---

1. For each pair of elements, use the Euclidean algorithm in the ring R to calculate a greatest common divisor $d = \gcd(a, b)$ and also to find $x, y \in R$ such that $d = ax + by$.
   (a) $a = x^4 + x$ and $b = x^3 + x$ in $\mathbb{F}_2[x]$.
   (b) $a = 11 + 24i$ and $b = 13 - i$ in $\mathbb{Z}[i]$.
   (c) $a = x^3 - x$ and $b = x^2 - 3x + 2$ in $\mathbb{R}[x]$.
   (d) $a = 9 - 5i$ and $b = 3 + 2i$ in $\mathbb{Z}[i]$.

---

2. For each given a, p, and R, determine whether $\overline{a}$ is a unit or a zero divisor in the ring of residue classes R/pR. If it is a unit find $\overline{a}^{-1}$, and if it is a zero divisor find a nonzero element $\overline{b}$ with $\overline{a} \cdot \overline{b} = \overline{0}$.
   (a) $a = 2 - i$, $p = 5 + 5i$, $R = \mathbb{Z}[i]$.
   (b) $a = x + 3$, $p = x^2 - 2$, $R = \mathbb{R}[x]$.
   (c) $a = 3 + 4i$, $p = 7 - 8i$, $R = \mathbb{Z}[i]$.
   (d) $a = x^2 + x$, $p = x^4 + 1$, $R = \mathbb{F}_2[x]$.
   (e) $a = x^2 + x$, $p = x^3 + 3x + 1$, $R = \mathbb{F}_5[x]$.

---

3. Determine / calculate / find the following:
   (a) All elements $a + b\sqrt{-2}$ with $N(a + b\sqrt{-2}) = 9$ in $\mathbb{Z}[\sqrt{-2}]$.
   (b) The quotient and remainder when $19 + 3i$ is divided by $4 + i$ in $\mathbb{Z}[i]$.
   (c) The quotient and remainder when x^5 is divided by $x^3 + x$ in $\mathbb{R}[x]$.
   (d) The solution to $(1 + i)x \equiv 3 \pmod{8 + i}$ in $\mathbb{Z}[i]$.
   (e) All z with $z \equiv 2 - i \pmod{3 + i}$ and $z \equiv 3 \pmod{4 + 5i}$ in $\mathbb{Z}[i]$.
   (f) All p with $p \equiv x \pmod{x^2}$ and $p \equiv 10 \pmod{x - 2}$ in $\mathbb{R}[x]$.
   (g) The number of residue classes in $\mathbb{F}_7[x]$ modulo $x^3 + 5x + 2$.
   (h) All of the units and zero divisors in $\mathbb{F}_3[x]$ modulo $x^2 + 2x$.
   (i) All of the units and zero divisors in $\mathbb{F}_5[x]$ modulo x^2.
   (j) The irreducible factorizations of $x^2 - x + 4$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, and $\mathbb{F}_5[x]$.
   (k) The number of monic irreducible polynomials in $\mathbb{F}_2[x]$ of degree 7.
   (l) The number of monic irreducible polynomials in $\mathbb{F}_7[x]$ of degree 4.
   (m) The number of monic irreducible polynomials in $\mathbb{F}_2[x]$ of degree 10.
   (n) Determine whether there exists a primitive root modulo (each of) 34, 35, 36, and 37.
   (o) Find a primitive root modulo 3^{2023} and the total number of primitive roots modulo 3^{2023}.
   (p) Find a primitive root modulo $2 \cdot 3^{2023}$ and the total number of primitive roots modulo $2 \cdot 3^{2023}$.
   (q) Find the number of residue classes in $\mathbb{Z}[i]$ modulo $7 - 5i$.
   (r) Find a fundamental region and list of residue class representatives for $\mathbb{Z}[i]$ modulo $2 - i$.
   (s) Find the prime factorization of $5 + 5i$ in $\mathbb{Z}[i]$.
   (t) Find the prime factorization of $11 + 12i$ in $\mathbb{Z}[i]$.
   (u) Find the prime factorization of 999 in $\mathbb{Z}[i]$.
   (v) Determine which of 104, 224, 420, and 666 can be written as the sum of two squares.
   (w) Find two different ways of writing the integer $260 = 2^2 \cdot 5 \cdot 13$ as a sum of two squares.
   (x) Find two different ways of writing the integer $450 = 2 \cdot 3^2 \cdot 5^2$ as a sum of two squares.
   (y) Find four Pythagorean right triangles with a hypotenuse of length 65.
   (z) Find two Pythagorean right triangles with a leg of length 49.

---

4. Let $R = \mathbb{F}_2[x]$ and $p = x^3 + x^2 + x + 1$.

   (a) List the 8 residue classes in R/pR.

   (b) Express $\overline{x^2} + \overline{x^2+1}$, $\overline{x^2} \cdot \overline{x^2+1}$, and $\overline{x^2+1}^2$ as $\overline{ax^2+bx+c}$ for some $a, b, c \in \mathbb{F}_2$.

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

   (d) Verify Euler's theorem for the unit $\overline{x^2+x+1}$ in R/pR.

   (e) Solve the congruence $x^2 \cdot q(x) \equiv x + 1 \pmod{x^3 + x^2 + x + 1}$ in $\mathbb{F}_2[x]$.

---

5. Calculate the following:

   (a) List the quadratic residues modulo 19.

   (b) Find the number of quadratic residues modulo 43.

   (c) Determine whether 7, 11, and 14 are quadratic residues modulo 43.

   (d) Determine whether 13 and 26 are quadratic residues modulo the prime 2027.

   (e) Determine whether 28 and 15 are quadratic residues modulo the prime 71.

   (f) Calculate the Legendre symbols $\left(\frac{103}{307}\right)$ and $\left(\frac{141}{307}\right)$.

---

6. Prove the following:

   (a) Show that the element $7 + 4\sqrt{3}$ is a unit in $\mathbb{Z}[\sqrt{3}]$ and find its multiplicative inverse.

   (b) Show that the element $(1+\sqrt{5})^{2023}$ is not a unit, but $(2+\sqrt{5})^{2023}$ is a unit in $\mathbb{Z}[\sqrt{5}]$.

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

   (d) Show that the element $2 + \sqrt{-7}$ is irreducible in $\mathbb{Z}[\sqrt{-7}]$.

   (e) Show that the element $1 + \sqrt{-7}$ is irreducible in $\mathbb{Z}[\sqrt{-7}]$. [Hint: Show that there are no elements of norm 2 or 4.]

   (f) Show that the element $1 + \sqrt{-7}$ is not prime in $\mathbb{Z}[\sqrt{-7}]$.

   (g) Show that $x^2 + x + 1$ is irreducible and prime in $\mathbb{F}_2[x]$.

   (h) Verify Euler's Theorem for the residue class of $x^2 + 1$ in $\mathbb{F}_2[x]$ modulo x^3.

   (i) Verify Fermat's Little Theorem for the residue class of i in $\mathbb{Z}[i]$ modulo $3 + 2i$.

   (j) Show that $\mathbb{F}_5[x]$ modulo $x^3 + x + 1$ is a field.

   (k) Show that $\mathbb{F}_5[x]$ modulo $x^4 + x + 1$ is not a field.

   (l) Show that $\mathbb{R}[x]$ modulo $x^2 + 2x + 8$ is a field.

   (m) Construct, with proof, a field with exactly 125 elements.

   (n) Verify Euler's theorem for the residue class of $1 + i$ modulo $4 + i$ in $\mathbb{Z}[i]$.

   (o) Prove that there exists a solution to $x^2 \equiv 11 \pmod{97}$. Note 97 is prime.
