E. Dummit's Math 4527 ~ Number Theory 2, Fall 2026 ~ Homework 7 Solutions

---

1. Find the prime ideal factorizations of each ideal in the given quadratic integer ring:

   (a) The ideals (2), (3), (5), and (7) in $\mathcal{O}_{\sqrt{-5}} = \mathbb{Z}[\sqrt{-5}]$.

   - For (2) we consider $x^2 + 5$ modulo 2: since it has a repeated root 1, we see $(2) = \boxed{(2, \sqrt{-5} - 1)^2}$.
   - For (3) we consider x^2+5 modulo 3: since it has roots 1 and 2, we get $(3) = \boxed{(3, \sqrt{-5} - 1) \cdot (3, \sqrt{-5} - 2)}$.
   - For (5) we consider $x^2 + 5$ modulo 5: since it has a repeated root 0, we get $(5) = \boxed{(\sqrt{-5})^2}$.
   - For (7) we consider x^2+5 modulo 7: since it has roots 3 and 4, we get $(7) = \boxed{(7, \sqrt{-5} - 3) \cdot (7, \sqrt{-5} - 4)}$.

   (b) The ideals (2), (3), (5), and (7) in $\mathcal{O}_{\sqrt{6}} = \mathbb{Z}[\sqrt{6}]$.

   - For (2) we consider $x^2 - 6$ modulo 2: since it has a repeated root 0, we see $(2) = \boxed{(2, \sqrt{6})^2}$.
   - For (3) we consider $x^2 - 6$ modulo 3: since it has a repeated root 0, we see $(3) = \boxed{(3, \sqrt{6})^2}$.
   - For (5) we consider x^2-6 modulo 5: since it has roots 1 and 4, we get $(5) = \boxed{(5, \sqrt{6} - 1) \cdot (5, \sqrt{6} - 4)}$.
   - For (7) we consider $x^2 - 6$ modulo 7: since it is irreducible, we see $\boxed{(7) \text{ is prime}}$.

   (c) The ideals (2), (3), (5), and (7) in $\mathcal{O}_{\sqrt{-11}} = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$.

   - For (2) we consider $x^2 - x + 3$ modulo 2: since it is irreducible, we see $\boxed{(2) \text{ is prime}}$.
   - For (3) we consider x^2-x+3 modulo 3: since it has roots 0 and 1, we get $(3) = \boxed{(3, \frac{1+\sqrt{-11}}{2}) \cdot (3, \frac{1+\sqrt{-11}}{2} - 1)}$.
   - For (5) we consider x^2-x+3 modulo 5: since it has roots 2 and 4, we get $(5) = \boxed{(5, \frac{1+\sqrt{-11}}{2} - 2) \cdot (5, \frac{1+\sqrt{-11}}{2} - 4)}$.
   - For (7) we consider $x^2 - x + 3$ modulo 7: since it is irreducible, we see $\boxed{(7) \text{ is prime}}$.

---

2. Solve the following problems related to factorization:

   (a) Find prime factorizations of $12 + 31i$, $183 - 12i$, $75 - 11i$, and $28 - 4i$ in $\mathbb{Z}[i]$.

   - First, $N(12+31i) = 5 \cdot 13 \cdot 17$. Since $5 = (2+i)(2-i)$, $13 = (3+2i)(3-2i)$, and $17 = (4+i)(4-i)$, checking which of these divide $12+31i$, and to which powers, yields $12+31i = \boxed{i(2+i)(3-2i)(4-i)}$.
   - Second, $N(183 - 12i) = 3^2 \cdot 37 \cdot 101$. Since $37 = (6+i)(6-i)$ and $101 = (10+i)(10-i)$, checking which of these divide $183 - 12i$, and to which powers, yields $183 - 12i = \boxed{3(6-i)(10+i)}$.
   - Fourth, $N(75-11i) = 2 \cdot 13^2 \cdot 17$. Since $2 = -i(1+i)^2$, $13 = (3+2i)(3-2i)$, and $17 = (4+i)(4-i)$, checking which of these divide $75-11i$, and to which powers, yields $75-11i = \boxed{(1+i)(3-2i)^2(4+i)}$.
   - Finally, $N(28-4i) = 2^5 5^2$. Since $2 = -i(1+i)^2$ and $5 = (1+2i)(1-2i)$, checking which of these divide $28 - 4i$, and to which powers, yields $28 - 4i = \boxed{(1+i)^5(1+2i)^2}$.

   (b) Find representations of the primes 2909 and 8161 as the sum of two squares of integers.

   - First we must solve $n^2 \equiv -1 \pmod{p}$, which we can do by computing $a^{(p-1)/4} \bmod p$ where a is a quadratic nonresidue modulo p, and then we compute the gcd of $n+i$ and p in $\mathbb{Z}[i]$.
   - For $p = 2909$ we compute $2^{(p-1)/4} \equiv 2031 \pmod{p}$, so we can take the smaller solution $n = -2031 \equiv 878 \pmod{p}$. Then we use the Euclidean algorithm:

$$\begin{aligned} 2909 &= 3(878+i) + (275-3i) \\ 878+i &= 3(275-3i) + (53+10i) \\ 275-3i &= (5-i)(53+10i) \end{aligned}$$

   The last nonzero remainder is $53 + 10i$, and indeed we can see that $2909 = \boxed{53^2 + 10^2}$.

- For $p = 8161$ we see 2, 3, and 5 are all quadratic residues, but $7^{(p-1)/4} \equiv 7959 \pmod{p}$, so we can take the smaller solution $n = -7959 \equiv 202 \pmod{p}$. Then we use the Euclidean algorithm:

$$\begin{aligned} 8161 &= 40(202+i) + (81-40i) \\ 202+i &= (2+i)(81-40i) \end{aligned}$$

  The last nonzero remainder is $81 - 40i$, and indeed we can see that $8161 = \boxed{81^2 + 40^2}$.

(c) Find prime factorizations for $70 + 60\sqrt{-2}$, $49 - 46\sqrt{-2}$, and 193 in $\mathbb{Z}[\sqrt{-2}]$.

- We have $N(70 + 60\sqrt{-2}) = 70^2 + 2 \cdot 60^2 = 2^2 5^2 11^2$. We have the irreducible factorizations $2 = -(\sqrt{-2})^2$, and $11 = (3 + \sqrt{-2})(3 - \sqrt{-2})$, while 5 is irreducible. Testing possible divisors yields $70 + 60\sqrt{-2} = \boxed{-(\sqrt{-2})^2 \cdot 5 \cdot (3 + \sqrt{-2})^2}$.
- We have $N(49 - 46\sqrt{-2}) = 49^2 + 2 \cdot 46^2 = 3^2 11 \cdot 67$. We have the irreducible factorizations $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$, $11 = (3 + \sqrt{-2})(3 - \sqrt{-2})$, and $67 = (7 + 3\sqrt{-2})(7 - 3\sqrt{-2})$. Testing possible divisors yields $49 - 46\sqrt{-2} = \boxed{(1 - \sqrt{-2})^2(3 + \sqrt{-2})(7 + 3\sqrt{-2})}$.
- Note that 193 is prime and congruent to 1 modulo 8, so it factors in $\mathbb{Z}[\sqrt{-2}]$. We can either solve $x^2 + 2 \equiv 0 \pmod{193}$ to get $x \equiv \pm 34$ and then use the Euclidean algorithm on 193 and $34 + \sqrt{-2}$ to get a gcd of $11 + 6\sqrt{-2}$ after one step, or just search for solutions of $193 = a^2 + 2b^2$ directly to see $193 = 11^2 + 2 \cdot 6^2$ and thus $193 = \boxed{(11 + 6\sqrt{-2})(11 - 6\sqrt{-2})}$.

(d) Find prime factorizations for $70 + 60\sqrt{-3}$, $48 + 46\sqrt{-3}$, and 193 in $\mathcal{O}_{\sqrt{-3}}$.

- We have $N(70 + 60\sqrt{-3}) = 70^2 + 3 \cdot 60^2 = 2^2 5^2 157$. In $\mathcal{O}_{\sqrt{-3}}$ both 2 and 5 are irreducible, while 157 is a prime congruent to 1 modulo 3 so it splits, and simply looking at our element yields $157 = (7 + 6\sqrt{-3})(7 - 6\sqrt{-3})$. Then we get the factorization $70 + 60\sqrt{-3} = \boxed{2 \cdot 5 \cdot (7 + 6\sqrt{-3})}$.
- We have $N(48 + 46\sqrt{-3}) = 48^2 + 3 \cdot 46^2 = 2^2 \cdot 3 \cdot 7 \cdot 103$. The element 2 is irreducible, while $3 = -(\sqrt{-3})^2$, $7 = (2 + \sqrt{-3})(2 - \sqrt{-3})$, and $103 = (10 + \sqrt{-3})(10 - \sqrt{-3})$. Testing possible divisors yields $48 + 46\sqrt{-3} = \boxed{-2(\sqrt{-3})(2 - \sqrt{-3})(10 + \sqrt{-3})}$.
- Note that 193 is prime and congruent to 1 modulo 3, so it factors in $\mathbb{Z}[\sqrt{-3}]$. We can either solve $x^2 + 3 \equiv 0 \pmod{193}$ to get $x \equiv \pm 24$ and then use the Euclidean algorithm on 193 and $24 + \sqrt{-3}$ to get a gcd of $1 + 8\sqrt{-2}$ after one step, or just search for solutions of $193 = a^2 + 3b^2$ directly to see $193 = 1^2 + 3 \cdot 8^2$ and thus $193 = \boxed{(1 + 8\sqrt{-3})(1 - 8\sqrt{-3})}$.

(e) Determine whether the integers 117, 263, and 950 can be written in the form $a^2 + b^2$ for integers a, b.

- We have $117 = 3^2 \cdot 13$ so since 13 is congruent to 1 modulo 4, it $\boxed{\text{can be written}}$ as $a^2 + b^2$.
- The integer 263 is prime and congruent to 3 modulo 4, so it $\boxed{\text{cannot be written}}$ as $a^2 + b^2$.
- We have $950 = 2 \cdot 5^2 \cdot 19$ so since 19 is congruent to 3 modulo 4, it $\boxed{\text{cannot be written}}$ as $a^2 + b^2$.

(f) Determine whether the integers 117, 263, and 950 can be written in the form $a^2 + 2b^2$ for integers a, b.

- We have $117 = 3^2 \cdot 13$ so since 13 is congruent to 5 modulo 8, it $\boxed{\text{cannot be written}}$ as $a^2 + 2b^2$.
- The integer 263 is prime and congruent to 7 modulo 8, so it $\boxed{\text{cannot be written}}$ as $a^2 + 2b^2$.
- We have $950 = 2 \cdot 5^2 \cdot 19$ so since 19 is congruent to 3 modulo 8, it $\boxed{\text{can be written}}$ as $a^2 + 2b^2$.

(g) Determine whether the integers 117, 263, and 950 can be written in the form $a^2 + 3b^2$ for integers a, b.

- We have $117 = 3^2 \cdot 13$ so since 13 is congruent to 1 modulo 3, it $\boxed{\text{can be written}}$ as $a^2 + 3b^2$.
- The integer 263 is prime and congruent to 2 modulo 3, so it $\boxed{\text{cannot be written}}$ as $a^2 + 3b^2$.
- We have $950 = 2 \cdot 5^2 \cdot 19$ so since 2 is congruent to 2 modulo 3, it $\boxed{\text{cannot be written}}$ as $a^2 + 3b^2$.

---

3. Let $R = \mathbb{Z}[\sqrt{-14}]$, and let $I_3 = (3, 1+\sqrt{-14})$, $I_3' = (3, 1-\sqrt{-14})$, $I_5 = (5, 1+\sqrt{-14})$, and $I_5' = (5, 1-\sqrt{-14})$.

   (a) Show that the elements 3, 5, and $1 \pm \sqrt{-14}$ are nonassociate irreducible elements of R, and that 15 has two inequivalent factorizations into irreducible elements in R. Deduce that R is not a UFD or a PID.

   - Since $N(a+b\sqrt{-14}) = a^2+14b^2$, we have $N(3) = 9$, $N(5) = 25$, and $N(1 \pm \sqrt{-14}) = 15$. Since there are no elements of R having norm 3 or 5, there are no nontrivial factorizations of 3, 5, or $1 \pm \sqrt{-14}$, and so these elements are irreducible.
   - We have $15 = 3 \cdot 5 = (1+\sqrt{-14}) \cdot (1-\sqrt{-14})$, and each factor is irreducible and none of them are associate (since the only units in R are ± 1), so the factorizations are not equivalent. Thus, R is not a UFD, hence also not a PID.

   (b) Show that I_3 and I_3' are both prime ideals of R and that $I_3 I_3'$ is the principal ideal (3).

   - We can do these calculations directly, but it is simpler to use Dedekind-Kummer: the minimal polynomial $x^2 + 14$ of $\sqrt{-14}$ factors modulo 3 as $(x-1)(x+1)$ and therefore (3) splits as $(1+\sqrt{-14}, 3) \cdot (-1+\sqrt{-14}, 3) = I_3 I_3'$, where I_3 and I_3' are prime ideals.

   (c) Show that I_5 and I_5' are both prime ideals of R and that $I_5 I_5'$ is the principal ideal (5).

   - By Dedekind-Kummer, the minimal polynomial x^2+14 of $\sqrt{-14}$ factors modulo 5 as $(x-1)(x+1)$ and therefore (3) splits as $(1+\sqrt{-14}, 5) \cdot (-1+\sqrt{-14}, 5) = I_5 I_5'$, where I_5 and I_5' are prime ideals.

   (d) Show that $I_3 I_5 = (1+\sqrt{-14})$ and $I_3' I_5' = (1-\sqrt{-14})$. Conclude that the two factorizations of 15 from part (a) yield the same factorization of the ideal (15) as a product of prime ideals.

   - We have $I_3 I_5 = (15,\ 3(1+\sqrt{-14}),\ 5(1+\sqrt{-14}),\ (1+\sqrt{-14})^2)$, and so $I_3 I_5$ contains $2 \cdot 3(1+\sqrt{-14}) - 5(1+\sqrt{-14}) = 1+\sqrt{-14}$, so $(1+\sqrt{-14}) \subseteq I_3 I_5$.
   - But clearly each generator of $I_3 I_5$ is a multiple of $1+\sqrt{-14}$, so $I_3 I_5 \subseteq (1+\sqrt{-14})$, and thus we must have equality. In the same way, we see that $I_3' I_5' = (1-\sqrt{-14})$.
   - Then we see $(15) = (3) \cdot (5) = I_3 I_3' \cdot I_5 I_5'$ and $(15) = (1+\sqrt{-14})(1-\sqrt{-14}) = I_3 I_5 \cdot I_3' I_5'$. Both factorizations are equivalent to $(15) = I_3 I_3' I_5 I_5'$, merely rearranged.

---

4. Let D be a squarefree integer not equal to 1. The discriminant of the quadratic integer ring $\mathcal{O}_{\sqrt{D}}$ is defined to be the discriminant of the minimal polynomial $m(x)$ of the generator of $\mathcal{O}_{\sqrt{D}}$. Recall that for a quadratic polynomial ax^2+bx+c, the discriminant is b^2-4ac.

   (a) Find the discriminant of $\mathcal{O}_{\sqrt{D}}$ in terms of D (note that there will be two cases, depending on whether $D \equiv 1 \pmod 4$ or not).

   - If $D \equiv 1 \pmod 4$, then the generator of $\mathcal{O}_{\sqrt{D}}$ is $\frac{1+\sqrt{D}}{2}$ with minimal polynomial $x^2 - x + \frac{1-D}{4}$, whose discriminant is $1 - 4 \cdot \frac{1-D}{4} = D$.
   - If $D \equiv 2$ or $3 \pmod 4$, then the generator of $\mathcal{O}_{\sqrt{D}}$ is $\sqrt{D}$ with minimal polynomial $x^2 - D$, whose discriminant is $4D$.

   (b) Show that the integer prime p is ramified in $\mathcal{O}_{\sqrt{D}}$ (i.e., its prime ideal factorization has a repeated factor) if and only if p divides the discriminant of $\mathcal{O}_{\sqrt{D}}$. [Hint: When does a quadratic have a repeated root?]

   - By the Dedekind-Kummer factorization theorem, we know that p is ramified if and only if the minimal polynomial $m(x)$ has a repeated root modulo p.
   - It is not hard to see that having a repeated root is equivalent to saying that the discriminant of $m(x)$ is zero: if the roots are r_1 and r_2 then one may check that the discriminant Δ of x^2+bx+c is $\Delta = (r_1-r_2)^2$, and so $r_1 = r_2$ if and only if $\Delta = 0$.
   - In particular, $m(x)$ has a repeated root modulo p if and only if $\Delta \equiv 0 \pmod p$, which is to say, if and only if p divides the discriminant.

   (c) Identify the ramified primes in $\mathcal{O}_{\sqrt{D}}$ for $D = -1$, -2, 5, 6, -10, and 21, and give their prime ideal factorizations.

   - By (a) and (b) the ramified primes are precisely those dividing the discriminant.
   - For $D = -1$ of discriminant -4, the only ramified prime is 2, and $(2) = (1+i)^2$.

- For $D = -2$ of discriminant -8, the only ramified prime is 2, and $(2) = (\sqrt{-2})^2$.
- For $D = 5$ of discriminant 5, the only ramified prime is 5, and $(5) = (\sqrt{5})^2$.
- For $D = 6$ of discriminant 24, the ramified primes are 2 and 3, and $(2) = (2, \sqrt{6})^2$ and $(3) = (3, \sqrt{6})^2$.
- For $D = -10$ of discriminant -40, the ramified primes are 2 and 5, and $(2) = (2, \sqrt{-10})^2$ and $(5) = (5, \sqrt{-10})^2$.
- For $D = 21$ of discriminant 21, the ramified primes are 3 and 7, and $(3) = (3, \frac{-3+\sqrt{21}}{2})^2$ and $(7) = (7, \frac{-7+\sqrt{21}}{2})$.

---

5. Recall that you proved on homework 6 that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain, hence also a PID and a UFD. Recall also that the Legendre symbol $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, so that 2 is a quadratic residue modulo an odd prime p precisely when $p \equiv 1$ or 7 (mod 8).

   (a) Show that every nonzero element in $\mathbb{Z}[\sqrt{2}]$ is associate to one having positive norm.
   - Note that $N(1+\sqrt{2}) = -1$, so if $N(x) < 0$, then $N((1+\sqrt{2})x) > 0$.

   (b) Prove that the prime elements in $\mathbb{Z}[\sqrt{2}]$, up to associates, are as follows:
   i. The element $2+\sqrt{2}$, of norm 2.
   ii. The primes p congruent to 3 or 5 modulo 8, of norm p^2.
   iii. The two conjugate factors $a+b\sqrt{2}$ and $a-b\sqrt{2}$ where $p = a^2 - 2b^2$ is a prime congruent to 1 or 7 modulo 8, of norm p.
   - Since $\mathbb{Z}[\sqrt{2}]$ is Euclidean, we only need to factor the minimal polynomial $q(x) = x^2 - 2$ modulo p.
   - For $p = 2$ we have $x^2 - 2 \equiv x^2 \bmod 2$, so we get the ideal factorization $(2) = (2, \sqrt{2})^2 = (\sqrt{2})^2$, so $2 = (\sqrt{2})^2$. We replace $\sqrt{2}$ with its associate $2+\sqrt{2}$ which has positive norm.
   - For $p \equiv 3$ or 5 mod 8, the polynomial $x^2 - 2$ is irreducible modulo p, so by Dedekind-Kummer the ideal (p) is prime and the element p is also prime of norm p^2.
   - With $p \equiv 1$ or 7 mod 8, the polynomial $x^2 - 2$ factors modulo p. If the factorization is $x^2 - 2 \equiv (x-r)(x+r)$ (mod p), we obtain the ideal factorization $(p) = (p, \sqrt{2}-r) \cdot (p, \sqrt{2}+r)$. Since $\mathbb{Z}[\sqrt{2}]$ is Euclidean, the ideal $(p, \sqrt{2}+r) = (a+b\sqrt{2})$ for some a, b that we can compute by applying the Euclidean algorithm to p and $\sqrt{2}+r$, and then $(p, r-\sqrt{2}) = (p, \sqrt{2}-r)$ is equal to $(a-b\sqrt{2})$.
   - This yields the ideal factorization $(p) = (a+b\sqrt{2})(a-b\sqrt{2})$ and so we get the element factorization $p = (a+b\sqrt{2})(a-b\sqrt{2})$ up to a unit factor, which per (a) we may assume is 1. This means $p = (a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2$, and we have $N(a+b\sqrt{2}) = a^2 - 2b^2 = p = N(a-b\sqrt{2})$, so both irreducible factors have norm p as claimed.

   (c) Find the irreducible factorizations of $10+\sqrt{2}$ and of $345+15\sqrt{2}$ in $\mathbb{Z}[\sqrt{2}]$.
   - We have $N(10+\sqrt{2}) = 2 \cdot 7^2$, so by (b) the possible irreducible factors up to associates are $\sqrt{2}$ and elements of norm 7, which by inspection we see are $3 \pm \sqrt{2}$.
   - Testing to see which elements divide $10+\sqrt{2}$ yields $10+\sqrt{2} = \boxed{(2-\sqrt{2})(3+\sqrt{2})^2}$.
   - Likewise, $N(345+15\sqrt{2}) = 3^2 5^2 17 \cdot 31$, so by (b) the possible factors up to associates are 3 (norm 3^2), 5 (norm 5^2), $5 \pm 2\sqrt{2}$ (norm 17), and $7 \pm 3\sqrt{2}$ (norm 31).
   - Testing to see which elements divide $345+15\sqrt{2}$ yields $345+15\sqrt{2} = \boxed{3 \cdot 5 \cdot (5-2\sqrt{2})(7+3\sqrt{2})}$.

   (d) Let n be a positive integer, and write $n = 2^k p_1^{n_1} \cdots p_k^{n_k} q_1^{m_1} \cdots q_d^{m_d}$, where $p_1, \cdots, p_k$ are distinct primes congruent to 1 or 7 modulo 8 and $q_1, \cdots, q_d$ are distinct primes congruent to 3 or 5 modulo 8. Prove that n can be written in the form $a^2 - 2b^2$ for some integers a and b if and only if all of the m_i are even.
   - The question of whether n can be written as $n = A^2 - 2B^2$ is equivalent to the question of whether n is the norm of an element $A + B\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Write $A + B\sqrt{2} = \rho_1 \rho_2 \cdots \rho_r$ as a product of irreducibles (unique up to units), and take norms to obtain $n = N(\rho_1) \cdot N(\rho_2) \cdot \cdots \cdot N(\rho_r)$.
   - By the classification in part (b), if ρ is irreducible in $\mathbb{Z}[\sqrt{2}]$, then $N(\rho)$ is either 2, a prime congruent to 1 or 7 modulo 8, or the square of a prime congruent to 3 or 5 modulo 8. Hence there exists such a choice of ρ_i with $n = \prod N(\rho_i)$ if and only if all the m_i are even.

---

6. The goal of this problem is to formulate the notions of gcd and lcm for ideals. Let R be an integral domain and A, B be ideals of R.

- We say an ideal K is a common divisor of A and B when $K|A$ and $K|B$, and K is a greatest common divisor when any other common divisor of A, B also divides K.
- We say an ideal E is a common multiple of A and B when $A|E$ and $B|E$, and E is a least common multiple when any other common multiple of A, B is also divisible by E.

(a) If R is a PID, show that (d) is a greatest common divisor of (a) and (b) if and only if d is a gcd of a and b. Deduce that the greatest common divisor of ideals I and J is the sum $I + J$.

- If R is a PID, note that (a) divides $(b) \iff$ there exists (k) with $(b) = (a)(k) = (ak) \iff$ there exists k with b and ak associates $\iff$ there exists k' with $b = ak' \iff a$ divides b.
- The equivalence of the ideal and element formulations of the greatest common divisor is then immediate from the above equivalence.
- The second statement follows by noting that $\gcd(a, b) = d$ we have $(d) = (a, b) = (a) + (b)$: by definition, the ideal (a, b) is principal, and any generator must be a common divisor that divides all other common divisors hence is a gcd.

(b) If R is a PID, show that (l) is a least common multiple of (a) and (b) if and only if l is an lcm of a and b. Deduce that the least common multiple of ideals I and J is the intersection $I \cap J$.

- The first statement is immediate from the equivalence of ideal and element divisibility, like above.
- The second statement follows by noting that for $\text{lcm}(a, b) = l$ we have $(l) = (a) \cap (b)$: by definition, $(a) \cap (b)$ is the set of all common multiples of a and b, so a generator of this principal ideal then has the property that all other common multiples are multiples of it, so it is an lcm.

The goal now is to show that the formulas $\gcd(I, J) = I + J$ and $\text{lcm}(I, J) = I \cap J$ also hold in quadratic integer rings. So let $R = \mathcal{O}_{\sqrt{D}}$ be a quadratic integer ring and I and J be ideals of R.

(c) Show that an ideal K is a common divisor of I and J if and only if K contains both I and J. Deduce that $\gcd(I, J) = I + J$.

- Since divisibility is the same as containment in R, we see $K|I$ and $K|J \iff K$ contains I and K contains $J \iff K$ contains $I + J \iff K$ divides $I + J$.
- This means any common divisor K divides $I + J$, so since $I + J$ is a common divisor (also by the above), this means $I + J$ is the gcd.

(d) Show that an ideal K is a common multiple of I and J if and only if K is contained in both I and J. Deduce that $\text{lcm}(I, J) = I \cap J$.

- In the same way, $I|K$ and $J|K \iff I$ and J both contain $K \iff I \cap J$ contains $K \iff I \cap J$ divides K.
- Thus, any common multiple is divisible by $I \cap J$, so $I \cap J$ is the least common multiple.

(e) Suppose I and J have prime ideal factorizations $I = P_1^{i_1} \cdots P_k^{i_k}$ and $J = P_1^{j_1} \cdots P_k^{j_k}$ for distinct prime ideals $P_1, \ldots P_k$. Give formulas for $I + J$ and $I \cap J$ in terms of the prime ideal factorizations.

- Following the analogy, we claim that $I+J = P_1^{\min(i_1,j_1)} \cdots P_k^{\min(i_k,j_k)}$ and $I \cap J = P_1^{\max(i_1,j_1)} \cdots P_k^{\max(i_k,j_k)}$. These formulas follow immediately from the same proofs used for the formulas for the gcd and lcm of elements in terms of prime factorizations, and the fact that $I + J$ is the gcd and $I \cap J$ is the lcm.
- Explicitly: the gcd has the largest possible power of each prime that divides both I and J, which is the min of the two exponents, and the lcm has the smallest power of each prime that is divisible by the corresponding power in I and J, which is the max of the two exponents.

---

7. [Challenge] The goal of this problem is to prove that $\mathbb{Z}[\sqrt{6}]$ is Euclidean. So suppose we want to divide $a+b\sqrt{6}$ by $c+d\sqrt{6}$ for $a, b, c, d \in \mathbb{Z}$, where $c+d\sqrt{6} \neq 0$.

   (a) Let $(a+b\sqrt{6})/(c+d\sqrt{6}) = x+y\sqrt{6}$ for $x, y \in \mathbb{Q}$. Show that if we can find integers m and n such that $\left|(x-m)^2 - 6(y-n)^2\right| < 1$, then taking quotient $q = m+n\sqrt{6}$ and remainder $r = (a+b\sqrt{6}) - q(c+d\sqrt{6})$ satisfies the Euclidean requirements.

   - We have $a+b\sqrt{6} = q(c+d\sqrt{6}) + r$ by definition, and also $\left|N(\frac{r}{c+d\sqrt{6}})\right| = \left|N(\frac{a+b\sqrt{6}-q(c+d\sqrt{6})}{c+d\sqrt{6}})\right| = \left|N(x+y\sqrt{6}-q)\right| = \left|(x-m)^2 - 6(y-n)^2\right| < 1$and thus $|N(r)| < \left|N(c+d\sqrt{6})\right|$, meaning that the size function $|N(r)|$ satisfies the Euclidean requirements.

   For integers m and n, define the (m,n)-star to be the region $\left|(x-m)^2 - 6(y-n)^2\right| < 1$ in the xy-plane.

   (b) Show that if the (m,n)-stars for integers m, n cover the entire xy-plane, then $\mathbb{Z}[\sqrt{6}]$ is Euclidean. Show that it suffices to show that they cover the single square $0 \leq x < 1$, $0 \leq y < 1$.

   - First suppose the (m,n)-stars cover the whole plane: then for any quotient $(a+b\sqrt{6})/(c+d\sqrt{6}) = x+y\sqrt{6}$, choose any (m,n)-star that contains (x,y): then $\left|(x-m)^2 - 6(y-n)^2\right| < 1$ by definition of the (m,n)-star, and then by (a) the Euclidean requirements are satisfied using $q = m+n\sqrt{6}$. This holds for all possible quotients $(a+b\sqrt{6})/(c+d\sqrt{6})$, so $\mathbb{Z}[\sqrt{6}]$ is Euclidean.
   - For the second part, since the (m,n)-star is obtained by translating the $(0,0)$-star, if the (m,n)-stars cover the unit square, then translating by all possible lattice vectors shows they cover the whole plane.

   (c) Show that the $(0,0)$-star covers the rectangle with $4/5 \leq x < 1$, $0 \leq y \leq 1/2$ and the rectangle with $0 \leq x < 1$, $0 \leq y \leq 2/5$, and that the $(-1,0)$-star covers the rectangle with $1/5 \leq x \leq 1/2$, $1/2 \leq y \leq 3/5$.

   - Observe that if $4/5 \leq x < 1$ and $0 \leq y \leq 1/2$ then $-0.86 \leq x^2 - 6y^2 < 1$ so the first rectangle is inside the (0,0)-star.
   - Likewise, if $0 \leq x \leq 1$ and $0 \leq y \leq 2/5$ then $-0.96 \leq x^2 - 6y^2 < 1$ so the second rectangle is inside the $(0,0)$-star.
   - Finally, if $1/5 \leq x \leq 1/2$, $1/2 \leq y \leq 3/5$ then $-0.72 \leq (x+1)^2 - 6y^2 \leq 0.75$ so the third rectangle is inside the $(-1,0)$-star.

   (d) Show that the (m,n)-stars for $(0,0)$, $(1,0)$, $(0,1)$, $(1,1)$, $(-1,0)$, $(2,0)$, $(-1,1)$, $(2,1)$ cover the square $0 \leq x \leq 1$, $0 \leq y \leq 1$. Deduce that $\mathbb{Z}[\sqrt{6}]$ is Euclidean. [Hint: Use the symmetry of the various star regions and (c). You may want to plot the regions in Mathematica using RegionPlot.]

   - By (c), the $(0,0)$-star covers the rectangle with $0 \leq x \leq 1$, $0 \leq y \leq 2/5$. Reflecting vertically, we see the $(0,1)$-star $0 \leq x \leq 1$, $3/5 \leq y \leq 1$.
   - Thus already we only have the strip $0 \leq x \leq 1$, $2/5 \leq y \leq 3/5$ remaining.
   - The $(0,0)$-star covers $4/5 \leq x < 1$, $0 \leq y \leq 1/2$ and so the $(0,1)$-star covers $4/5 \leq x < 1$, $1/2 \leq y \leq 1$, which is the portion with $0 \leq x \leq 1/5$.
   - Likewise, their horizontal reflections $(1,0)$ and $(1,1)$ cover the portion with $4/5 \leq x \leq 1$, $2/5 \leq y \leq 3/5$.
   - Finally, the $(-1,0)$-star covers the rectangle with $1/5 \leq x \leq 1/2$, $1/2 \leq y \leq 3/5$, its vertical reflection the $(-1,1)$-star covers $1/5 \leq x \leq 1/2$, $2/5 \leq y \leq 1/2$, and then their horizontal reflections the $(2,0)$ and $(2,1)$-stars cover $1/2 \leq x \leq 4/5$, $2/5 \leq y \leq 3/5$.
   - We see, all together, that we have covered the entire square, so by (b), this means $\mathbb{Z}[\sqrt{6}]$ is Euclidean.

   Remark: A similar method can be used to show $\mathbb{Z}[\sqrt{7}]$ is Euclidean.
