E. Dummit's Math 3527 ~ Number Theory I, Spring 2023 ~ Homework 5, due Tue Feb 14th.

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 values of $\varphi(101)$, $\varphi(40000)$, and $\varphi(6^{10})$.
   (b) The number of positive integers less than or equal to 2023 that are relatively prime to 2023.
   (c) The last two digits of 519^{242} when it is written out in base 10.
   (d) A unit that has order $\varphi(18)$ modulo 18.
   (e) The order of 10 modulo 41.
   (f) The order of 10 modulo 89.
   (g) The rational number with decimal expansion $0.\overline{2023}$.
   (h) The rational number with decimal expansion $0.\overline{123456789}$.
   (i) The rational number with decimal expansion $3.14\overline{592}$.
   (j) The period of the repeating decimal 9/41 and its expansion. [Hint: See part e.]
   (k) The period of the repeating decimal 7/89. [Hint: See part f.]
   (l) The period of the repeating decimal 4/23.
   (m) All primes p such that $1/p$ has a repeating decimal expansion of period 5.
   (n) All primes p such that $1/p$ has a repeating decimal expansion of period 6.

---

2. Find the following things, and include relevant justification (you do not need to give details of successive squarings, just the results of computing powers):
   (a) The order of 5 modulo 97.
   (b) The order of 5 modulo 102.
   (c) The order of 2 modulo 81.
   (d) The order of 5 modulo 2022.
   (e) Which of the elements from (a)-(d) are primitive roots?

---

3. Let $m = 2029$. Notice that m is prime and also that the prime factorization of $m-1$ is $2028 = 2^2 \cdot 3 \cdot 13^2$.
   (a) Show that 2 is a primitive root modulo m.
   (b) Find all the solutions to the congruence $x^2 \equiv 3 \pmod{m}$, given that $3 \equiv 2^{1980} \pmod{m}$.
   (c) Find all the solutions to the congruence $x^5 \equiv 1 \pmod{m}$.
   (d) Find all of the elements of order 4 modulo m. [Hint: Problem 6 from homework 4 may be of use.]

---

4. The message **BRKNARJWQDBTRNBJANCQNENAHKNBCMXPB** has been encrypted using a Caesar shift. Decode it.

---

5. Consider the Rabin cryptosystem with key $N = 1\,359\,692\,821 = 32359 \cdot 42019$.
   (a) Encode the plaintext $m = 414\,892\,055$.
   (b) Find the four decodings of the ciphertext $c = 823\,845\,737$.

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

6. 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 $\varphi(2^n - 1)$.

---

7. The goal of this problem is to show that if $N = pq$ is an Rabin/RSA modulus, then computing $\varphi(N)$ is equivalent to factoring N.

   (a) Suppose that $N = pq$ and $\varphi = (p-1)(q-1)$, where p, q are real numbers. Find a formula for p and q in terms of N and φ.

   (b) Deduce that if $N = pq$ is a product of two primes, then factoring N is equivalent to computing $\varphi(N)$.

   (c) Given the information that N is a product of two primes, where

$$\begin{aligned} N &= 116508516476947091445330217632 01 \\ \varphi(N) &= 116508516476947017494175999912 52 \end{aligned}$$

   find the prime factors of N.
