E. Dummit's Math 1365 ~ Intro to Proof, Fall 2019 ~ Homework 5, due Oct 16th.

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.

---

1. Answer the following (work is not required):
   (a) Find the prime factorization of 1001.
   (b) Find the prime factorization of 2019^{10}.
   (c) Find the gcd and lcm of 288 and 600.
   (d) Find the gcd and lcm of $2^8 3^{11} 5^7 7^8 11^2$ and $2^4 3^8 5^7 7^7 11^{11}$.
   (e) 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 $0 \leq a \leq 10$.
   (f) Find the multiplicative inverse of $\overline{7}$ modulo 10.
   (g) Find all integers n with the property that $\overline{n} + \overline{7} = \overline{1}$ modulo 23. [Hint: The answer is *not* "$n = 17$".]
   (h) Does $\overline{14}$ have a multiplicative inverse modulo 49? If so, find it, and if not, explain why not.
   (i) Does $\overline{16}$ have a multiplicative inverse modulo 49? If so, find it, and if not, explain why not.

---

2. Let $n > 1$ be a positive integer.
   (a) Show that if no prime $\leq \sqrt{n}$ divides n, then n is prime. [Hint: Try proving the contrapositive instead.]
   (b) Use part (a) to explain why the representation $131 = 2 \cdot 5 \cdot 11 + 3 \cdot 7$ immediately shows that 131 is prime.

---

3. Prove that $\log_2 3$ is irrational. [Hint: Suppose otherwise, so that $\log_2 3 = a/b$. Convert this to statement about positive integers and find a contradiction.]

---

4. Draw the addition and multiplication tables modulo 7. (For ease of writing, you may omit the bars in the residue class notation.) For each residue class, identify whether it has a multiplicative inverse, and if so, calculate it.

---

5. 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) If $\overline{a}$ represents the equivalence class of a modulo m, prove 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 $\overline{a}$.

---

6. 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 $0 \leq r \leq 9$.)

   (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, simply test the 4 possible cases. 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.

---

7. 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 $a^2 + b^2 = 2019$.

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