E. Dummit's Math 3527 ~ Number Theory I, Spring 2020 ~ Homework 3, due Wed Jan 29th.

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. Either staple the pages of your assignment together and write your name on the first page, or paperclip the pages and write your name on all pages.

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

1. 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 $\overline{a} \cdot \overline{x} = \overline{0}$.

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

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

   (c) $a = 1776$, $m = 2020$.

   (d) $a = 1789$, $m = 2020$.

---

2. Find the general solution n to each of the given congruences:

   (a) $4n + 3 \equiv 2 \pmod{19}$.

   (b) $3n \equiv 7 \pmod{21}$.

   (c) $3n \equiv 9 \pmod{21}$.

   (d) $1789n \equiv 1492 \pmod{2020}$.

   (e) $36n \equiv 128 \pmod{2020}$.

---

3. Using the Chinese Remainder Theorem or otherwise, find the general solution n to each system of simultaneous congruences:

   (a) $n \equiv 4 \pmod{11}$ and $n \equiv 1 \pmod{15}$.

   (b) $n \equiv 7 \pmod{999}$ and $n \equiv 37 \pmod{1001}$.

   (c) $n \equiv 7 \pmod{84}$ and $n \equiv 21 \pmod{35}$.

   (d) $n \equiv 7 \pmod{85}$ and $n \equiv 21 \pmod{34}$.

   (e) $n \equiv 2 \pmod{8}$, $n \equiv 1 \pmod{5}$, and $n \equiv 3 \pmod{9}$.

   (f) $n \equiv 17 \pmod{44}$, $n \equiv 39 \pmod{90}$, and $n \equiv 9 \pmod{80}$.

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

4. Let m be a positive integer and a, b, c be any integers. Prove the following basic properties of residue class arithmetic modulo m (these properties are mentioned but not proven in the notes; you are expected to give the details of the proofs):

   (a) Prove that $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ for any $\overline{a}$ and $\overline{b}$.

   (b) Prove that the operation $\cdot$ is associative modulo m: namely, that $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$ for any $\overline{a}$, $\overline{b}$, and $\overline{c}$.

   (c) Prove that the residue class $\overline{1}$ is a multiplicative identity modulo m, namely, that $\overline{1} \cdot \overline{a} = \overline{a}$ for any $\overline{a}$.

---

5. The goal of this problem is to discuss some applications of modular arithmetic to solving equations in integers. (We will return several times to these ideas later in the course.)

   (a) If n is a positive integer, prove that n^2 is congruent to 0 or 1 modulo 4.

   (b) Show that the sum of two squares must be congruent to 0, 1, or 2 modulo 4.

   (c) Deduce that there do not exist integers a and b such that $a^2 + b^2 = 2019$.

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

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

---

6. Suppose n is an integer.

   (a) Show that $n^5 - n \equiv 0 \pmod{30}$.

   (b) Show that $n^8 - n^2 \equiv 0 \pmod{84}$.

---

7. 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) Let R be a commutative ring with 1. If x and y are arbitrary elements of R, prove that $(x+y)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$ for any positive integer n. [Hint: Use induction on n.]
