Homework 3

MATH 110 | Introduction to Number Theory | Summer 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. In chapter 4 of the textbook, we see that Gaussian integers and Eisenstein integers also have **unique prime factorization**. However, this property is not always satisfied. The following problems lead to a counterexample.

Let's consider the collection of complex numbers of the form

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

(a) `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) 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 1.(b) shows that

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

(c) 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 1.(b).

(d) 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 1.(b).

(e) 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 1.(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 this problem shows that the prime factorization property **fails** in $\mathscr{O}$ due to the following counterexample

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

Problem 2. Prove that there are infinitely many positive integer triples (x, y, z) such that

$$x^2 + 2y^2 = 3z^2.$$

Hint. Find an appropriate rational point that will act as a "pivot", much like in the case of classifying Pythagorean triples that we saw in this lecture.

Problem 3. Let p be any prime number and let a and b be any two integers.

(a) Prove that if $a \equiv b \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.
(b) Prove that if $a \equiv b \pmod{p}$, then $a^{p^2} \equiv b^{p^2} \pmod{p^3}$.
(c) Can you generalise?

Problem 4. Solve the congruences $5x \equiv 11 \pmod{37}$ and $11y \equiv 5 \pmod{37}$. If solutions exist, simplify $xy \pmod{37}$.