E. Dummit's Math 3527 ~ Number Theory I, Spring 2022 ~ Homework 4, due Fri Feb 18th.

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. 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.
   (f) The smallest positive integer s such that $3^s \equiv 1 \pmod{11}$.
   (g) The values of $\varphi(101)$, $\varphi(40000)$, and $\varphi(6^{10})$.
   (h) The number of positive integers less than or equal to 2020 that are relatively prime to 2020.
   (i) The remainder when 2^{4000} is divided by 41.
   (j) The remainder when 3^{65} is divided by 17.
   (k) The last two digits of 519^{242} when it is written out in base 10.
   (l) A unit that has order $\varphi(18)$ modulo 18.

---

2. 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 using Euler's theorem to reduce the size of the exponent.
   (c) 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.
   (d) Suppose you are asked to compute $551061249623402^{212491283589123452346457346325457999248101 34}$ modulo pq, where $p = 32475982347098567309881$ and $q = 43498562345124558203957$. (These values p and q are both prime.) Without actually doing the calculation, which of the methods (a)-(c) would be most efficient? Explain.
   (e) Suppose you are asked to compute $4359827345989033^{338381313096502512487912 7509}$ modulo N, where $N = 774474179081739059134688868419410928055229466015696684839317695166499006603861910228042427007 9583$, 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)-(c) would be most efficient? Explain.

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

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

---

4. Let $n = \underline{d_k d_{k-1} \dots d_1 d_0}$ be a positive integer written in base 10, so that $n = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10 + d_0$, where each d_i is a digit with $d_i \in \{0, 1, \dots, 9\}$, and the leading digit $d_n \neq 0$. It is a straightforward proof by strong induction that every positive integer has a unique base-10 representation.

   (a) Show that $n \equiv d_0 + d_1 + \cdots + d_k \pmod 9$, and deduce that n is divisible by 9 precisely when the sum of the digits of n is divisible by 9.

   (b) Show that $n \equiv d_0 - d_1 + d_2 - \cdots + (-1)^n d_n \pmod{11}$, and deduce that n is divisible by 11 precisely when the alternating sum of the digits of n is divisible by 11.

---

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

   (a) If p 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 $a^2 \equiv -1 \pmod p$.

---

6. Let $m \geq 2$ be an integer.

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

   (b) If m is composite and greater than 4, show that $(m-1)!$ is divisible by m. What happens when $m = 4$? [Hint: If $m = ab$, there are two cases, one where $a \neq b$ and the other where $a = b$.]

---

7. Let $n \geq 2$ be an integer.

   (a) Show that 2 has order n modulo $2^n - 1$. [Hint: What are 2^1, 2^2, ... , 2^{n-1} modulo $2^n - 1$?]

   (b) Show that n divides $\varphi(2^n - 1)$.
