E. Dummit's Math 3527 ∼ Number Theory 1, Spring 2024 ∼ Homework 3, due Tue Jan 30th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Submit scans of your responses via Canvas.

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

1. Calculate the following:

   (a) The values of $\overline{5}+\overline{12}$, $\overline{5}-\overline{12}$, and $\overline{5}\cdot\overline{12}$ in $\mathbb{Z}/14\mathbb{Z}$. Write your answers as $\overline{a}$ where $0 \le a \le 13$.

   (b) The addition and multiplication tables modulo 7. (For ease of writing, you may omit the bars in the residue class notation.)

   (c) All of the unit residue classes modulo 7 and their multiplicative inverses.

   (d) The multiplication table modulo 8. (Again, you may omit the bars.)

   (e) All of the unit residue classes modulo 8 and their multiplicative inverses.

---

2. For each integer a and modulus m, determine whether the residue class $\overline{a}$ is a unit modulo m, or a zero divisor modulo m. If $\overline{a}$ is a unit then find its multiplicative inverse, while if $\overline{a}$ is a zero divisor then find a nonzero residue class $\overline{x}$ such that $\overline{x}\cdot\overline{a}=\overline{0}$.

   (a) $a = 14$, $m = 49$.

   (b) $a = 16$, $m = 49$.

   (c) $a = 125$, $m = 2024$.

   (d) $a = 1081$, $m = 2024$.

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

3. The goal of this problem is to demonstrate that the uniqueness of integer prime factorizations is not as obvious as it may seem. Let S be a nonempty set of positive integers, and define an S-prime to be an element $p \in S$ such that there do not exist $a, b \in S$ such that $ab = p$ and $1 < a, b < p$. (If S is the set of all positive integers, then this definition reduces to the usual one for prime numbers.) Let $E = \{2, 4, 6, 8, 10, \dots\}$ be the set of even positive integers and let $R = \{1, 5, 9, 13, 17, \dots\}$ be the set of positive integers congruent to 1 modulo 4.

   (a) Which of 2, 4, 6, 8, 10, 12, 14, and 16 are E-primes?

   (b) Show that $2n \in E$ is an E-prime if and only if n is odd. [Hint: Show the contrapositive.]

   (c) Show that 60 has two different factorizations as a product of E-primes. Deduce that E does not have unique E-prime factorization.

   (d) Explain why any odd prime congruent to 1 modulo 4 (e.g., 5, 13, 17) is an R-prime.

   (e) Which of the composite numbers 9, 21, 25, 33, 45, 49 are R-primes?

   (f) Find an integer in R that has two different R-prime factorizations. Deduce that R does not have unique R-prime factorization. [Hint: Multiply some of the composite R-primes in (e) together.]

---

4. Let R be a commutative ring with 1 and let r be an element of R.

   (a) Show that if r is a unit then $-r$ and r^{-1} are also units.

   (b) Show that if r and s are units, then rs is also a unit.

---

5. The goal of this problem is to establish the binomial theorem; for no additional charge, we will do this in an arbitrary commutative ring with 1. Define the binomial coefficient $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ for integers $0 \leq k \leq n$, and note that $\binom{n}{0} = \binom{n}{n} = 1$ for every n. (Recall the definition of $n!$ from homework 1.)

   (a) Show that $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ for every $0 \leq k \leq n$. Conclude in particular that $\binom{n}{k}$ is always an integer.

   (b) Suppose that R is a commutative ring with 1. If x and y are arbitrary elements of R, prove that $(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + y^n$ for any positive integer n. [Hint: Use induction on n. You may prefer to use summation notation $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k$ instead.]

---

6. Suppose a, b, c, m are integers and $m > 0$. Prove the following basic properties of modular congruences (these properties are mentioned but not proven in the notes; you are expected to give the details of the proofs):

   (a) For any a, $a \equiv a \pmod{m}$.

   (b) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

   (c) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

   (d) If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$ for any $c > 0$.

---

7. The goal of this problem is to discuss some applications of modular arithmetic to solving equations in integers (these are generally called Diophantine equations).

   (a) If n is a positive integer, show that n^2 is congruent to 0 or 1 modulo 4. [Hint: Square the four possible residue classes modulo 4.]

   (b) Show that there do not exist integers a and b such that $a^2 + b^2 = 2023$. [Hint: Work modulo 4.]

   (c) Strengthen (a) by showing that if n is a positive integer, then n^2 is congruent to 0, 1, or 4 modulo 8.

   (d) Show that there do not exist integers a, b, and c such that $a^2 + b^2 + c^2 = 2023$.
