E. Dummit's Math 3527 ∼ Number Theory 1, Spring 2026 ∼ Homework 3, due Fri Jan 30th.

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. 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) For a positive integer n, when is $2n \in E$ an E-prime? Briefly justify your answer.

   (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 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.]

---

2. 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.

---

3. For each element in each ring $\mathbb{Z}[\sqrt{D}]$, determine whether it is a unit and if so find its multiplicative inverse.

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

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

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

4. Prove that the following numbers are irrational:

   (a) $\sqrt[3]{2}$.

   (b) $\log_3 7$.

---

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 $0 \le k \le n$, 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 $0 \le k \le n$. 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) If $d|m$, then $a \equiv b \pmod{m}$ implies $a \equiv b \pmod{d}$.

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

   (c) If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for all positive integers n.

---

7. The goal of this problem is to illustrate some applications of modular arithmetic to solving equations in integers (such equations are 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 $a^2 + b^2 + c^2 = 2023$.
