E. Dummit's Math 1365 ~ Intro to Proof, Fall 2022 ~ Homework 6, due Tue Oct 25th.

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. Identify all pages containing each problem when submitting the assignment.

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

1. Find the following:

   (a) Find the values of $\overline{6} + \overline{13}$, $\overline{6} - \overline{13}$, and $\overline{6} \cdot \overline{13}$ in $\mathbb{Z}/11\mathbb{Z}$. Write your answers as $\overline{a}$ where $0 \leq a \leq 10$.

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

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

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

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

   (f) Find the multiplicative inverse of $\overline{7}$ modulo 10 or explain why it does not exist.

   (g) Find the multiplicative inverse of $\overline{14}$ modulo 49 or explain why it does not exist.

   (h) Find the multiplicative inverse of $\overline{16}$ modulo 49 or explain why it does not exist.

---

2. Each of the following proofs has an error: identify it and briefly explain why it causes the proof to be incorrect:

   (a) Proposition: All horses are the same color.
   Proof: Induction on n, the number of horses. The base case $n = 1$ is trivial because any 1 horse is the same color as itself. For the inductive step, suppose that any $n+1$ horses are the same color. Ignoring the last horse yields means that we need to show that n horses are the same color, which is true by the induction hypothesis. Therefore the result holds by induction.

   (b) Proposition: For every positive integer n, $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1)$.
   Proof: Induction on n. The base case $n = 1$ follows because $1 = \frac{1}{2}(1)(2)$. For the inductive step, suppose that $1 + 2 + 3 + \cdots + n + (n+1) = \frac{1}{2}(n+1)(n+2)$. Subtracting $n+1$ from both sides yields $1 + 2 + 3 + \cdots + n = \frac{1}{2}(n+1)(n+2) - (n+1) = \frac{1}{2}n(n+1)$ which is true by the induction hypothesis. Therefore the result holds by induction.

   (c) Proposition: If n is an integer such that $2n \equiv 6 \pmod{10}$ then $n \equiv 3 \pmod{10}$.
   Proof: Suppose that $2n \equiv 6 \pmod{10}$. Multiplying both sides by $2^{-1} \pmod{10}$ yields $2^{-1}(2n) \equiv 2^{-1}6 \pmod{10}$ which simplifies to $n \equiv 3 \pmod{10}$, as claimed.

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

3. Suppose a, b, c, m are integers and $m > 0$. Prove the following properties of modular arithmetic:

   (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 $c > 0$.

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

   (f) 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 $\overline{c}$.

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

---

4. The goal of this problem is to discuss modular exponentiation, which is frequently used in cryptography. If n is a positive integer, we define $\overline{a}^n$ (mod m) to be the n-term product $\underbrace{\overline{a}\cdot\overline{a}\cdot\cdots\cdot\overline{a}}_{n\text{ terms}}$ (mod m). By an easy induction, one has $\overline{a}^n = \overline{a^n}$ (i.e., the nth power of the residue class $\overline{a}$ is the residue class of the nth power a^n).

   (a) Find the residue classes $\overline{2}^2$, $\overline{2}^3$, $\overline{2}^4$, $\overline{2}^5$, $\overline{2}^6$, $\overline{3}^2$, $\overline{3}^3$, $\overline{3}^4$, $\overline{3}^5$, and $\overline{3}^6$ (mod 10). (Write your answers as residue classes $\overline{r}$ where $0 \le r \le 9$.)

   (b) Show that if $a \equiv b$ (mod m), then for any positive integer n, it is true that $a^n \equiv b^n$ (mod m).

   (c) It is natural to think that if $n_1 \equiv n_2$ (mod m), then $a^{n_1} \equiv a^{n_2}$ (mod m); i.e., that exponents "can also be reduced mod m". Show that this is incorrect by verifying that 2^2 is not congruent to 2^7 modulo 5.

   (d) Show in fact that if $a \not\equiv 0$ modulo 5, then $a^4 \equiv 1$ (mod 5). Deduce that $a^{n_1} \equiv a^{n_2}$ (mod 5) whenever $n_1 \equiv n_2$ (mod 4), so that the exponents actually behave "modulo 4". [Hint: For the first part, simply test the 4 possible cases. For the second part, use (b) to see that $a^{4k} \equiv 1$ (mod 5) for any k.]

   Now suppose we want to find the remainder when we divide 2^{516} by 61. Here is an efficient approach: compute the values $2^1 \equiv 2$, $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv 16^2 \equiv 12$, $2^{16} \equiv 12^2 \equiv 22$, $2^{32} \equiv 22^2 \equiv -4$, $2^{64} \equiv 16$, $2^{128} \equiv 12$, $2^{256} \equiv 22$, $2^{512} \equiv 57$ modulo 61 by squaring each previous term and reducing. Then simply evaluate $2^{516} = 2^{512} \cdot 2^4 \equiv 57 \cdot 16 \equiv 58$ (modulo 61), so the remainder is 58.

   (e) Use the method described above to find the remainder when 3^{261} is divided by 43.

   - Remark: Efficient calculations with modular exponentiation are a fundamental part of the RSA cryptosystem, which is still in wide use today.

---

5. Let p be a prime. The goal of this problem is to prove that $a^p \equiv a$ (mod p) for every integer a, which is a result known as Fermat's Little Theorem.

   (a) Show that the binomial coefficient $\binom{p}{k}$ is divisible by p for each integer k with $0 < k < p$.

   (b) Prove that $a^p \equiv a$ (mod p) for every positive integer a.

   (c) Show in fact that $a^p \equiv a$ (mod p) for all integers a. [Hint: The value of $a^p - a$ mod p only depends on what residue class a lies in mod p.]

---

6. The goal of this problem is to discuss some applications of modular arithmetic to solving equations in integers.

   (a) If n is a positive integer, prove that n^2 is congruent to 0 or 1 modulo 4. [Hint: Consider n 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 $a^2 + b^2 = 2023$.

   (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 $a^2 + b^2 + c^2 = 2023$.
