MATH 427: PS 11

CHARLES REZK

Due in class W 29 Nov.

(1) Let \( R = \mathbb{Z}[\sqrt{-5}] \), and let \( a = 6 \) and \( b = 2 + 2\sqrt{-5} \). Show that \( \{a, b\} \) does not have a GCD in \( R \). (Hint: both \( p = 2 \) and \( q = 1 + \sqrt{-5} \) are common factors of \( a \) and \( b \), so show that there is no common factor \( g \) divisible by both \( a \) and \( b \). Use the norm function to do this.)

(2) Let \( R = \mathbb{Z}[i] \) and consider the ideal \( J = (3) \) in \( R \). Show that \( F := R/J \) is a field with nine elements.

In the following exercises, let \( R = \mathbb{Z}[\sqrt{2}] = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \} \). This is a subring of the real numbers.

(3) Define \( N : R \to \mathbb{Z} \) by \( N(a + b\sqrt{2}) := (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \), for \( a, b \in \mathbb{Z} \). Show that (i) \( N(1) = 1 \), (ii) \( N(xy) = N(x)N(y) \), and (iii) \( N(x) = 0 \) if and only if \( x = 0 \). (Your proof in (iii) will need to use the fact that \( \sqrt{2} \) is irrational.)

(4) Show that \( x \in R^\times \) if and only if \( N(x) \in \{1, -1\} \).

(5) Show that \( R^\times \) is an infinite set.

In the following exercises \( F \) is a finite field, with \( |F| = q \).

(6) Show that \( F^\times \) contains an element of order 2 if and only if \( q \) is odd, and show that if such an element exists it is unique. (Hint: we proved in class that any finite group of even order has an element of order 2. The uniqueness statement is something you proved on PS 11.)

(7) Let \( \phi : F^\times \to F^\times \) be the function defined by \( \phi(a) = a^2 \). If \( q \) is odd show that \( |\text{Ker } \phi| = 2 \) and that \( G := \phi(F^\times) \) is a subgroup of index 2 in \( F^\times \).

(8) Show that if \( q \equiv 1 \mod 4 \), then \(-1 \in G \).

(9) Show that if \( q \) is odd, then \( q \equiv 1 \mod 4 \) if and only if there exists an element \( a \in F \) such that \( a^2 = -1 \).

(10) Use the previous exercise to prove Lagrange’s theorem: if \( p \) is a prime number such that \( p \equiv 1 \mod 4 \), then there exists an integer \( m \) such that \( p | (m^2 + 1) \).

Department of Mathematics, University of Illinois, Urbana, IL

E-mail address: rezk@illinois.edu