E. Dummit's Math 4527 ~ Number Theory 2, Spring 2025 ~ Homework 6 Solutions

1. In each given quadratic integer ring, determine which of the given elements are units, which are irreducible, and which are reducible. Also, for the units, compute their multiplicative inverses, and for the reducible elements find a nontrivial factorization.

   (a) $R = \mathbb{Z}[i]$, elements $4-i$, $3+i$, $3-2i$, 7.

   - We have $N(4-i) = 17$ which is prime so $\boxed{4-i \text{ is irreducible}}$.
   - We have $N(3+i) = 10 = 2 \cdot 5$ which is not prime. There do exist elements of norm 2 (namely $1+i$) and 5 (namely $2 \pm i$), and indeed we can divide $(3+i)/(1+i) = 2-i$, so $\boxed{3+i \text{ is reducible}}$ and we get a nontrivial factorization $3+i = (1+i)(2-i)$.
   - We have $N(3-2i) = 13$ which is prime so $\boxed{3-2i \text{ is irreducible}}$.
   - We have $N(7) = 49$ which is not prime. However, any nontrivial factorization would have to be into a product of two elements of norm 7, but there are no such elements because there are no integer solutions to $a^2 + b^2 = 7$. Thus $\boxed{7 \text{ is irreducible}}$.

   (b) $R = \mathcal{O}_{\sqrt{-3}}$, elements $\dfrac{1+\sqrt{-3}}{2}$, $2+\sqrt{-3}$, $3+\sqrt{-3}$, $\dfrac{5+\sqrt{-3}}{2}$.

   - We have $N(\dfrac{1+\sqrt{-3}}{2}) = 1$ which is a unit, so $\boxed{\dfrac{1+\sqrt{-3}}{2} \text{ is a unit}}$. Its inverse is $\dfrac{1-\sqrt{-3}}{2}$.
   - We have $N(2+\sqrt{-3}) = 7$ which is prime so $\boxed{2+\sqrt{-3} \text{ is irreducible}}$.
   - We have $N(3+\sqrt{-3}) = 12$ which is not prime. There are no elements of norm 2 but there are elements of norm 3 (e.g., $\pm\sqrt{-3}$) and 4 (e.g., $1 \pm \sqrt{-3}$). Indeed, we can divide $(3+\sqrt{-3})/\sqrt{-3} = 1-\sqrt{-3}$, so $\boxed{3+\sqrt{-3} \text{ is reducible}}$ and we get a nontrivial factorization $3+\sqrt{-3} = (\sqrt{-3})(1-\sqrt{-3})$.
   - We have $N(\dfrac{5+\sqrt{-3}}{2}) = 7$ which is prime so $\boxed{\dfrac{5+\sqrt{-3}}{2} \text{ is irreducible}}$.

   (c) $R = \mathcal{O}_{\sqrt{5}}$, elements $2+\sqrt{5}$, $3-2\sqrt{5}$, $7+5\sqrt{5}$, $1+\sqrt{5}$.

   - We have $N(2+\sqrt{5}) = -1$ which is a unit in $\mathbb{Z}$, so $\boxed{2+\sqrt{5} \text{ is a unit}}$. Its inverse is $-2+\sqrt{5}$.
   - We have $N(3-2\sqrt{5}) = -11$ which is a negative prime so $\boxed{3-2\sqrt{5} \text{ is irreducible}}$.
   - We have $N(7+5\sqrt{5}) = -76$ which is not prime, so we have various potential factorizations. One could search systematically for elements of norm dividing -76 but this is not really necessary since we have an obvious factorization $7+5\sqrt{5} = \dfrac{7+5\sqrt{5}}{2} \cdot 2$. Thus, $\boxed{7+5\sqrt{5} \text{ is reducible}}$.
   - We have $N(1+\sqrt{5}) = -4$ which is not prime, so we could have a factorization as a product of an element of norm 2 with an element of norm -2. However, if $N(\dfrac{a+b\sqrt{5}}{2}) = 2$ then we would have $a^2 - 5b^2 = 8$, and there are no solutions to this equation because it says $a^2 \equiv 3 \pmod{5}$, impossible. Thus, $\boxed{1+\sqrt{5} \text{ is irreducible}}$.

   (d) $R = \mathcal{O}_{\sqrt{7}}$, elements $2-\sqrt{7}$, $3+\sqrt{7}$, $1+\sqrt{7}$, $8-3\sqrt{7}$.

   - We have $N(2-\sqrt{7}) = -3$ which is a negative prime so $\boxed{2-\sqrt{7} \text{ is irreducible}}$.
   - We have $N(3+\sqrt{7}) = 2$ which is prime so $\boxed{3+\sqrt{7} \text{ is irreducible}}$.
   - We have $N(1+\sqrt{7}) = 6$ which is not prime, so we have various potential factorizations (either norm 2 times norm 3 or norm -2 times norm -3). Noting the two elements we just identified have such norms, we try dividing $(1+\sqrt{7})/(2-\sqrt{7}) = -3-\sqrt{7}$. This yields a nontrivial factorization $1+\sqrt{7} = (2-\sqrt{7})(-3-\sqrt{7})$ so $\boxed{1+\sqrt{7} \text{ is reducible}}$.
   - We have $N(8-3\sqrt{7}) = 1$ which is a unit, so $\boxed{8-3\sqrt{7} \text{ is a unit}}$. Its inverse is $8+3\sqrt{7}$.

2. For each pair of elements a, b in the given Euclidean domain R, find a greatest common divisor d and write it in the form $d = xa + yb$ for some $x, y \in R$. (You may wish to work through problems 4 and 5 before doing parts (c), (d), and (e).)

   (a) $R = \mathbb{Z}[i]$, $a = 57 + 17i$, $b = 26 + 22i$.

   - First, $\dfrac{57+17i}{26+22i} = \dfrac{8}{5} - \dfrac{7}{10}i$, so rounding to the nearest Gaussian integer yields the quotient $2 - i$, and the remainder is then $(57 + 17i) - (2 - i)(26 + 22i) = -17 - i$.
   - Next, $\dfrac{26+22i}{-17-i} = -\dfrac{8}{5} - \dfrac{6}{5}i$, so rounding to the nearest Gaussian integer yields the quotient $-2 - i$, and the remainder is then $(26 + 22i) - (-2 - i)(-17 - i) = -7 + 3i$.
   - Finally, since $\dfrac{-17-i}{-7+3i} = 2 + i$, the quotient is $2 + i$ and the remainder is 0.
   - The last nonzero remainder is $\boxed{-7+3i}$ so it is a gcd. To express the gcd as a linear combination, we solve for the remainders:

   $$\begin{aligned} -17 - i &= 1 \cdot (57 + 17i) - (2 - i) \cdot (26 + 22i) \\ -7 + 3i &= 1 \cdot (26 + 22i) - (-2 - i)(-17 - i) \\ &= 1 \cdot (26 + 22i) - (-2 - i)\,[1 \cdot (57 + 17i) - (2 - i) \cdot (26 + 22i)] \\ &= -4 \cdot (26 + 22i) + (2 + i) \cdot (57 + 17i) \end{aligned}$$

   and so we have $-7 + 3i = \boxed{-4 \cdot (26 + 22i) + (2 + i) \cdot (57 + 17i)}$.

   (b) $R = \mathbb{Z}[i]$, $a = 9 + 43i$, $b = 22 + 10i$.

   - First, $\dfrac{9+43i}{22+10i} = \dfrac{157}{146} + \dfrac{107}{73}i$, so rounding to the nearest Gaussian integer yields the quotient $1 + i$, and the remainder is then $(9 + 43i) - (1 + i)(22 + 10i) = -3 + 11i$.
   - Next, $\dfrac{22+10i}{-3+11i} = \dfrac{22}{65} - \dfrac{136}{65}i$, so rounding to the nearest Gaussian integer yields the quotient $-2i$, and the remainder is then $(22 + 10i) - (-2i)(-3 + 11i) = 4i$.
   - Next, $\dfrac{-3+11i}{4i} = \dfrac{11}{4} + \dfrac{3}{4}i$, so rounding to the nearest Gaussian integer yields the quotient $3 + i$, and the remainder is then $(-3 + 11i) - (3 + i)(4i) = 1 - i$.
   - Finally, $\dfrac{4i}{1-i} = -2 + 2i$, so the quotient is $-2 + 2i$ and the remainder is 0.
   - The last nonzero remainder is $\boxed{1-i}$ so it is a gcd. Backsolving yields

   $$\begin{aligned} -3 + 11i &= 1 \cdot (9 + 43i) - (1 + i) \cdot (22 + 10i) \\ 4i &= (22 + 10i) - (-2i)\,[1 \cdot (9 + 43i) - (1 + i) \cdot (22 + 10i)] \\ &= (3 - 2i) \cdot (22 + 10i) + (2i) \cdot (9 + 43i) \\ 1 - i &= [1 \cdot (9 + 43i) - (1 + i) \cdot (22 + 10i)] - (3 + i)\,[(3 - 2i) \cdot (22 + 10i) + (2i) \cdot (9 + 43i)] \\ &= (3 - 6i) \cdot (9 + 43i) + (-12 + 2i) \cdot (22 + 10i) \end{aligned}$$

   and so we have $1 - i = \boxed{(3 - 6i) \cdot (9 + 43i) + (-12 + 2i) \cdot (22 + 10i)}$.

   (c) $R = \mathbb{Z}[\sqrt{-2}]$, $a = 33 + 5\sqrt{-2}$, $b = 8 + 11\sqrt{-2}$.

   - First, $\dfrac{33+5\sqrt{-2}}{8+11\sqrt{-2}} = \dfrac{11}{9} - \dfrac{19}{18}\sqrt{-2}$, so rounding to the nearest element of R yields the quotient $1 - \sqrt{-2}$, and the remainder is then $(33 + 5\sqrt{-2}) - (1 - \sqrt{-2})(8 + 11\sqrt{-2}) = 3 + 2\sqrt{-2}$.
   - Then $\dfrac{8+11\sqrt{-2}}{3+2\sqrt{-2}} = 4 + \sqrt{-2}$, and so the quotient is $4 + \sqrt{-2}$ and the remainder is 0.
   - The last nonzero remainder is $\boxed{3+2\sqrt{-2}}$ so it is a gcd.
   - Backsolving yields $3 + 2\sqrt{-2} = \boxed{1 \cdot (33 + 5\sqrt{-2}) - (1 - \sqrt{-2})(8 + 11\sqrt{-2})}$.

(d) $R = \mathbb{Z}[\sqrt{2}]$, $a = 31 + 15\sqrt{2}$, $b = 10 + \sqrt{2}$.

- First, $\dfrac{31+15\sqrt{2}}{10+\sqrt{2}} = \dfrac{20}{7} + \dfrac{17}{14}\sqrt{2}$, so rounding to the nearest element of R yields the quotient $3+\sqrt{2}$, and the remainder is then $(31+15\sqrt{2}) - (3+\sqrt{2})(10+\sqrt{2}) = -1+2\sqrt{2}$.
- Then $\dfrac{10+\sqrt{2}}{-1+2\sqrt{2}} = 2+3\sqrt{2}$, and so the quotient is $2+3\sqrt{2}$ and the remainder is 0.
- The last nonzero remainder is $\boxed{-1+2\sqrt{2}}$ so it is a gcd.
- Backsolving yields $-1+2\sqrt{2} = \boxed{1\cdot(31+15\sqrt{2}) - (3+\sqrt{2})(10+\sqrt{2})}$.

(e) $R = \mathcal{O}_{\sqrt{-3}}$, $a = 19+\sqrt{-3}$, $b = 14+7\sqrt{-3}$.

- First, $\dfrac{19+\sqrt{-3}}{14+7\sqrt{-3}} = \dfrac{41}{49} - \dfrac{17}{49}\sqrt{-3}$, so rounding to the nearest element of R yields the quotient $\dfrac{1}{2} - \dfrac{1}{2}\sqrt{-3}$, and the remainder is then $(19+\sqrt{-3}) - (\frac{1}{2} - \frac{1}{2}\sqrt{-3})(14+7\sqrt{-3}) = \dfrac{3}{2} + \dfrac{9}{2}\sqrt{-3}$.
- Then $\dfrac{14+7\sqrt{-3}}{(3+9\sqrt{-3})/2} = \dfrac{11}{6} - \dfrac{5}{6}\sqrt{-3}$, so rounding to the nearest element of R yields the quotient $2-\sqrt{-3}$, and the remainder is then $(14+7\sqrt{-3}) - (2-\sqrt{-3})(\frac{3}{2}+\frac{9}{2}\sqrt{-3}) = -\dfrac{5}{2} - \dfrac{1}{2}\sqrt{-3}$.
- Finally, $\dfrac{(3+9\sqrt{-3})/2}{(-5-\sqrt{-3})/2} = -\dfrac{3}{2} - \dfrac{3}{2}\sqrt{-3} \in R$, so this is the quotient and the remainder is zero.
- The last nonzero remainder is $\boxed{-\dfrac{5}{2} - \dfrac{1}{2}\sqrt{-3}}$ so it is a gcd.
- Backsolving yields $-\dfrac{5}{2} - \dfrac{1}{2}\sqrt{-3} = \boxed{(-2+\sqrt{-3})\cdot(19+\sqrt{-3}) + \dfrac{1-3\sqrt{-3}}{2}\cdot(14+7\sqrt{-3})}$.

---

3. Show that the rings $(\mathbb{Z}/15\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})$ and $(\mathbb{Z}/24\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ are isomorphic.

- By the Chinese remainder theorem, $\mathbb{Z}/15\mathbb{Z} \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$, and $(\mathbb{Z}/24\mathbb{Z}) \cong (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.
- Thus, both rings are isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})$, and hence are isomorphic to each other.
- Alternatively, both rings are isomorphic to $\mathbb{Z}/120\mathbb{Z}$.

---

4. Let $R = \mathbb{Z}[\sqrt{-2}]$, and let $a+b\sqrt{-2}$ and $c+d\sqrt{-2}$ be elements of R with $c+d\sqrt{-2} \neq 0$.

(a) Show that $\dfrac{a+b\sqrt{-2}}{c+d\sqrt{-2}} = x+y\sqrt{-2}$ for rational x, y. Then let s be the closest integer to x and t be the closest integer to y, and set $q = s+t\sqrt{-2}$ and $r = (a+b\sqrt{-2}) - (s+t\sqrt{-2})(c+d\sqrt{-2})$. Prove also that $N(r) \le \dfrac{3}{4}N(c+d\sqrt{-2})$.

- First, we rationalize the denominator: $\dfrac{a+b\sqrt{-2}}{c+d\sqrt{-2}} = \dfrac{(a+b\sqrt{-2})(c-d\sqrt{-2})}{c^2+2d^2} = \dfrac{ac+2bd}{c^2+2d^2} + \dfrac{bc-ad}{c^2+2d^2}\sqrt{-2}$.
- Now note $\dfrac{r}{c+d\sqrt{-2}} = \dfrac{a+b\sqrt{-2}}{c+d\sqrt{-2}} - q = (x-s)+(y-t)\sqrt{-2}$ and $|x-s| \le \dfrac{1}{2}$ and $|y-t| \le \dfrac{1}{2}$.
- Then $N\left(\dfrac{r}{c+d\sqrt{-2}}\right) = N[(x-s)+(y-t)\sqrt{-2}] = (x-s)^2 + 2(y-t)^2 \le \dfrac{1}{4} + 2\cdot\dfrac{1}{4} = \dfrac{3}{4}$.
- Since N is multiplicative, by rearranging we immediately obtain $N(r) \le \dfrac{3}{4}N(c+d\sqrt{-2})$ as required.

(b) Show that R is a Euclidean domain.

- By part (a), N is a norm yielding a division algorithm on R, since the norm of the remainder term is less than the norm of $c + d\sqrt{-2}$.

(c) Show that $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ are also Euclidean domains under the absolute value of the field norm $\left|N(a + b\sqrt{D})\right| = \left|a^2 - Db^2\right|$.

- In the same way we can rationalize the denominator to see $\dfrac{a + b\sqrt{D}}{c + d\sqrt{D}} = x + y\sqrt{D}$ with s, t the nearest integers to x, y, and we take $q = s + t\sqrt{D}$ and $r = (a + b\sqrt{D}) - (s + t\sqrt{D})(c + d\sqrt{D})$.
- Then $\left|N\left(\dfrac{r}{c + d\sqrt{D}}\right)\right| = \left|N[(x - s) + (y - t)\sqrt{D}]\right| = \left|(x - s)^2 - D(y - t)^2\right| \le \dfrac{D}{4} < 1$. Thus $N(r) < N(b)$, so this norm function makes R into a Euclidean domain.

---

5. The goal of this problem is to prove that $\mathcal{O}_{\sqrt{-D}}$ is a Euclidean domain for $-D = -3$, -7, and -11, which extends the result of problem 4 (establishing this fact for $-D = -2$, 2, and 3).

(a) Suppose ABC is an acute triangle. Show that the point P inside ABC that maximizes the distance to the nearest vertex of ABC is the circumcenter (i.e., the center of the circle through the vertices of ABC, or equivalently, the point O such that $OA = OB = OC$).

- Let r be the circumradius of ABC. If we draw a circle of radius r centered at each vertex of ABC, then these circles cover all of ABC, so every point inside ABC is within a distance r of at least one of the three vertices of ABC. On the other hand, the circumcenter of ABC is a distance r from all three vertices. Therefore, the maximal possible distance is r, and it is attained at the circumcenter.
- This result can also be proven variationally: if $PA < PC \le PB$, then moving P towards the perpendicular bisector of AB along a circle centered at C will increase the minimum distance, and then if $PA = PC \le PB$, moving P along the perpendicular bisector towards the circumcenter will also increase the minimum distance. Thus, the maximum value of the minimal distance must occur at the circumcenter.

(b) Suppose that $-D = -3$, -7, or -11. Prove that any complex number $z \in \mathbb{C}$ differs from an element in $\mathcal{O}_{\sqrt{-D}}$ by a complex number whose norm (i.e., the square of its absolute value) is at most $\dfrac{(1 + D)^2}{16D}$. [Hint: The elements of $\mathcal{O}_{\sqrt{-D}}$ form a lattice Λ in the complex plane. Identify a fundamental region for this lattice and then use symmetry to reduce the minimal distance calculation to part (a).]

- As noted in the hint, the elements of $\mathcal{O}_{\sqrt{-D}} = \{a + b\frac{1+\sqrt{-D}}{2} \ : \ a, b \in \mathbb{Z}\}$ form a lattice Λ in the complex plane with basis vectors 1 and $\frac{1+\sqrt{-D}}{2}$. Therefore, since we only care about differences between a complex number $z \in \mathbb{C}$ and elements of Λ, we can equivalently compute the greatest possible distance between a point in a fundamental domain for $\mathbb{C}/\Lambda$ with one of the boundary vertices.
- The fundamental domain is a parallelogram with vertices 0, 1, $\frac{1+\sqrt{-D}}{2}$, and $\frac{3+\sqrt{-D}}{2}$: we wish to compute the maximum possible distance between a point in the fundamental domain and the nearest of these four vertices.
- By symmetry, we may assume the point is in the triangle formed by 0, 1, $\frac{1+\sqrt{-D}}{2}$. Then by part (a), the maximum possible distance is the distance from the circumcenter to any of the vertices.
- It is then a straightforward geometric calculation to check that the circumcenter is $O = \dfrac{1}{2} + \dfrac{\sqrt{-D} - 1/\sqrt{-D}}{4}i$ and the circumradius is $r = \dfrac{\sqrt{-D} + 1/\sqrt{-D}}{4}$ (it is not hard to see that the distance between O and the three listed vertices is equal to r).
- Thus, any complex number $z \in \mathbb{C}$ differs from an element in $\mathcal{O}_{\sqrt{-D}}$ by a complex number whose norm (i.e., the square of its absolute value) is at most $r^2 = \dfrac{(1 + D)^2}{16D}$, as claimed.

(c) Prove that $\mathcal{O}_{\sqrt{-D}}$ is a Euclidean domain for $-D = -3$, -7, and -11. [Hint: Adapt the proof in 4b.]

- Suppose we are dividing $a+b\sqrt{-D}$ by $c+d\sqrt{-D}$. If we compute $\dfrac{a+b\sqrt{-D}}{c+d\sqrt{-D}} = x+y\sqrt{-D}$, then by the result of (b), there exists an element $\alpha \in \mathcal{O}_{\sqrt{-D}}$ such that $N(x+y\sqrt{-D}) \le \dfrac{(1+D)^2}{16D} < 1$ for each of the values $D = -3, -7, -11$.
- Then we can take the quotient $q = \alpha$ and remainder $r = (a+b\sqrt{-D}) - \alpha(c+d\sqrt{-D}) = x+y\sqrt{-D}$. Then $N\left[\dfrac{r}{c+d\sqrt{-D}}\right] = N(x+y\sqrt{-D}) < 1$ and so $N(r) < N(c+d\sqrt{-D})$ as required.
- Thus, $\mathcal{O}_{\sqrt{-D}}$ is a Euclidean domain as claimed.

---

6. The goal of this problem is to prove that for any squarefree integer $D \ge 3$, the ring $\mathbb{Z}[\sqrt{-D}]$ is not a unique factorization domain, generalizing the technique used for $D = 5$.

(a) Show that $\sqrt{-D}$, $1+\sqrt{-D}$, $1-\sqrt{-D}$, and 2 are irreducible elements in $\mathbb{Z}[\sqrt{-D}]$. [Hint: For the first three, show that the only elements of norm less than D are integers.]

- Note that $N(1 \pm \sqrt{-D}) = D+1$ and $N(\sqrt{-D}) = D$. Furthermore, note that $N(a+b\sqrt{-D}) = a^2+Db^2$, so the only elements of norm less than D have $b = 0$.
- Then if $r = a+b\sqrt{-D}$ and $s = c+d\sqrt{-D}$ give a nontrivial factorization $rs = 1 \pm \sqrt{-D}$, since $N(r)N(s) = D+1$ and $D^2 > D+1$, we see that one of r, s must have norm less than D hence be an integer. But clearly, there are no integers other than ± 1 that divide $1 \pm \sqrt{-D}$.
- In the same way, we see that $\sqrt{-D}$ cannot have a nontrivial factorization either, since it is not divisible by any integers other than ± 1.
- For 2, since $N(2) = 4$, the only nontrivial factorization would be into two elements of norm 2. But there are no integer solutions to $a^2+Db^2 = 2$ for any $D > 3$.

(b) Show that either D (if D is even) or $D+1$ (if D is odd) has two different factorizations into irreducibles in $\mathbb{Z}[\sqrt{-D}]$, and deduce that $\mathbb{Z}[\sqrt{-D}]$ is not a unique factorization domain.

- If D is even, then we can write $D = (-\sqrt{-D}) \cdot (\sqrt{-D}) = 2 \cdot$ [stuff], while if D is odd then we can write $D+1 = (1+\sqrt{-D}) \cdot (1-\sqrt{-D}) = 2 \cdot$ [stuff].
- By part (a) we know that the two factorizations cannot be equivalent, because 2 is not an associate of $\sqrt{-D}$ or $1 \pm \sqrt{-D}$, since (for example) they do not have the same norm.

(c) What goes wrong if you try to use the proof to show that $\mathbb{Z}[\sqrt{D}]$ is not a UFD for squarefree $D \ge 3$?

- The problem is that there could be many elements of small norm, because $N(a+b\sqrt{D}) = a^2-Db^2$, and so it is not necessarily true that the elements $1 \pm \sqrt{D}$ are irreducible.
- For example, in $\mathbb{Z}[\sqrt{7}]$, we have $1+\sqrt{7} = (3+\sqrt{7}) \cdot (-2+\sqrt{7})$, and both of the elements on the right have prime norm (so they are irreducible, while $1+\sqrt{7}$ is not).

---

7. [Challenge] Let $R = \mathbb{Z}[\sqrt{-3}]$ and let $I = (2, 1+\sqrt{-3})$ in R.

(a) Show that $I^2 = (2)I$ in R but that $I \ne (2)$.

- We have $I^2 = (4, 2(1+\sqrt{-3}), -2+2\sqrt{-3}) = (4, 2(1+\sqrt{-3})) = (2)I$ since $-2+2\sqrt{-3} = 2(1+\sqrt{-3})-4$.
- However, $I \ne (2)$ since I contains $1+\sqrt{-3}$, while (2) does not.

(b) Show that there are two residue classes in R/I and deduce that I is a prime ideal.

- Since I contains $1+\sqrt{-3}$, in R/I we have $a+b\sqrt{-3} \equiv a-b$, and since I contains 2 we see that each residue class is represented by 0 or 1.
- Furthermore, since $I \ne R$ (since for example I does not contain 1) we conclude that R/I has two residue classes. Thus, by problem 7 of homework 5, we conclude $R/I \cong \mathbb{Z}/2\mathbb{Z}$ and so I is a prime ideal.

(c) Show that I is the unique proper ideal of R properly containing (2) and also the unique prime ideal of R containing (2). [Hint: Consider the ideals of $R/(2)$ and use the correspondence between ideals of R containing J and ideals of R/J.]

- By the correspondence theorem, the ideals of $R/(2)$ correspond to the ideals of R containing (2). We are searching for nontrivial proper ideals of $R/(2)$.
- Observe that there are four residue classes in $R/(2)$, represented by 0, 1, $\sqrt{-3}$, and $1+\sqrt{-3}$. Both 1 and $\sqrt{-3}$ are units while $(1+\sqrt{-3})^2 = 0$, so we see that the only nontrivial proper ideal of $R/(2)$ is $(1+\sqrt{-3})$.
- Thus, the only proper ideal of R properly containing (2) is $(2, 1+\sqrt{-3})$.
- Furthermore, since $R/(2)$ contains a zero divisor, we see that (2) is not a prime ideal of R. So since the other proper ideal of R containing (2) is I, and I is prime by (b), I is the only prime ideal of R containing I.

(d) Show that (2) cannot be written as a product of prime ideals of R.

- If $(2) = P_1 \cdots P_n$ for some prime ideals P_i, then each P_i would contain (2), hence by (c) we have $P_i = I$ for each i.
- But then we would have $(2) = I^n$ for some n. However $I^n = (2^{n-1})I \neq (2)$ by a trivial induction using part (a).
- This is a contradiction, so (2) cannot be written as a product of prime ideals of R.

Remark: This problem illustrates that factorization into prime ideals can fail if we do not work in the full quadratic integer ring. Working in the correct ring $\mathcal{O}_{\sqrt{-3}} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ will solve the issues that arise in this example, since in fact $I = (2)$ is a prime ideal inside $\mathcal{O}_{\sqrt{-3}}$ because 2 and $1+\sqrt{-3}$ are now associates.