E. Dummit's Math 3527 $\sim$ Number Theory I, Spring 2023 $\sim$ Homework 4, due Tue Feb 7th.

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. Submit scans of your responses via Canvas.

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

1. 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) $n \equiv 1 \pmod{44}$, $n \equiv 81 \pmod{90}$, and $n \equiv 61 \pmod{80}$.

---

2. Calculate each of the following things:

   (a) The orders of the elements 2, 3, 4 modulo 7.

   (b) The order of 2 modulo 31.

   (c) The order of 3 modulo 40.

   (d) The order of -11 modulo 17.

   (e) The orders of 2, 4, and 8 modulo 25. [Hint: They divide 20.]

   (f) The smallest positive integer s such that $3^s \equiv 1 \pmod{11}$.

   (g) The remainder when 2^{4000} is divided by 41.

   (h) The remainder when 3^{65} is divided by 17.

---

3. Consider the problem of finding the remainder when 2^{4096} is divided by $209 = 11 \cdot 19$. (Note that $4096 = 2^{12}$.)

   (a) Solve the problem using successive squaring only.

   (b) Solve the problem by computing 2^{4096} modulo 11 and modulo 19 separately, then using the Chinese Remainder Theorem to determine the result modulo 209.

   (c) Suppose you are asked to compute $55106124962340^{21249128358912345234645734632545799924810134}$ modulo pq, where $p = 3247598234709856730988 1$ and $q = 43498562345124558203957$. (These values p and q are both prime.) Without actually doing the calculation, which of the methods (a)-(b) would be most efficient? Explain.

   (d) Suppose you are asked to compute $435982734598903^{3383813130965025124879127509}$ modulo N, where $N = 774474179081739059134688868419410928055229466015696684839317695166499006603861910228042427007958 3$, and you are also told that N is composite but are *not* given the prime factors. Without actually doing the calculation, which of the methods (a)-(b) would be most efficient? Explain.

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

4. Show that 5 has order 16 modulo 102 and order 36 modulo 111.

---

5. Suppose n is a positive integer.

   (a) Show that $n^5 - n \equiv 0 \pmod{30}$. [Hint: By the Chinese Remainder Theorem, this is equivalent to showing $n^5 - n$ is divisible by 2, 3, and 5.]

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

---

6. The goal of this problem is to discuss elements of order 2 and order 4 modulo m.

   (a) If $p > 2$ is prime, show that there is a unique element of order 2 in $\mathbb{Z}/p\mathbb{Z}$. [Hint: If k has order 2, then p divides $k^2 - 1 = (k-1)(k+1)$.]

   (b) Show using an example that if m is composite, then there may be more than one element of order exactly 2 in $\mathbb{Z}/m\mathbb{Z}$.

   (c) Show that an element a has order 4 in $\mathbb{Z}/m\mathbb{Z}$ if and only if its square a^2 has order 2.

   (d) Deduce that if $p > 2$ is prime, then the elements of order 4 in $\mathbb{Z}/p\mathbb{Z}$ are the elements a with $a^2 \equiv -1 \pmod{p}$.

---

7. Let $m \geq 2$ be an integer. The goal of this problem is to study the value of $(m-1)!$ modulo m.

   (a) If m is prime, show that $(m-1)! + 1$ is divisible by m.

   (b) Show that $m = 4$ is a counterexample to the statement of the proposition below, and identify the error in the proof:
   Proposition: If m is composite, then $(m-1)!$ is divisible by m.
   Proof: Suppose $m = ab$ where a and b are greater than 1 and less than m. Then both a and b appear as terms in the product $(m-1)! = (m-1) \cdot (m-2) \cdots 2 \cdot 1$, so $(m-1)!$ is divisible by ab.

   (c) If m is composite and greater than 4, prove that $(m-1)!$ is in fact divisible by m.
