

# MATH 100B: Homework #4

Due on Feb 8, 2024 at 12:00pm

*Professor McKernan*

Section A02 6:00PM - 6:50PM

Section Leader: Castellano-Macías

Source Consulted: Textbook, Lecture, Discussion, Office Hour

**Ray Tsai**

A16848188

**Problem 1**

Let  $R$  be an integral domain. Let  $a$  and  $b$  be two elements of  $R$ . Show that if  $d$  and  $d'$  are both a gcd for the pair  $a$  and  $b$ , then  $d$  and  $d'$  are associates.

*Proof.* Since  $d$  and  $d'$  both divides  $a$  and  $b$  and  $d$  is a gcd,  $d'|d$ . However,  $d'$  is also a gcd, so  $d|d'$ . The result then follows.  $\square$

## Problem 2

Let  $R$  be a UFD.

- (a) Prove that for every pair of elements  $a$  and  $b$  of  $R$ , we may find an element  $m = [a, b]$  that is a least common multiple, that is

- (i)  $a|m$  and  $b|m$ ,
- (ii) and if  $a|m'$  and  $b|m'$  then  $m|m'$ .

Show that any two lcm's are associates.

*Proof.* Let  $a, b \in R$ . If either  $a$  or  $b$  is 0, then 0 is the only possible common multiple of  $a$  and  $b$ , and thus 0 is their lcm. Since  $R$  is a UFD, we may put  $a$  and  $b$  into a standard form of prime factorizations

$$a = up_1^{m_1} p_2^{m_2} \dots p_k^{m_k} \quad \text{and} \quad b = vp_1^{n_1} p_2^{n_2} \dots p_k^{n_k},$$

where  $u, v$  are invertible and  $p_i$  and  $p_j$  are associates if and only if  $i = j$ . Let  $m = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$  such that  $l_i = \max(m_i, n_i)$ . It is obvious that  $a|m$  and  $b|m$ . Suppose that  $a|m'$  and  $b|m'$ . Then,  $m' = op_1^{h_1} p_2^{h_2} \dots p_k^{h_k}$ , where  $h_i \geq m_i$  and  $h_i \geq n_i$ , for all  $i$ . However, this means that  $h_i \geq \max(m_i, n_i)$ , so  $m|m'$ . Hence,  $m$  is a least common multiple of  $a$  and  $b$ . Suppose that  $m'$  is also a least common multiple of  $a, b$ . Then, we have  $m'|m$ , which makes  $m$  and  $m'$  associates.  $\square$

- (b) Show that if  $(a, b)$  denotes the gcd then  $(a, b)[a, b]$  is an associate of  $ab$ .

*Proof.* Again, we put  $a$  and  $b$  into a standard form of prime factorizations

$$a = up_1^{m_1} p_2^{m_2} \dots p_k^{m_k} \quad \text{and} \quad b = vp_1^{n_1} p_2^{n_2} \dots p_k^{n_k}.$$

Let  $d = \alpha p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$ ,  $m = \beta p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$ , where  $d = (a, b)$ ,  $m = [a, b]$ , and  $\alpha, \beta$  are invertible. Then, we know  $l_i = \max(m_i, n_i)$  and  $s_i = \min(m_i, n_i)$ , for all  $i$ . However, this means that  $l_i + s_i = m_i + n_i$ , and thus

$$dm = \alpha \beta p_1^{m_1+n_1} p_2^{m_2+n_2} \dots p_k^{m_k+n_k} = \alpha \beta (uv)^{-1} ab.$$

Since  $\alpha \beta (uv)^{-1}$  is invertible,  $dm$  and  $ab$  are associates, and this completes the proof.  $\square$

### Problem 3

Find the greatest common divisor of the following polynomials over  $\mathbb{Q}$ ,

- (a)  $x^3 - 6x + 7$  and  $x + 4$ .

*Proof.*  $x + 4$  is prime as it is degree 1, so either  $x + 4 \mid x^3 - 6x + 7$  or they are coprime. However,  $x^3 - 6x + 7 = (x + 4)(x^2 - 4x + 10) - 33$ , so the greatest common divisor of the two polynomials is 1.  $\square$

- (b)  $x^3 - 1$  and  $x^7 - x^4 + x^3 - 1$ .

*Proof.* Note that  $x^7 - x^4 + x^3 - 1 = (x^3 - 1)(x^4 + 1)$ , so  $x^3 - 1$  is their common divisor.  $\square$

## Problem 4

Find the greatest common divisor of  $135 - 14i$  and  $155 + 34i$  in the ring of Gaussian integers  $\mathbb{Z}[i]$ .

*Proof.* We apply the Euclidean Algorithm. Since

$$\frac{155 + 34i}{135 - 14i} = \frac{(135 + 14i)(155 + 34i)}{135^2 + 14^2} = \frac{20294 + 6726i}{18421} \approx 1.1 + 0.37i,$$

we may pick  $q = 1$  and the remainder is  $r = (155 + 34i) - (135 - 14i)q = 20 + 48i$ .

Since

$$\frac{135 - 14i}{20 + 48i} = 0.75 - 2.5i,$$

we may pick  $q = 1 - 2i$  and the remainder  $r = (135 - 14i) - (20 + 48i)q = 19 - 22i$ .

Since

$$\frac{20 + 48i}{19 - 22i} = -0.8 + 1.6i,$$

we may pick  $q = -1 + 2i$  and the remainder  $r = (20 + 48i) - (19 - 22i)q = -5 - 12i$ .

Since

$$\frac{19 - 22i}{-5 - 12i} = 1 + 2i,$$

$-5 - 12i \mid 19 - 22i$  so there are no remainders left. Hence, the gcd of  $135 - 14i$  and  $155 + 34i$  is  $-5 - 12i$ .  $\square$

## Problem 5

- (a) Show that the elements 2, 3 and  $1 \pm \sqrt{-5}$  are irreducible elements of  $R = \mathbb{Z}[\sqrt{-5}]$ .

*Proof.* Define  $f : \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{Z}_{\geq 0}$  as  $f(a + b\sqrt{-5}) = a^2 + 5b^2$ . For  $a + b\sqrt{-5} \in R$ , we know

$$\begin{aligned} f((a + b\sqrt{-5})(c + d\sqrt{-5})) &= f(ac - 5bd + (ad + bc)\sqrt{-5}) \\ &= a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2 \\ &= (a^2 + 5b^2)(c^2 + 5d^2) \\ &= f(a + b\sqrt{-5})f(c + d\sqrt{-5}), \end{aligned}$$

and  $f(a + b\sqrt{-5}) \geq 0$ . Notice that  $f(a + b\sqrt{-5}) \geq 5$  if  $b$  is positive, so  $f(a + b\sqrt{-5}) = a^2 + 5b^2 = 1$  if and only if  $a + b\sqrt{-5} = 1$ , and thus  $f(a + b\sqrt{-5}) \geq 2$  when  $a + b\sqrt{-5}$  is not 0 or 1.

Let  $m = a + b\sqrt{-5}, n = c + d\sqrt{-5} \in R$ . Suppose that  $mn = 2$ . Then,  $f(2) = 4 = f(m)f(n)$ , so  $f(m)$  or  $f(n)$  is a multiple of 2. Suppose that  $f(m)$  is a multiple of 2. We know  $f(m) = a^2 + 5b^2$  cannot be 2, as  $f(m) > 2$  if  $b$  is positive but there are no integers such that  $a^2 = 2$ , so  $f(m) = 4$ . But then  $f(n) = 1$ , so  $n = 1$ , which is invertible. Hence, 2 is irreducible.

Suppose that  $mn = 3$ . Similarly,  $f(3) = 9 = f(m)f(n)$ , so  $f(m)$  or  $f(n)$  is a multiple of 3. Suppose that  $f(m)$  is a multiple of 3. We know  $f(m) = a^2 + 5b^2$  cannot be 3, as  $f(m) > 3$  if  $b$  is positive but there are no integers such that  $a^2 = 3$ , so  $f(m) = 9$ . But then  $f(n) = 1$ , so  $n = 1$ , which is invertible. Hence, 3 is irreducible.

Suppose that  $mn = 1 \pm \sqrt{-5}$ . Then,  $f(1 \pm \sqrt{-5}) = f(m)f(n) = 6$ . Suppose for the sake of contradiction that  $m, n \neq 1$ . Then, either  $f(m)$  or  $f(n)$  must be 2. However, we already know  $f(k) \neq 2$  for all  $k \in R$ , contradiction. Hence, either  $m$  or  $n$  is 1, so  $1 \pm \sqrt{-5}$  is irreducible.  $\square$

- (b) Show that every element of  $R$  can be factored into irreducibles.

*Proof.* By Proposition 6.11, it suffices to show that the set of principal ideals of  $R$  satisfies ACC. Suppose that we have an increasing sequence of principal ideals of  $R$

$$\langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots \subset \langle a_n \rangle \subset \cdots,$$

for  $a_1 \neq 0$  and  $a_i = a_j$  if and only if  $i = j$ . Suppose for the sake of contradiction that the increasing sequence does not stabilize. Since for  $i \in \mathbb{Z}^+$ ,  $a_{i+1} = ka_i$  for some  $k \in R$ , we know  $f(a_{i+1}) = f(k)f(a_i)$ . Hence,  $f(a_{i+1}) \geq 2f(a_i)$ , as  $k \neq 1$ . Since the sequence does not stabilize and  $f(a_i)$  is finite,  $f(a_n) < 1$  for large enough  $n$ . But then  $a_n = 0$ , which forces  $\langle a_n \rangle = \{0\}$ , and this contradiction completes the proof.  $\square$

- (c) Show that  $R$  is not a UFD.

*Proof.* Consider 2. We already know 2 is irreducible. Notice that,  $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ . Suppose for the sake of contradiction that  $2 = x(1 + \sqrt{-5})$ , for some  $x \in R$ . Then,  $x = \frac{1 - \sqrt{-5}}{2} \notin R$ , contradiction. Similarly, we also know  $2 \nmid 1 - \sqrt{-5}$ . Hence, 2 does not divide  $1 \pm \sqrt{-5}$ , so 2 is not prime. The result now follows from Proposition 6.17.  $\square$