

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 2024 that are relatively prime to 2024.
  - (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  $0.\overline{2024}$ .
  - (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 exactly 5.
  - (n) All primes  $p$  such that  $1/p$  has a repeating decimal expansion of period exactly 6.
- 

2. Find the following things, and include relevant justification (you can just give the results of the needed modular exponentiations; you do not need to give details of the calculations.):

- (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 2024.
  - (e) Which of the elements from (a)-(d) are primitive roots?
- 

3. Let  $p = 2029$ . Notice that  $p$  is prime and also that the prime factorization of  $p - 1$  is  $2028 = 2^2 \cdot 3 \cdot 13^2$ .

- (a) Show that 2 is a primitive root modulo  $m$ . (You can just give the results of the needed modular exponentiations; you do not need to give details of the calculations.)
  - (b) Find all four solutions to the congruence  $x^4 \equiv 1 \pmod{p}$ .
  - (c) Find both solutions to the congruence  $x^2 \equiv 3 \pmod{m}$ , given that  $3 \equiv 2^{1980} \pmod{p}$ .
- 

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

---

5. Consider the Rabin cryptosystem with key  $N = 1359692821 = 32359 \cdot 42019$ .

- (a) Encode the plaintext  $m = 117285016$ .
  - (b) Find the four decodings of the ciphertext  $c = 823845737$ .
-

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

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. 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  $\varphi$ .
  - (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

$$\begin{aligned} N &= 22592848554175369912787642584639796662881202104422604037797641281978785567961 \\ \varphi(N) &= 22592848554175369912787642584639796662567375207606558304355492609701088213924 \end{aligned}$$

find the prime factors of  $N$ . (You can just give the first six and last six digits of each: e.g., as 123456...135791.)

---