PAWS 2025: ANALYSIS AND IMPLEMENTATION OF ALGORITHMS IN NUMBER THEORY
PROBLEM SET 0

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

Welcome to PAWS! Below are the exercises for Problem Set 0. 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. Computational Problems

Magma is a software package designed for computations in algebra, number theory, algebraic geometry, and algebraic combinatorics. It is a great tool for implementing number theoretic algorithms. A free online calculator for short computations is available here.

You are welcome to use Magma or your favorite computer algebra system for the problem sets.

Question 1: Complete as much as you can of the Magma scavenger hunt here. Remember to end your statements with semi-colons! The link also has additional Magma resources!

Question 2:

(a) Factor the polynomial $x^6 - 1$ over $\mathbb{Q}$, and then over $\mathbb{F}_7$. Over which field does it have more irreducible factors? Can you explain why?

(b) How many monic irreducible univariate polynomials of degree 4 are there over $\mathbb{F}_5$?

(c) Up to isomorphism, how many subfields does $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ have? Can you check that the strict subfields among these are isomorphic to $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{6})$, and $\mathbb{Q}(\sqrt{3})$?

(c) Create the ring $L = \mathbb{Z}[x]/(x^2 + 1)$. What is the value of x in L? Of x^4?

(d) Consider the matrix $M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ over $\mathbb{F}_5$. What are its rank, trace, and determinant? What are its minimal and characteristic polynomials? What is its order in $\mathrm{GL}_2(\mathbb{F}_5)$?

2. Theoretical Problems

Let $f(n)$ and $g(n)$ be functions defined on the natural numbers. We say that $f(n)$ **is big-O of** $g(n)$, and write

$$f(n) = O(g(n)),$$

if there exist constants $C > 0$ and $n_0 \in \mathbb{N}$ such that, for all $n \geq n_0$,

$$|f(n)| \leq C\,|g(n)|.$$

Question 3:

(a) Prove that for all $x \in \mathbb{R}_{>0}$, we have $\ln(x) \leq x$.
(Hint: you can differentiate)

(b) Prove that $\frac{x}{\ln(x)}$ goes to $+\infty$ as $x \to +\infty$.
(Hint: you can use (a) and the equality $\ln(x) = 2\ln(\sqrt{x})$)

(c) Using a change of variables, compute the limit of $\frac{x\ln(x)}{x\ln(\ln(x))}$ as $x \to +\infty$.

Question 4: Select the dominant term(s) having the steepest increase in n to simplify the following expressions, for example: $O(10n + n^2) = O(n^2)$.

(a) $O(100n + 0.01n^2)$
(b) $O(0.01n + 100n^2)$
(c) $O(n^2 \ln(\ln(n)) + n \ln(n))$
(d) $O(n^2 + n\sqrt{n})$
(e) $O(100n \log_3 n + n^3 + 100n)$
(f) $O(0.003 \log_4 n + \log_2 \log_2 n)$

Let L/K be a field extension. We denote by $[L : K] = \dim_K(L)$ the **degree** of the extension L/K. When $[L : K]$ is finite, we say that L/K is a **finite field extension**. In that case, for any $\alpha \in L$, we call **minimal polynomial** of α the unique monic polynomial $m_\alpha \in K[x]$ of smallest degree such that $m_\alpha(\alpha) = 0$.

Question 5:

(a) Determine the minimal polynomial of $1 + i$ over $\mathbb{Q}$.
(b) Determine the minimal polynomial of $1 + i$ over $\mathbb{Q}(i)$.

Question 6:

(a) Prove that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Conclude that $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$.
(Hint: one inclusion is obvious, for the other consider $(\sqrt{2} + \sqrt{3})^2$, etc.)
(b) Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.
(c) Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$.

3. Intermediate Problems

Question 7: Let K be a field. A splitting field of $f \in K[x]$ is a field extension L/K of smallest degree such that f factors as linear in L as a product of linear factors.

(a) Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 - 2$.
(b) Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + x^2 + 1$.

Question 8: Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$.

4. Advanced Problems

Question 9: Determine the Galois group of the splitting field over $\mathbb{Q}$ of the following polynomials:

(a) $x^8 - 3$
(b) $x^4 - 14x^2 + 9$
(c) $x^4 - 7$

Question 10: Let $n \in \mathbb{Z}_{>0}$.

(a) Prove that $\cos(\frac{2\pi}{n})$ and $\sin(\frac{2\pi}{n})$ are algebraic over $\mathbb{Q}$.
(b) Compute $[\mathbb{Q}(\cos(\frac{2\pi}{9}) : \mathbb{Q}]$.
(c) Show that $\mathbb{Q}(\cos(\frac{2\pi}{n}))/\mathbb{Q}$ is Galois.
(d) Is $\mathbb{Q}(\sin(\frac{2\pi}{n}))/\mathbb{Q}$ a Galois extension in general?