E. Dummit's Math 3527 ~ Number Theory 1, Spring 2020 ~ Midterm 2 Review Problems

---

1. Define / describe / state the following things:

   - Euclidean domains
   - The Euclidean algorithms in $\mathbb{Z}[i]$ and $F[x]$
   - Irreducible and prime elements
   - Unique factorization
   - The structure of R/rR
   - Units and zero divisors in R/rR
   - Multiplicative inverses of units in R/rR
   - The Chinese remainder theorem in R/rR
   - The order of a unit in a ring
   - Fermat's little theorem in R/rR
   - Euler's theorem in R/rR
   - Roots of polynomials
   - Factorization and irreducibility in $F[x]$
   - Finite fields
   - Primitive roots in finite fields
   - Primitive roots modulo m
   - Residue classes in $\mathbb{Z}[i]$ modulo p
   - Factorization in $\mathbb{Z}[i]$
   - Sums of two squares
   - Pythagorean triples

---

2. 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 $\mathbb{Z}[i]$.

---

3. 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) $a = x^2 + x$, $p = x^3 + 3x + 1$, $R = \mathbb{F}_5[x]$.

---

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) Calculate $\overline{x^2} + \overline{x^2 + 1}$, $\overline{x^2} \cdot \overline{x^2 + 1}$, and $\overline{x^2 + 1}^2$ in R/pR and express the results 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) Show that $\overline{x}$ is a primitive root in R/pR.

---

5. (The A-Zs of Chapter 4) Determine / calculate / find the following:

   (a) The quotient and remainder when $19 + 3i$ is divided by $4 + i$ in $\mathbb{Z}[i]$.
   (b) The quotient and remainder when x^5 is divided by $x^3 + x$ in $\mathbb{R}[x]$.
   (c) The remainder when $x^{666} + x^{420}$ is divided by $x - 2$ in $\mathbb{Q}[x]$.
   (d) The solution to $(1 + i)n \equiv 3 \pmod{8 + i}$ in $\mathbb{Z}[i]$.
   (e) The solution to $(x^2 + 1)p \equiv x \pmod{x^3 + x + 1}$ in $\mathbb{F}_2[x]$.
   (f) All z with $z \equiv 2 - i \pmod{3 + i}$ and $z \equiv 3 \pmod{4 + 5i}$ in $\mathbb{Z}[i]$.
   (g) All p with $p \equiv x \pmod{x^2}$ and $p \equiv 10 \pmod{x - 2}$ in $\mathbb{R}[x]$.
   (h) The irreducible factorizations of $x^2 - x + 4$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, and $\mathbb{F}_5[x]$.
   (i) The number of residue classes in $\mathbb{F}_7[x]$ modulo $x^3 + 5x + 2$.
   (j) The number of residue classes in $\mathbb{Z}[i]$ modulo $7 - 5i$.
   (k) All of the units and zero divisors in $\mathbb{F}_3[x]$ modulo $x^2 + 2x$.
   (l) All of the units and zero divisors in $\mathbb{F}_5[x]$ modulo x^2.
   (m) The number of monic irreducible polynomials in $\mathbb{F}_2[x]$ of degree 7.
   (n) The number of monic irreducible polynomials in $\mathbb{F}_7[x]$ of degree 4.
   (o) The number of monic irreducible polynomials in $\mathbb{F}_2[x]$ of degree 10.
   (p) Whether or not there exists a primitive root modulo (each of) 34, 35, 36, and 37.
   (q) A primitive root modulo 3^{2020} and the total number of primitive roots modulo 3^{2020}.
   (r) A primitive root modulo $2 \cdot 3^{2020}$ and the total number of primitive roots modulo $2 \cdot 3^{2020}$.
   (s) A list of residue class representatives for $\mathbb{Z}[i]$ modulo $2 - i$.
   (t) The prime factorization of $5 + 5i$ in $\mathbb{Z}[i]$.
   (u) The prime factorization of $11 + 12i$ in $\mathbb{Z}[i]$.
   (v) The prime factorization of 999 in $\mathbb{Z}[i]$.
   (w) Which of the integers 104, 224, 420, and 666 can be written as the sum of two squares.
   (x) Two different ways of writing the integer $450 = 2 \cdot 3^2 \cdot 5^2$ as a sum of two squares.
   (y) Four Pythagorean right triangles with a hypotenuse of length 65.
   (z) Two Pythagorean right triangles with a leg of length 49.

---

6. Prove the following:

   (a) Show that $\mathbb{F}_5[x]$ modulo $x^3 + x + 1$ is a field.
   (b) Show that $\mathbb{F}_5[x]$ modulo $x^4 + x + 1$ is not a field.
   (c) Show that $\mathbb{R}[x]$ modulo $x^2 + 2x + 8$ is a field.
   (d) Show that $x^3 + x + 1$ is irreducible and prime in $\mathbb{F}_7[x]$.
   (e) Construct, with proof, a field with exactly 125 elements.
   (f) Verify Euler's Theorem for the residue class of $x^2 + 1$ in $\mathbb{F}_2[x]$ modulo x^3.
   (g) Verify Fermat's Little Theorem for the residue class of i in $\mathbb{Z}[i]$ modulo $2 + i$.
   (h) Show that the element $4 + 5i$ is irreducible and prime in $\mathbb{Z}[i]$.
   (i) 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.]
   (j) Show that the element $1 + \sqrt{-7}$ is not prime in $\mathbb{Z}[\sqrt{-7}]$. [Hint: It divides $8 = 2 \cdot 4$.]
