Homework 2 (due Jan. 29)

MATH 110 | Introduction to Number Theory | Winter 2023

Whenever you use a result or claim a statement, provide a **justification** or a **proof**, unless it has been covered in the class. In the later case, provide a **citation** (such as "by the *2-out-of-3 principle*" or "by Coro. 0.31 in the textbook").

You are encouraged to *discuss* the problems with your peers. However, you must write the homework **by yourself** using your words and **acknowledge your collaborators**.

Problem 1. Let a, b and n be positive integers. `Prove` that

(a) (5 pts) $\gcd(a^n, b^n) = \gcd(a, b)^n$ and $\operatorname{lcm}(a^n, b^n) = \operatorname{lcm}(a, b)^n$;
(b) (5 pts) $\gcd(a \cdot n, b \cdot n) = \gcd(a, b) \cdot n$ and $\operatorname{lcm}(a \cdot n, b \cdot n) = \operatorname{lcm}(a, b) \cdot n$;

Problem 2 (10 pts)**.** Write the prime factorization of $N = 13!$ and then count the divisors of N (give the number, you do not need to list all of them in order to count).

Remark. Recall that for any positive integer n, we denote by $n!$ (read n **factorial**) the product of all the integers between 1 and n.

Problem 3 (10 pts)**.** Let n be any positive integer. `Prove` that there exists a positive integer k (depending on n) such that the following list of n consecutive integers:

$$k, k+1, \cdots, k+n-1$$

contains *no* prime number at all.

Hint. Use the factorial (but $k = n!$ is NOT the correct answer, start from this and try to see what are missing). You also need the *2-out-of-3* property of division.

Remark. From the problem, we can see that the gaps between consecutive prime numbers can be arbitrarily large.

Problem 4. As in class, consider the collection of complex numbers of the form

$$\mathscr{O} := \left\{ a + b\sqrt{-5} \;\middle|\; a, b \in \mathbb{Z} \right\}.$$

(a) (3 pts) `Prove` that the set $\mathscr{O}$ equipped with the addition and multiplication of complex numbers satisfies the following properties:

(i) $\mathscr{O}$ is closed under addition: for any $\alpha, \beta \in \mathscr{O}$, we have $\alpha + \beta \in \mathscr{O}$.
(ii) $\mathscr{O}$ is closed under negation: for any $\alpha \in \mathscr{O}$, we have $-\alpha \in \mathscr{O}$.
(iii) $\mathscr{O}$ is closed under multiplication: for any $\alpha, \beta \in \mathscr{O}$, we have $\alpha\beta \in \mathscr{O}$.

Remark. In the terms of Algebra, $\mathscr{O}$ is a *subring* of the ring $\mathbb{C}$ of complex numbers.

(b) (4 pts) Consider the integer-valued function N defined on $\mathscr{O}$:

$$N(a+b\sqrt{-5}) := a^2+5b^2.$$

`Prove` that

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

for any two elements α and β in $\mathscr{O}$.

Remark. Say that an element $\alpha \in \mathscr{O}$ **divides** another element $\beta \in \mathscr{O}$, denoted by $\alpha \mid \beta$ if there is an element $\gamma \in \mathscr{O}$ such that $\beta = \alpha\gamma$. Hence, problem 4.(b) shows that

$$\alpha \mid \beta \implies N(\alpha) \mid N(\beta).$$

(c) (2 pts) Say that an element $\varepsilon \in \mathscr{O}$ is a **unit** if ε divides 1. `Prove` that all the units in $\mathscr{O}$ are 1 and -1.

Hint. Assume $\varepsilon \in \mathscr{O}$ is a unit other than ± 1, then use problem 4.(b).

(d) (8 pts) Say that an element $\alpha \in \mathscr{O}$ is a **prime element** if

(i) α is nonzero and not a unit;

(ii) whenever $\alpha = \gamma\delta$ with $\gamma, \delta \in \mathscr{O}$, we necessarily have one of γ, δ being a unit.

`Prove` that the following four elements are prime elements: 2, 3, $1+\sqrt{-5}$, and $1-\sqrt{-5}$.

Hint. Proceed by way of contradiction, then use problem 4.(b).

(e) (3 pts) Say that two elements $\alpha, \beta \in \mathscr{O}$ are **associated** if both $\alpha \mid \beta$ and $\beta \mid \alpha$. `Prove` that none pair of the four elements 2, 3, $1+\sqrt{-5}$, and $1-\sqrt{-5}$ are associated.

Hint. Use the definition of *division* and problem 4.(c).

Remark. A **prime factorization** of a nonzero element $\alpha \in \mathscr{O}$ is a representation

$$\alpha = \varepsilon p_1 \cdots p_n,$$

where $\varepsilon \in \mathscr{O}$ is a unit and $p_1, \cdots, p_n \in \mathscr{O}$ are prime elements in $\mathscr{O}$. Say that α has a **unique** prime factorization if whenever there is another prime factorization

$$\alpha = \varepsilon' p_1' \cdots p_m',$$

we necessarily have $m = n$ and there is a bijection $\phi\colon \{1, \cdots, n\} \to \{1, \cdots, m\}$ such that each p_i ($1 \leqslant i \leqslant n$) is *associated* to $p'_{\phi(i)}$.

Say that the **unique prime factorization property** holds in $\mathscr{O}$ if any nonzero element $\alpha \in \mathscr{O}$ has a *unique prime factorization*.

Then problem 4 shows that the prime factorization property **fails** in $\mathscr{O}$ due to the following counterexample

$$6 = 2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5}).$$