PAWS 2025: ANALYSIS AND IMPLEMENTATION OF ALGORITHMS IN NUMBER THEORY
PROBLEM SET 5

THOMAS BOUCHET, KATE FINNERTY, ASIMINA S. HAMAKIOTES, YONGYUAN HUANG

Welcome to PAWS! Below are the exercises for Problem Set 5. The questions are loosely in ascending order of difficulty. Feel free to skip around and try whatever exercises would be the most helpful for you. Try as many as you can but don't feel like you need to complete them all!

1. Beginner Problems

Question 1: Show that the set of fractional ideals of a $\mathcal{O}_K$ forms a group under multiplication.

Question 2: Find a $\mathbb{Z}$-basis for the ideal generated by $\{3, 2+\theta, 1-\theta^2, 1+\theta+\theta^3\}$ in the number field $K = \mathbb{Q}(\theta)$, where θ has minimal polynomial $x^4 - x^3 + x^2 - 2x + 2$.

Question 3: Compute a fundamental unit for $\mathbb{Q}(\sqrt{5})$.

Question 4: Use Hermite normal forms to implement an algorithm to compute the sum of two ideals of $\mathcal{O}_K$.

2. Intermediate Problems

Question 5: A ring R is an Euclidean domain if it admits an Euclidean algorithm.

(1) Show that every Euclidean domain is a principal ideal domain.
(2) Prove that $\mathbb{Z}[\sqrt{-3}]$ is not a principal ideal domain.

Question 6:

(a) In the ring $\mathbb{Z}[x]$, compute the norm of the ideal $(2, x^2)$ in $\mathbb{Z}[x]$ and determine the maximal ideal that contains $(2, x^2)$.
(b) In the ring $\mathbb{Z}[\sqrt{5}]$, show that the principal ideal (3) is prime.

Question 7: In the number field $K = \mathbb{Q}(\sqrt{-5})$, compute Minkowski's bound and list all ideals with norm bounded by it. Use this to determine the structure of the class group of K.

3. Advanced Problems

Question 8: Implement Algorithm 6.5.8 (Computation of a System of Fundamental Units) in

`Magma`. For the LLL reduction, you can use the native command `LLL`. Use the online documentation for this command at this link.

Question 9: Compute a system of fundamental units and the class group for the number field defined by $f(x) = x^4 - 3x - 5$.

Question 10: List all imaginary quadratic fields with class number 1, for p prime and $p < 200$, and conclude that your list includes all imaginary quadratic fields with class number 1 using the theorem of Stark, 1967:

Theorem. If the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ has class number 1 for a prime number p, then $p < 200$.