pi\overline{\pi}$ (here $\bar{\cdot}$ denotes complex conjugation).
2. Compute the complete lattice of subfields of $\mathbf{Q}(\zeta_{15})$.
3. Show that the elements $p \in S_{15}$ are characterised by congruence conditions modulo 15.
4. Compute the natural density of the set S_{15}.

Exercise 6

Let $d > 0$ be a squarefree positive integer and let $\mathcal{O}_d := \mathbf{Z}[\sqrt{d}]$. Recall that the ring $\mathcal{O}_d$ is equal to the ring of integers $\widetilde{\mathcal{O}}_d$ of $\mathbf{Q}(\sqrt{d})$ if and only if $d \not\equiv 1 \bmod 4$.

1. Prove that $x^2 - dy^2 = -1$ has a solution in $x, y \in \mathbf{Z}$ if and only if there exists $u \in \mathcal{O}_d^\times$ such that $N_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}(u) = -1$.
2. Suppose that $d \equiv 1 \bmod 8$. Show that -1 is the norm of some unit in $\mathcal{O}_d$ if and only if it is the norm of some unit in $\widetilde{\mathcal{O}}_d = \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.
3. Assume from now on that $d \equiv 5 \bmod 8$. Show that the ideal $\mathfrak{p}_2 := (2, 1+\sqrt{d}) \subseteq \mathcal{O}_d$ is prime and show that $\mathcal{O}_d/\mathfrak{p}_2 \cong \mathbf{F}_2$.
4. Show that $2\widetilde{\mathcal{O}}_d$ is a prime ideal in $\widetilde{\mathcal{O}}_d = \mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ and that there is a commutative diagram

$$\begin{array}{ccc} \widetilde{\mathcal{O}}_d & \dashrightarrow & \mathbf{F}_4 \\ \uparrow & & \uparrow \\ \mathcal{O}_d & \dashrightarrow & \mathbf{F}_2 \end{array}$$

   where the upper horizontal arrow is reduction modulo 2 and the lower horizontal arrow is reduction modulo $\mathfrak{p}_2$.
5. Show that if $x \in \widetilde{\mathcal{O}}_d$ is such that $(x \bmod 2) \in \mathbf{F}_2$ then $x \in \mathcal{O}_d$.
6. Deduce that for $u \in \widetilde{\mathcal{O}}_d^\times$ either u or u^3 is in $\mathcal{O}_d$. Conclude that, also in this case, -1 is the norm of some unit in $\mathcal{O}_d$ if and only if it is the norm of some unit in $\widetilde{\mathcal{O}}_d$.
7. By Dirichlet's unit theorem, we have

$$\widetilde{\mathcal{O}}_d^\times = \langle -1 \rangle \times \langle u_d \rangle$$

   where u_d is determined up to sign. Write a program in PARI that computes the proportion of positive squarefree $d \equiv 5 \bmod 8$ up to 10^6 such that $u_d \in \mathcal{O}_d$. Based on your computation, what do you think is the "true" proportion of d's satisfying this property?