E. Dummit's Math 3527 ~ Number Theory 1, Fall 2026 ~ Homework 8, due Tue Nov 11th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly and submit via Gradescope, making sure to select page submissions for each problem. **Use of generative AI in any manner is not allowed on this or any other course assignments.**

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. For each element in each ring $\mathbb{Z}[\sqrt{D}]$, (i) determine whether it is a unit and if so find its multiplicative inverse, and (ii) if it is not a unit, determine whether it is irreducible or reducible, and (iii) if it is reducible, find a nontrivial factorization.

   (a) The elements $-i$, $3+2i$, $1+i$, and $1+5i$ in $\mathbb{Z}[i]$.

   (b) The elements $1+2\sqrt{5}$, $9+4\sqrt{5}$, $5+\sqrt{5}$, and $21+4\sqrt{5}$ in $\mathbb{Z}[\sqrt{5}]$.

---

2. Use the Euclidean algorithm in each Euclidean domain to compute a greatest common divisor of each pair of elements, and then to write it as a linear combination of the elements (make sure to give some details of the Euclidean algorithm in your response):

   (a) The polynomials x^6-1 and x^8-1 in $\mathbb{R}[x]$.

   (b) The elements $11+27i$ and $-9+7i$ in $\mathbb{Z}[i]$.

   (c) The polynomials x^3+x^2+1 and x^4+x in $\mathbb{R}[x]$.

   (d) The elements x^4+2x+1 and x^3+x in $\mathbb{F}_3[x]$.

   (e) The elements $9+43i$ and $22+10i$ in $\mathbb{Z}[i]$.

---

3. Let $R=\mathbb{F}_3[x]$ and $p=x^2+x$.

   (a) List the 9 residue classes in R/pR. (You may omit the bars in the residue class notation.)

   (b) Construct the addition and multiplication tables for R/pR.

   (c) Identify all of the units and zero divisors in R/pR.

   (d) Find the order of each unit in R/pR. Are there any primitive roots?

---

4. Let $R=\mathbb{F}_2[x]$ and $p=x^3+x+1$.

   (a) List the 8 residue classes in R/pR. (You may omit the bars in the residue class notation.)

   (b) Construct the addition and multiplication tables for R/pR.

   (c) Show that R/pR is a field by explicitly identifying the inverse of every nonzero element. [Hint: Use the multiplication table from (b).]

   (d) Find the order of each unit in R/pR. Are there any primitive roots?

Part II: Solve the following problems. Justify all answers with rigorous, clear explanations.

5. Let $r\in\mathbb{Z}[\sqrt{D}]$ be nonzero and not a unit. Prove that r has at least one factorization as a product of irreducibles: namely, $r=r_1\cdots r_k$ for some irreducible elements $r_1,\ldots,r_k$. [Hint: Induct on $|N(r)|$.]

---

6. The goal of this problem is to prove that the ring $R = \mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain under its norm function $N(a + b\sqrt{-2}) = a^2 + 2b^2$ using a similar argument to the one used to show $\mathbb{Z}[i]$ is Euclidean.

   (a) Suppose that $c + d\sqrt{-2}$ is not zero. Write $\dfrac{a + b\sqrt{-2}}{c + d\sqrt{-2}}$ in the form $x + y\sqrt{-2}$ for rational numbers x and y. [Hint: Rationalize the denominator.]

   (b) With notation from part (a), let s be the closest integer to x and t be the closest integer to y. Set $q = s + t\sqrt{-2}$ and $r = (a + b\sqrt{-2}) - (s + t\sqrt{-2})(c + d\sqrt{-2})$. Prove that $N(r) \leq \dfrac{3}{4}N(c + d\sqrt{-2})$.

   (c) Deduce that R is a Euclidean domain.

   (d) Use the Euclidean algorithm in R to find the greatest common divisor of $33 + 5\sqrt{-2}$ and $8 + 11\sqrt{-2}$ in R, and then write the gcd as a linear combination of these elements.

   Remark: By a similar argument, one may show that $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$ are also Euclidean domains.

---

7. Show the following things:

   (a) Show that the element $4 + 5i$ is irreducible and prime in $\mathbb{Z}[i]$.

   (b) Show that the element $x^2 + 4x + 5$ is irreducible and prime in $\mathbb{R}[x]$.

   (c) Show that the element $x^2 + 4x + 5$ is neither irreducible nor prime in $\mathbb{C}[x]$.

   (d) Show that the element $3 + 5i$ is neither irreducible nor prime in $\mathbb{Z}[i]$.

---

8. Let $R = \mathbb{Z}[\sqrt{-10}]$.

   (a) Show that there are no elements of norm 2 or 7 in R.

   (b) Show that the element $2 + \sqrt{-10}$ is irreducible in R.

   (c) Show that the element $2 + \sqrt{-10}$ is not prime in $\mathbb{Z}[\sqrt{-10}]$.

   (d) Explain briefly why R cannot be a Euclidean domain.
