18.781 Problem Set 7

Due Monday, October 31 in class.

1(a). The text offers a (pictorial) proof that division with remainder works in the Gaussian integers $\mathbb{Z}[i]$: that if α and β are Gaussian integers with $\beta \neq 0$, then there are Gaussian integers μ and ρ with

$$\alpha = \mu\beta + \rho, \qquad \mathrm{Norm}(\rho) \leq \mathrm{Norm}(\beta)/2.$$

(The Gaussian integers μ and ρ may not be unique.) Explain a way (given α and β) actually to compute $\mu = m_1 + im_2$ and $\rho = r_1 + ir_2$, using just ordinary arithmetic operations on the integer coordinates

$$\alpha = a_1 + ia_2, \qquad \beta = b_1 + ib_2.$$

If this were a computer-friendly class, I would ask you to write code to compute m_1, m_2, r_1, and r_2 from a_1, a_2, b_1, and b_2. But here some words describing what to do will suffice. (Hint: By looking at the diagram on page 107, you can perhaps at least guess that m_1 is the integer minimizing

$$|\alpha - m_1\beta|^2.$$

You can find the real number m_1 minimizing this expression by geometry.)

1(b). As a test of the procedure you developed in (a), find μ and ρ when $\alpha = 137$, $\beta = 37 + i$. (If you didn't solve (a), you can still solve this by trial and error.)

1(c). Find $\gcd(137, 37 + i)$ in the Gaussian integers. (Hint: it is not 1.)

2. In this problem p is a prime congruent to 1 modulo 4.

2(a). Suppose a is any non-zero integer modulo p. Define

$$b \equiv a^{(p-1)/4} \pmod{p}.$$

Prove that either $b^2 \equiv -1 \pmod{p}$ or $b^2 \equiv 1 \pmod{p}$. Prove that if a is a primitive root modulo p, then the first possibility occurs.

2(b). Prove that there is exactly one integer m such that

$$2 \leq m \leq (p-1)/2, \qquad m^2 \equiv -1 \pmod{p}.$$

2(c). Describe a reasonable way to find the integer m as in (b). (Testing every m between 2 and $(p-1)/2$ is too slow.)

2(d). Suppose that $\gcd(p, m + i) = x + iy$ (calculated in the Gaussian integers $\mathbb{Z}[i]$). Prove that $x^2 + y^2 = p$.

2(e). Find the integer m in case $p = 137$.

2(f). Solve the Diophantine equation $x^2 + y^2 = 137$. (This is easy to do by guessing; but the problems up to now tell you how to write a solution immediately.)

3. This problem is about quadratic algebraic integers (page 125 in the text). Always N is a fixed non-zero integer not divisible by p^2 for any prime p.

3(a). Suppose that $N \equiv 1 \pmod 4$. If a and b are rational numbers, prove that $a + b\sqrt{N}$ is a quadratic integer if and only if either

$$a \text{ and } b \text{ are both integers}$$

or

$$2a \text{ and } 2b \text{ are both odd integers.}$$

3(b). Suppose that $N \not\equiv 1 \pmod 4$. If a and b are rational numbers, prove that $a + b\sqrt{N}$ is a quadratic integer if and only if a and b are both integers.

4. This problem is about the quadratic integers

$$\mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} | x, y \in \mathbb{Z}\}.$$

The norm of such an integer is defined to be

$$\text{Norm}(x + y\sqrt{-5}) = x^2 + 5y^2;$$

this is multiplicative just as for Gaussian integers. The only elements of norm 1 (the units) are ± 1. Just as for Gaussian integers, we can define primes and prove the existence of prime factorization; you can assume all of that.

4(a). Prove that there are no elements of $\mathbb{Z}[\sqrt{-5}]$ having norm 2 or norm 3.

4(b). Prove that 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all primes in $\mathbb{Z}[\sqrt{-5}]$.

4(c). Using these four primes, give an example showing that unique factorization fails in $\mathbb{Z}[\sqrt{-5}]$.