E. Dummit's Math 3527 $\sim$ Number Theory I, Spring 2020 $\sim$ Homework 5, due Wed Feb 12th.

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.

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

1. Find the following things:
   (a) The order of 5 modulo 97.
   (b) The order of 10 modulo 41.
   (c) The order of 5 modulo 102.
   (d) The order of 10 modulo 89.
   (e) The order of 2 modulo 81.
   (f) The order of 3 modulo 2020.
   (g) Which of the elements from (a)-(f) are primitive roots?

---

2. Calculate each of the following things:
   (a) The rational number with decimal expansion $0.\overline{1213}$.
   (b) The rational number with decimal expansion $0.\overline{123456789}$.
   (c) The rational number with decimal expansion $0.26\overline{7}$.
   (d) The rational number with decimal expansion $3.14\overline{592}$.
   (e) The period of the repeating decimal $9/41$ and its expansion. [Hint: See 1(b).]
   (f) The period of the repeating decimal $4/23$.
   (g) The period of the repeating decimal $7/89$.
   (h) All primes p such that $\frac{1}{p}$ has a repeating decimal expansion of period 5.
   (i) All primes p such that $\frac{1}{p}$ has a repeating decimal expansion of period 6.

---

3. Let $m = 2027$. Notice that m is prime and also that the prime factorization of $m - 1$ is $2026 = 2 \cdot 1013$.
   (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 $3 \equiv 2^{282} \pmod{m}$.
   (c) Find all the solutions to the congruence $x^5 \equiv 1 \pmod{m}$.

---

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

---

5. One special class of substitution ciphers consists of the affine ciphers, which encode letters using a linear function of the form $f(x) = mx + b \pmod{26}$, where we take the convention that **a** corresponds to the residue class $0 \pmod{26}$, **b** corresponds to $1 \pmod{26}$, ... , and **z** corresponds to $25 \pmod{26}$.

   (a) Encrypt the message **doitnow** using the affine cipher $f(x) = 3x + 11 \pmod{26}$.

   If the function $f(x) = ax + b \pmod{26}$ is used to encrypt a message, then the function $f^{-1}(x) = a^{-1}(x - b) \pmod{26}$ will decrypt the message.

   (b) Find the decryption function for the encryption function $f(x) = 3x + 11 \pmod{26}$ and use it to decrypt the message **QGLQNLAAJYX**.

   (c) In order for an affine cipher to be decryptable, the function $f(x) = ax + b \pmod{26}$ must have a valid inverse function. Using this information, determine the total number of possible affine encryption functions (include the functions with $a = 1$ in your count).

   (d) Is affine encryption difficult to break or easy to break? Explain briefly.

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

6. Observe that $1/7 = 0.\overline{142857}$, and that $142 + 857 = 999$. The goal of this problem is to prove in general that if p is prime and the repeating-decimal expansion of d/p has even period $2k$, then the sum of the k-digit first half of the repeating part with the k-digit last half is equal to the k-digit number $999 \cdots 9$.

   (a) Verify the result for $1/13$ (of period 6) and $4410/9091$ (of period 10).

   (b) If d/p has even period $2k$, show that p divides $10^k + 1$. [Hint: Explain why p cannot divide $10^k - 1$.]

   (c) Suppose that $d/p = 0.\overline{a_1 a_2 \cdots a_k b_1 b_2 \cdots b_k}$. If $A = a_1 a_2 \cdots a_k$ and $B = b_1 b_2 \cdots b_k$, show that $10^k - 1$ must divide $A + B$. [Hint: Show that $\dfrac{(10^k + 1)d}{p} = A + \dfrac{A + B}{10^k - 1}$.]

   (d) With notation as in part (b), deduce that $A + B = 10^k - 1 = 999 \cdots 9$. [Hint: How large can $A + B$ be?]

---

7. The goal of this problem is to show that if $N = pq$ is an 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

$$\begin{aligned} N &= 8130390764015866244802763 \\ \varphi(N) &= 8130390764010072092213320 \end{aligned}$$

   find the prime factors of N.
