E. Dummit's Math 1365 ~ Intensive Mathematical Reasoning, Fall 2023 ~ Homework 6, due Tue Oct 24th.

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 $0 \le a \le 10$.
   (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 invertible 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 invertible 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.

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

2. Suppose a, b, c, d, m are integers and $m > 0$. Prove the following properties of modular arithmetic:
   (a) If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$ for any $c > 0$.
   (b) If $d|m$ and $d > 0$, then $a \equiv b \pmod{m}$ implies $a \equiv b \pmod{d}$.
   (c) Prove that the operation $+$ is commutative modulo m: namely, that $\overline{a}+\overline{b} = \overline{b}+\overline{a}$ for any $\overline{a}$ and $\overline{b}$.
   (d) 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 $\overline{c}$.
   (e) Prove that the residue class $\overline{1}$ is a multiplicative identity modulo m, namely, that $\overline{1}\cdot\overline{a} = \overline{a}$ for any $\overline{a}$.

---

3. The goal of this problem is to discuss modular exponentiation, which is frequently used in cryptography. If n is a positive integer, we define $\overline{a}^n \pmod{m}$ to be the n-term product $\underbrace{\overline{a}\cdot\overline{a}\cdot\cdots\cdot\overline{a}}_{n \text{ terms}} \pmod{m}$. 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 $\overline{3}^6 \pmod{10}$. (Write your answers as residue classes $\overline{r}$ where $0 \le r \le 9$.)
   (b) Show that if $a \equiv b \pmod{m}$, then for any positive integer n, it is true that $a^n \equiv b^n \pmod{m}$.
   (c) It is natural to think that if $n_1 \equiv n_2 \pmod{m}$, then $a^{n_1} \equiv a^{n_2} \pmod{m}$; 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 $a^4 \equiv 1 \pmod{5}$. Deduce that $a^{n_1} \equiv a^{n_2} \pmod{5}$ whenever $n_1 \equiv n_2 \pmod{4}$, so that the exponents actually behave "modulo 4". [Hint: For the first part, test the 4 possible residue classes for a. For the second part, use (b) to see that $a^{4k} \equiv 1 \pmod{5}$ 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.

---

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

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

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

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

---

5. The goal of this problem is to establish a simple way to show large integers are composite without finding an explicit factorization.

   (a) Show that if there exists an integer a such that $a^m \not\equiv a \pmod{m}$, then m is composite. [Hint: The result of problem 4 states that if p is prime, then $a^p \equiv a \pmod{p}$ for all integers a.]

   (b) Given that $2^{23381} \equiv 9352 \pmod{23381}$, what can be concluded about whether 23381 is prime or composite?

   (c) Given that $2^{23377} \equiv 2 \pmod{23377}$, what can be concluded about whether 23377 is prime or composite?

   - Remark: The powers in parts (b) and (c) can be calculated quickly using the method discussed in problem 3(e).

---

6. The goal of this problem is to prove the rational root test from algebra, and derive some of its consequences.

   (a) Suppose $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a polynomial with integer coefficients, meaning that $a_n, a_{n-1}, \ldots, a_0$ are integers. Prove the rational root test: if r/s is a rational root in lowest terms, meaning that r, s are relatively prime and $p(r/s) = 0$, then $r|a_0$ and $s|a_n$. [Hint: Clear denominators and rearrange to show that $s|a_n r^n$ and $r|a_0 s^n$.]

   (b) Suppose x is such that $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ for some integers $a_{n-1}, \ldots, a_0$. Show that if x is not an integer, then x is irrational.

   (c) If n is an integer, prove that $\sqrt{n}$ is irrational unless n is a perfect square.

   (d) Prove that $\sqrt{2}+\sqrt{3}$ is irrational. [Hint: Show $\sqrt{2}+\sqrt{3}$ is not an integer, then consider $[(\sqrt{2}+\sqrt{3})^2-5]^2$.]
