

SOLUTIONS TO HOMEWORK 8

Due Monday, November 8 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:

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

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

Ans: $(2 + 3\sqrt{-3}) * -\zeta = \frac{11 + \sqrt{-3}}{2}$ and $(2 - 3\sqrt{-3}) * -\zeta^2 = \frac{11 - \sqrt{-3}}{2}$. Since $-\zeta$ and $-\zeta^2$ are units (each is the other’s inverse) these are fundamentally the same factorization of 31.

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

Ans: It’s clear that any element of $\mathbb{Z}[\zeta]$ has the form $(a + b\sqrt{-3})/2$ where $a \equiv b \pmod{2}$. As in previous homeworks we can define a norm, $\text{Norm}((a + b\sqrt{-3})/2) = (a^2 + 3b^2)/4$. Now it’s not quite as clear that the norm is actually an integer, but if a and b are both odd, then $a^2 + 3b^2 \equiv 1 + 3 * 1 \equiv 0 \pmod{4}$, and if a and b are even, then similarly $a^2 + 3b^2 \equiv 0 \pmod{4}$, so the norm is always an integer.

Now, let $p \equiv 2 \pmod{3}$ be an ordinary prime. Its norm is p^2 . As usual, a non-trivial factorization of p leads to a non-trivial factorization of p^2 . But, can $a^2 + 3b^2 = 4 * p$ have a solution? Reducing both sides modulo 3, we get $a^2 \equiv 2 \pmod{3}$, which is impossible.

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

Ans: By part (b), we need only consider primes congruent to 0 or 1 (mod 3), and there is only one prime congruent to 0 (mod 3), namely 3.

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

The idea in general is to look for a solution of $a^2 + 3b^2 = 4 * p$. We then have as a factorization $\frac{a + b\sqrt{-3}}{2} \frac{a - b\sqrt{-3}}{2} = p$. This is a non-trivial factorization because the norm of each term on the left hand side is p .

$$\begin{aligned}
7 &= 2^2 + 3 * 1^2 = (2 + \sqrt{-3})(2 - \sqrt{-3}) \\
13 &= 1^2 + 3 * 2^2 = (1 + 2\sqrt{-3})(1 - \sqrt{-3}) \\
19 &= 4^2 + 3 * 1^2 = (4 + \sqrt{-3})(4 - \sqrt{-3}) \\
31 &= 2^2 + 3 * 3^2 = (2 + 3\sqrt{-3})(2 - 3\sqrt{-3}) \\
37 &= 5^2 + 3 * 2^2 = (5 + 2\sqrt{-3})(5 - 2\sqrt{-3}) \\
43 &= 4^2 + 3 * 3^2 = (4 + 3\sqrt{-3})(4 - 3\sqrt{-3})
\end{aligned}$$

Of course, these can be rewritten in terms of ζ because $\sqrt{-3} = 2\zeta + 1$.

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

Ans: (8.8.6) A sum of three numbers, each zero or one, sum to a multiple of four (if and) only if each is zero.

Ans: (8.8.7) If $4^m(8n + 7)$ is a sum of three squares, then by 8.8.5 $m > 0$. So, $x^2 + y^2 + z^2 \equiv 0 \pmod{4}$, so by the previous problem, x, y , and z are all even. Hence, factoring out a two from each of them, we get that $4^{m-1}(8n + 7)$ is a sum of three squares.

Ans: (8.8.8) Repeating the argument above m times, we get that $8m + 7$ is a sum of three squares, which contradicts 8.8.5.

3. Suppose that

$$f(x) = \pm x^n + a_{n-1}x^{n-1} + \cdots + a_1x \pm 1$$

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.)

Ans: We are assuming that $\pm r^n + a_{n-1}r^{n-1} + \cdots + a_1r \pm 1 = 0$. Multiplying both sides of this equation by r^{-n} , we get that $\pm 1 + a_{n-1}r^{-1} + \cdots + a_1(r^{-1})^{n-1} \pm (r^{-1})^n = 0$, and hence r^{-1} is an algebraic integer.

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.)

Ans: Let r be a root of $x^2 + a_1x + a_2$. Then, as in the previous problem, r^{-1} is a root of $a_2x^2 + a_1x + 1$. This yields a monic polynomial if and only if $a_2 = \pm 1$. Say $a_2 \neq \pm 1$. Could r^{-1} still be a quadratic integer?

Say r^{-1} is a root of $x^2 + b_1x + b_2$. Then it is also a root of $a_2x^2 + a_2b_1x + a_2b_2$, as well as $a_2x^2 + a_1x + 1$ from the previous paragraph. Subtracting the second from the first, we find that it is also a root of $(a_2b_1 - a_1)x + (a_2b_2 - 1)$. Note that the constant term of this polynomial cannot be zero because $a_2 \neq \pm 1$. As this polynomial has a root, that implies that the coefficient of x is also non-zero, and thus r^{-1} is a rational number. Of course, that implies that r is also a rational number. These are both quadratic integers by assumption, and so a result on page 125 says that $r = \pm 1$.

So quadratic integers whose inverses are also quadratic integers come in two types: either $r = \pm 1$, or r is the root of an equation $x^2 + bx \pm 1$. By the quadratic equation, in the second case,

$$r = \frac{-b \pm \sqrt{b^2 \pm 4}}{2}$$

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

Ans: Roots of unity lie on the unit circle in the complex plane, so the only real ones are ± 1 . These are both quadratic integers by the book's definition. Assume r is a non-real root of unity and a quadratic integer. The inverse of a root of unity is also its complex conjugate, and since r satisfies a polynomial with integer coefficients, so does its complex conjugate. Thus r^{-1} is also a quadratic integer.

From our description in 4, there are very few non-real numbers which are quadratic integers and whose inverses are also quadratic integers: for $\sqrt{b^2 \pm 4}$ to be imaginary, it must be $\sqrt{0^2 - 4}$ or $\sqrt{(\pm 1)^2 - 4}$. So, we need only check whether $\pm\sqrt{-4}/2$ and $(\pm 1 \pm \sqrt{-3})/2$ are roots of unity. It turns out they all are: the first two are $\pm i$, $(-1 \pm \sqrt{-3})/2$ are third roots of unity, and $(1 \pm \sqrt{-3})/2$ are sixth roots of unity.

6. Give an example of a "rational quaternion"

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

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

Ans: Writing $r^2 + k_1r + k_2 = 0$ we get conditions on a, b, c, d :

$$a^2 - b^2 - c^2 - d^2 + k_1a + k_2 + (2ab + k_1b)i + (2ac + k_1c)j + (2ad + k_1d)k = 0.$$

So, if $a = 0$ and $k_1 = 0$ (it's not necessary to assume that, but it does produce an example), then the only requirement is that $b^2 + c^2 + d^2 = k_2$, where k_2 is some integer. For example, $b = c = 2/3$, $d = 1/3$ works.

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.

Ans: Write $m = p_1p_2 \cdots p_n$, where the p_i 's are distinct primes. Then

$$-(\sqrt{-m})^2 = m = p_1 \cdots p_n,$$

so to show that the ring does not have unique factorization it will suffice to show that $\sqrt{-m}$ is an irreducible element and that it does not divide any of the primes p_i .

We can define a norm map sending $a + b\sqrt{-m}$ to $a^2 + mb^2$ or, if $-m \equiv 1 \pmod{4}$, sending $(a + b\sqrt{-m})/2$ to $(a^2 + mb^2)/4$. As in 1(c), this maps to the integers in both instances. It is multiplicative as usual (because complex conjugation is, and the norm comes from multiplying an element with its conjugate). The norm of $\sqrt{-m}$ is m . A proper factor of $\sqrt{-m}$ must have norm dividing m , and hence $a^2 + mb^2$ must be a proper factor of m or $4m$, with the second case occurring if $-m \equiv 1 \pmod{4}$. In the first case, we must have $b = 0$, but then a^2 dividing m implies $a = \pm 1$ since m is squarefree. In the second case, we must have $b = 0$ or $b = \pm 1$. If $b = 0$ then

$a = 2$ (because m is squarefree, a^2 must divide 4, and because $a \equiv b \pmod{2}$ in order for this to be an algebraic integer, $a = 2$ not 1.) But $2/2 = 1$ is a trivial factor. So, we're left with the case $b = \pm 1$.

We can't rule this case out simply by norm considerations. But if we had a factorization of $\sqrt{-m}$, we know it would look like

$$\frac{a_1 \pm \sqrt{-m}}{2} * \frac{a_2 \pm \sqrt{-m}}{2} = \sqrt{-m}.$$

The argument changes slightly depending on whether we are considering both pluses, both minuses, or one of each. Say they're both pluses. Then $a_1 a_2 - m = 0$ and $a_1 + a_2 = 2$. The first equation guarantees that a_1 and a_2 have the same sign, and then the second equation guarantees they are both 1, but $m \neq 1$, a contradiction. The "minuses" and the "one of each" cases are very similar.

Hence, $\sqrt{-m}$ is irreducible. But might it divide one of the p_i 's? It's norm is m , and p_i 's norm is p_i^2 , and since m has more than one prime factor, we get that it can't divide p_i^2 . Hence, we do not have unique factorization.