Math 303 Homework 13

November 27, 2022

Exercise 1. (a) List the possible values of x^2 modulo 4.

(b) List the possible values of $x^2 + y^2$ modulo 4.

(c) Prove that if p is a prime and $p = x^2 + y^2$ for some integers x and y, then $p \equiv 1 \bmod 4$ or $p = 2$.

Exercise 2. Prove that $a + bi = c + di$ if and only if $a = c$ and $b = d$. Hint: One way to do this is to solve for i and get a contradiction.

Exercise 3. Find quotients and remainders for dividing α by β in each of the following, and check that the norm of the remainder is bounded above by half the norm of β.

(a) $\alpha = 11 + 10i$, $\beta = 4 + i$.

(b) $\alpha = 41 + 24i$, $\beta = 11 - 2i$.

(c) $\alpha = 37 + 2i$, $\beta = 11 + 2i$.

(d) $\alpha = 1 + 8i$, $\beta = 2 - 4i$. (In this case the algorithm from the proof gives two different possible answers, can you find both?)

Exercise 4. Prove that if $p \in \mathbb{Z}$ is an ordinary prime with $p \equiv 3 \bmod 4$, then p remains prime in $\mathbb{Z}[i]$. Hint: Suppose that $p = \alpha\beta$ with $N(\alpha), N(\beta) > 1$. By taking norms of both sides, conclude that p can be written as a sum of two squares and then apply an exercise from the first section.

Problem 5. Let p be a prime. We used the following fact in the notes: If

$$q(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

is a monic[1] degree d polynomial with integer coefficients, and $d > 0$, then there are at most d congruence classes of integers r such that

$$q(r) \equiv 0 \bmod p.$$

In this exercise you will prove that this is true using induction on d.

[1] That just means the coefficient of the highest power of x is 1.

(a) First prove the base case, when $d = 1$: if $q(x) = x + b$, prove that there is exactly one congruence class of solutions to $q(x) \equiv 0 \bmod p$. (Hint: This is not hard.)

(b) Before moving on to the inductive step, you will have to prove the following. Suppose $q(x)$ is a monic, degree d polynomial and r is an integer such that

$$q(r) \equiv 0 \bmod p$$

Find a monic, degree $(d - 1)$ polynomial $f(x)$ such that

$$q(x) \equiv (x - r)f(x) \bmod p,$$

by which we mean that the coefficients are equivalent modulo p. This step is the key one; it might be worth trying some examples to get a feel for what's going on. Also, remember: when working modulo p, you can *divide* by any number not divisible by p.

(c) Show that if

$$q(x) \equiv f(x)g(x) \bmod p$$

then any root of $q(x)$ modulo p must be a root of $f(x)$ or a root of $g(x)$ modulo p. (Do you see why it's important that p is prime here?)

(d) Use the previous two parts to complete the inductive step.