

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

HOMEWORK 2: GAUSSIAN INTEGERS II

This homework is due at the start of class on Wednesday Sep 20. It is MUCH longer than last week's assignment, so plunge in RIGHT AWAY.

Reminder: Office hours are Monday and Wednesday at 11 in 1118 LGRT.

1. Recall that for integers m, a with $a \neq 0$, $\text{Rem}(m \div a)$ is the unique integer $r \in [0, |a|)$ such that $m = qa + r$ for some $q \in \mathbb{Z}$; i.e. it is the remainder when you divide m by a .

Suppose a is a positive integer, m, n are integers and $r = \text{Rem}(m \div a)$, $s = \text{Rem}(n \div a)$ are their remainders upon division by a .

(a) Suppose $r + s < a$. Show that $\text{Rem}((m + n) \div a) = r + s$.

(b) More generally, show that $\text{Rem}((m + n) \div a) = \text{Rem}((r + s) \div a)$.

2. Suppose an integer t is of the form $t = 4k + 3$ with $k \in \mathbb{Z}$. Show that t cannot be expressed as $t = x^2 + y^2$ with $x, y \in \mathbb{Z}$.

Hint: proceed by contradiction and divide by 4.

3. Show that if p is a prime of the form $4k + 3$ with $k \in \mathbb{Z}$, then p is a Gaussian prime.

4. Given that $167^2 + 32^2 = 28913$, find integers a, b such that $28913000 = a^2 + b^2$.

Hint: $1000 = 100 + 900$.

5. Compute the Gaussian Prime Factorization of $\gamma = 1527 - 199i$.

Hint: $2371330 = 2 \cdot 5 \cdot 13 \cdot 17 \cdot 29 \cdot 37$.

6. Recall that we say $\beta \div \alpha$ has quotient $\kappa \in \mathbb{G}$ and remainder $\rho \in \mathbb{G}$ if $\beta = \kappa\alpha + \rho$ and $|\rho|^2 < |\alpha|^2$.

Calculate “the” quotient κ and “the” remainder ρ for $\beta \div \alpha$; explain in each case if the quotient and remainder are unique or not.

(a) $\alpha = 2 + i$ and $\beta = 14 + i$.

(b) $\alpha = 1 + i$ and $\beta = 1 + 2i$.

7. Recall that for $\alpha \in \mathbb{G}$, $(\alpha) = \{\alpha\lambda \mid \lambda \in \mathbb{G}\}$ is called the “ideal” generated by α . Similarly, for $\alpha, \beta \in \mathbb{G}$, we define

$$(\alpha, \beta) = \{\alpha\lambda + \beta\mu \mid \lambda, \mu \in \mathbb{G}\}$$

and call this the ideal generated by α and β .

- (a) Prove that if $\gamma \in (\alpha, \beta)$, then $\gamma\delta \in (\alpha, \beta)$ for all $\delta \in \mathbb{G}$.
- (b) Prove that $(\alpha, \beta) = \mathbb{G}$ if and only if $1 \in (\alpha, \beta)$.
- (c) Prove that $(\alpha, \beta) = \mathbb{G}$ if and only if $(\alpha, \beta) \cap \mathbb{G}^\times$ is not empty.

8. Show that $(6 + i, 19 - 7i) = \mathbb{G}$.

9. For each $r \in \mathbb{N}$, let $B_r = \{\alpha \in \mathbb{G} \mid |\alpha|^2 \leq r\}$ be the set of those Gaussian integers which are of norm at most r (i.e. those Gaussian integers whose distance from the origin is at most \sqrt{r} : these are the grid points inside the circle of radius r around the origin).

(a) Draw a picture of the set $B_{20} \cap (1 + 3i, 3 + i)$, which are those grid points within the circle of radius 20 that are in the ideal $(1 + 3i, 3 + i)$.

(b) What are the elements of smallest norm in the ideal $(1 + 3i, 3 + i)$? Are these all associates of one another?

(c) Now draw a picture of the set $B_{20} \cap (1 + i)$.

(d) Can you make a conjecture about the ideals $(1 + i)$ and $(1 + 3i, 3 + i)$ based on (a) and (b)? Can you prove that conjecture?

10. Recall that for $\alpha, \gamma \in \mathbb{G}$ we write $\alpha \mid \gamma$ (read: α divides γ) if there exists $\lambda \in \mathbb{G}$ such that $\gamma = \alpha\lambda$.

(a) Suppose $\alpha, \beta, \gamma \in \mathbb{G}$ and $(\alpha, \beta) = \mathbb{G}$. Show that if $\alpha \mid \gamma$ and $\beta \mid \gamma$, then $\alpha\beta \mid \gamma$.

(b) Show via an example that in (a) we cannot dispense with the assumption $(\alpha, \beta) = \mathbb{G}$.

Extra Credit.

A. Find integers a, b such that $p = a^2 + b^2$ where p is the prime

$$p = 2938741902873409187309487102983740198723094871902387717.$$

A little advice: there is only one pair (a, b) of positive integers that solves this and a and b are each greater than 10^{24} , so I think that rules out trial and error.