Math 3032: Abstract Algebra

Assignment 6

due April 4, 2023

The goal of this assignment is to solve the following classical problem: given an integer n, find all integer solutions (a, b) to the equation

$$a^2 + ab + b^2 = n. \tag{$\star$}$$

Let's call an integer n *representable* if there exists a solution (a, b) to $(\star)$, and let's call each solution a *representation of* n.

1. Set $\zeta := \frac{1+\sqrt{-3}}{2}$, and let $R := \mathbb{Z}[\zeta] \subset \mathbb{C}$ be the smallest subring containing ζ. This ring is called the *Eisenstein integers*.

   Show that every element of R is uniquely expressible as $a + b\zeta$ for $a, b \in \mathbb{Z}$. Show that the function $N : R \to \mathbb{Z}$ defined by

   $$N(a + b\zeta) := a^2 + ab + b^2$$

   is a multiplicative norm. Hint: What is the complex conjugate $\bar{\zeta}$? If $\alpha = a + b\zeta$, what is $\|\alpha\|$?

2. Show that negative numbers are not representable, and that 0 is representable in a unique way. Thus, for the rest of the exercise, we'll only try to represent positive integers.

3. Show that R has six units, and find them. For fixed n, given a solution (a, b) to $(\star)$, find five other solutions.

   Show that if n_1 and n_2 are representable, then so is $n = n_1 n_2$. Given representations (a_1, b_1) of n_1 and (a_2, b_2) of n_2, find a formula for a representation of $n = n_1 n_2$.

4. Prove that R is a UFD. Hint: Show that N is Euclidean.

   If $\pi \in R$ is prime, we'll call it an *Eisenstein prime*. A number which is prime in $\mathbb{Z}$ will be called a *rational prime*.

5. Suppose that p is a rational prime. Show that if p is also an Eisenstein prime, then p is not representable, but that p^2 is, and that p^2 has exactly six representations.

6. Suppose that p is a rational prime. Show that if p is not an Eisenstein prime, then it factors into exactly two Eisenstein-prime factors π, π', and in fact that $\pi' = \bar{\pi}$ is the complex conjugate to π.

7. Show that the rational prime $p = 2$ is not representable.

8. Show that the rational prime $p = 3$ is representable, and that it has exactly six representations. What are they? In particular, show that if $N(\pi) = 3$, then $\bar{\pi}$ and π are associate.

9. Show that if a rational prime $p > 3$ is representable, then its two Eisenstein factors $\pi, \bar{\pi}$ are not associate to each other.

10. Suppose that m is an integer and $N(m + \zeta) = kp$ is a multiple of a rational prime p. Show that in this case p cannot be an Eisenstein prime.

11. The statement "$N(m + \zeta)$ is a multiple of p" is equivalent to the statement

$$m^2 + m + 1 \equiv 0 \pmod{p}. \qquad (\star\star)$$

Show that if p is representable, then equation $(\star\star)$ has a solution m.

12. Suppose that p is an odd rational prime. Show that equation $(\star\star)$ has a solution m if and only if -3 is a square mod p.

13. The following famous theorem, called *quadratic reciprocity*, was first proved by Gauss:

> **Theorem:** Suppose that p and q are distinct odd rational primes, possibly negative. Then p is a square mod q if and only if $(-1)^{\frac{q-1}{2}} q$ is a square mod p.

Using this theorem, classify the rational primes p which are representable.

14. Suppose that $p > 3$ is a representable rational prime. Show that p^d is representable in exactly $6 \times (d + 1)$ ways. Where does the "6" come from?

15. Suppose that p is a non-representable rational prime. Show that p^d is representable if and only if d is even, in which case it is representable in exactly 6 ways. Where does the "6" come from?

16. Show that if m and n are relatively prime rational integers, then the number of representations of mn is

$$(\text{number of representations of } m) \times (\text{number of representations of } n)/6.$$

Where does the "6" come from?

17. Suppose that $n = 2^{d_2} 3^{d_3} \cdots p^{d_p} \cdots$ is a (rational) prime factorization of n. Write a formula for the number of representations of n in terms of the exponents $d_2, d_3, \ldots$. Hint: the formula should have the form

$$(\text{number}) \times \prod_{p \equiv 1 \pmod 3} (\text{formula involving } d_p) \times \prod_{p \equiv 2 \pmod 3} (\text{formula involving } d_p).$$