18.781 Problem Set 8

Due Monday, November 7 in class. This looks longer than previous problem sets. Here are two possible reasons. First, problems 1–3 are meant to be fairly easy. Second (in response to some complaint that the previous problem sets were too straightforward) problems 6 and 7 are meant to be more challenging. If you can do them, that's wonderful. If not, you shouldn't feel that you've suddenly stopped understanding the class.

1. This problem is about the Eisenstein integers $R = \mathbb{Z}[\zeta]$, with

$$\zeta = (-1 + \sqrt{-3})/2.$$

Call a prime in R an *Eisenstein prime.*

1(a). Here are two factorizations of 31 in the Eisenstein integers:

$$31 = (2 + 3\sqrt{-3})(2 - 3\sqrt{-3}) = (\frac{11 + \sqrt{-3}}{2})(\frac{11 - \sqrt{-3}}{2}).$$

Explain why this does not violate unique factorization in the Eisenstein integers.

1(b). Suppose that p is an ordinary prime congruent to 2 modulo 3. Show that p must be an Eisenstein prime.

1(c). For every ordinary prime p smaller than 50 that is not an Eisenstein prime, find a non-trivial factorization in R.

2. Problems 8.8.6–8.8.8 in the text; assume the result of problem 8.8.5.

3. Suppose that

$$f(x) = \pm x^n + a_{n-1}x^{n-1} + \cdots + a_1 x \pm 1$$

is a polynomial with integer coefficients with leading coefficient and constant coefficient both equal to ± 1. Suppose the complex number r is a root of f (so that r is an algebraic integer). Prove that r^{-1} is also an algebraic integer. (Hint: you can write down explicitly a polynomial of which r^{-1} is a root.)

4. Find all the quadratic integers r (text, page 125) whose inverses are also quadratic integers. (You're supposed to offer some way of writing all of them as explicitly as you can: exactly how to do that is up to you.)

5. Find all the quadratic integers r which are roots of 1 (that is, which satisfy $r^n = 1$ for some positive integer n).

6. Give an example of a "rational quaternion"

$$r = a + bi + cj + dk, \qquad a, b, c, d \in \mathbb{Q}$$

such that r satisfies a monic polynomial equation with integer coefficients, but r is *not* a Hurwitz integer.

7. Suppose that $m > 1$ is an integer not divisible by any prime squared. Prove that if m is not prime, then the ring of algebraic integers in $\mathbb{Q}[\sqrt{-m}]$ does *not* have the unique factorization property.