CIMPA school **Computational number theory**
University of the Philippines Diliman **9-20 January 2023**
Teachers: Valerio Talamanca and Francesco Campagna

Programming challenges

Use PARI/GP to answer the following questions.

Notation and conventions: For a number field K we denote by $\mathcal{O}_K$ its ring of integers. Everything in the text of the exercises happens inside a fixed algebraic closure of $\mathbf{Q}$ (but whatever happens in your computer may not!).

Some training on number fields

Consider the polynomial $f(x) = x^6 - 2x^4 - 9x^3 + 16x^2 + 24x + 24$ over $\mathbf{Q}$.

1. Show that f is irreducible over $\mathbf{Q}$ and let L be the number field generated over the rationals by a root of f.
2. Show that L is not a Galois extension of $\mathbf{Q}$ and compute Galois group G and defining polynomial for its Galois closure.
3. Show that L contains a subfield isomorphic to $\mathbf{Q}[x]/(x^3 - x^2 - x + 4)$. What are the other subfields of L? Show that the results you obtain are compatible with the ones obtained in the previous question by looking at the subgroups lattice of G here.
4. Compute an integral basis for L and the order of the class group Cl_L. Find at least 10 prime ideals of L whose class in Cl_L has order 5.
5. Use Dirichlet's units theorem and point (3) to predict the rank and the torsion of the unit group $\mathcal{O}_L^\times$. Verify then directly with PARI/GP your conclusions by computing the full unit group of $\mathcal{O}_L$.
6. Compute numerically the following limit:

$$\lim_{x\to\infty} \frac{\#\{\text{prime ideals of } \mathbf{Q} \text{ up to } x \text{ that split completely in } \mathbf{Q} \subseteq L\}}{\#\{\text{prime ideals of } \mathbf{Q} \text{ up to } x\}}$$

   and verify that it is very close to $1/12$.

More training: write the function

This exercise asks you to write various functions in PARI/GP. You are completely free to write the functions as you like (for instance, you can decide in which form the input is given).

1. Write a function that, given as input an integer a and a bound n, returns the ratio between the number of primes $p \leq n$ for which $\langle a \rangle = \mathbf{F}_p^\times$ and the total number of primes $p \leq n$.
   - Test your function with $n = 10^6$ and $a = 2, 3, 5, 8, 9$.
   - What is in your opinion the integer a for which your function with $n = 10^6$ gives the largest result? And the smallest?
2. Write a function that, given as input two Galois number fields K and L, returns as output a polynomial defining $K \cap L$.
   - Test your function with the number fields defined by

     $$f(x) = x^{20} - 11x^{18} + 52x^{16} - 139x^{14} + 241x^{12} - 287x^{10} + 241x^8 - 139x^6 + 52x^4 - 11x^2 + 1$$

     and

     $$\begin{aligned} g(x) = x^{20} &- 5x^{19} + 11x^{18} - 12x^{17} + 14x^{16} - 14x^{15} - 54x^{14} + 17x^{13} + 84x^{12} \\ &+ 14x^{11} + 76x^{10} + 432x^9 + 654x^8 + 588x^7 + 425x^6 + 236x^5 + 77x^4 + 2x^3 \\ &- 7x^2 - x + 1. \end{aligned}$$

     You should obtain an intersection of degree 10.
3. Given a number field K and a prime p, the *splitting type* of p in K is the list $(f_1, .., f_g)$ of residue degrees $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbf{Z}/p\mathbf{Z}]$ coming from the factorisation $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$. We order the list $(f_1, .., f_g)$ in such a way that $f_i \leq f_{i+1}$.

   Write a function that, given as inputs two number fields K_1, K_2 and a bound n, prints the primes $p \leq n$ and their corresponding splitting type in K_1 and K_2.
   - Test your function on the number fields defined by $f(x) = x^8 - 31$ and $g(x) = x^8 - 496$. What do you notice? Are these two number fields isomorphic?

Mystery 1: strange splittings

Consider the polynomial $f(x) = x^8 - x^7 + 2x^6 + 3x^5 - x^4 + 3x^3 + 2x^2 - x + 1$ and let K be the number field obtained by adjoining to $\mathbf{Q}$ a root of f.

1. Show that K is Galois over $\mathbf{Q}$ and compute its Galois group.

2. Show that there is a chain of subfields

$$\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{-39}) \subseteq \mathbf{Q}(\sqrt{-3}, \sqrt{13}) \subseteq K.$$

3. The previous point can also be solved by showing that $K = \mathbf{Q}\left(\sqrt{-3}, \sqrt{(-1+\sqrt{13})/2}\right)$. Verify this statement.

4. Compute the primes $\mathfrak{p} \subseteq \mathbf{Q}(\sqrt{-39})$ with norm up to 2000 that split completely in K. There is something that all these primes have in common. What is it?

5. Compute the primes $\mathfrak{p} \subseteq \mathbf{Q}(\sqrt{-39})$ with norm up to 2000 that split completely in $\mathbf{Q}(\sqrt{-3}, \sqrt{13})$. There is something that all these primes have in common. What is it?

6. Based on your computations, can you make a conjecture that relates the Galois group $\mathrm{Gal}(K/\mathbf{Q}(\sqrt{-39}))$ and the class group of $\mathbf{Q}(\sqrt{-39})$?

The phenomena that this problem displays will be explained in the course *Explicit class field theory.*

Mystery 2: a strange equation over finite fields

Consider the equation in two variables $y^2 + y = x^3 - 1590140x - 771794326$.

1. For every prime p let

$$S_p := \{(x, y) \in \mathbf{F}_p^2 : y^2 + y = x^3 - 1590140x - 771794326\}$$

   Compute $\#S_p$ for all $p \leq 1000$.

2. Compute the proportion of primes $p \leq 1000$ for which $p = S_p$. Is it a random value?

3. Make a change of variables to put the equation in the form $y^2 = f(x)$ where $f(x)$ is a monic degree 3 polynomial. Find a polynomial that defines the splitting field L of f over $\mathbf{Q}$.

4. Show that L has a unique quadratic subfield K. There is something connecting the field K and the primes p such that $p = S_p$. Can you guess what it is?

The phenomena that this problem displays will be explained in the course *CM elliptic curves.*