1. Find the following things:

(a) The order of 5 modulo 97.
   - By Fermat (or Euler), the order of 5 divides \( \varphi(97) = 96 \), and \( 5^{96} \equiv 1 \pmod{97} \).
   - Using successive squaring we can compute \( 5^{96/2} \equiv 5^{48} \equiv -1 \pmod{97} \) and \( 5^{96/3} \equiv 5^{32} \equiv 35 \pmod{97} \). Hence the order cannot divide 48 or 32, and so 5 must have \text{order 96}.

(b) The order of 10 modulo 41.
   - By Fermat (or Euler), the order of 10 divides \( \varphi(41) = 40 \), and \( 10^{40} \equiv 1 \pmod{41} \).
   - Using successive squaring we can compute \( 10^{40/2} \equiv 10^{20} \equiv 1 \pmod{41} \) and \( 10^{40/5} \equiv 10^8 \equiv 16 \pmod{41} \), so the order of 10 in fact divides 20.
   - Then we can compute \( 10^{20/2} = 10^{10} = 1 \pmod{41} \) so the order divides 10, and in fact \( 10^{10/2} = 10^5 \equiv 1 \pmod{41} \) so the order divides 5. Since the order is not 1, we conclude that 10 has \text{order 5}.

(c) The order of 5 modulo 102.
   - By Euler, the order of 5 divides \( \varphi(102) = \varphi(2 \cdot 3 \cdot 17) = 32 \), and \( 5^{32} \equiv 1 \pmod{102} \).
   - Then \( 5^2 \equiv 25, 5^4 \equiv 13, 5^8 \equiv 67, 5^{16} \equiv 1 \pmod{102} \). Hence 5 has \text{order 16}.

(d) The order of 10 modulo 89.
   - By Fermat (or Euler), the order of 10 divides \( \varphi(89) = 88 \), and \( 10^{88} \equiv 1 \pmod{89} \).
   - Using successive squaring we can compute \( 10^{88/2} \equiv 10^{44} \equiv 1 \pmod{89} \) and \( 10^{88/11} \equiv 10^8 \equiv 45 \pmod{89} \). Hence the order in fact divides 44.
   - Then we can find \( 10^{44/2} \equiv 10^{22} \equiv -1 \pmod{89} \) and \( 10^{44/11} \equiv 10^4 \equiv 32 \pmod{89} \). Since neither of these is congruent to 1, we conclude that the order cannot divide 22 or 4, so 10 has \text{order 44}.

(e) The order of 2 modulo 81.
   - By Euler, the order of 2 divides \( \varphi(81) = 80 \), and \( 2^{80} \equiv 1 \pmod{81} \).
   - Using successive squaring we can compute \( 2^{80/2} \equiv 2^{40} \equiv 1 \pmod{81} \) and \( 2^{80/3} \equiv 2^{20} \equiv 28 \pmod{81} \). Hence the order cannot divide 27 or 18, and so 2 must have \text{order 54}.

(f) The order of 3 modulo 20.
   - By Euler, the order of 3 divides \( \varphi(200) = \varphi(2^2 \cdot 5 \cdot 101) = 800 \), and \( 3^{800} \equiv 1 \pmod{200} \).
   - Using successive squaring we can compute \( 3^{800/2} \equiv 3^{400} \equiv 1 \pmod{200} \) and \( 3^{800/5} \equiv 3^{160} \equiv 541 \pmod{200} \). Hence the order in fact divides 400 (but not 160).
   - Then \( 3^{400/2} = 3^{200} \equiv 1 \pmod{200} \) so the order divides 200, and \( 3^{200/2} = 3^{100} \equiv 1 \pmod{200} \) so the order divides 100. But since \( 3^{100/2} = 3^{50} \equiv 1009 \pmod{200} \) and \( 3^{100/5} \equiv 1801 \pmod{200} \) the order cannot divide 50 or 20, so 3 has \text{order 100}.

(g) Which of the elements from (a)-(f) are primitive roots?
   - We are looking for the elements modulo \( m \) having order \( \varphi(m) \).
   - The elements 5 mod 97 from (a) and 2 mod 81 from (e) are primitive roots, and the others are not.

2. Calculate each of the following things:

(a) The rational number with decimal expansion 0.1273.
   - If \( x = 0.1273 \) then \( 10^4x = 1213.1273 \) so \( (10^4 - 1)x = 1213 \) and so \( x = \frac{1213}{9999} \).

(b) The rational number with decimal expansion 0.123546789.
• If $x = 0.123456789$ then $(10^9 - 1)x = 123456789$ so $x = \frac{123456789}{999999999} = 0.123456789$.

(c) The rational number with decimal expansion 0.267.

• If $x = 0.267$ then $(10^3 - 10^2)x = 267 - 26 = 241$ so $x = \frac{241}{900}$.

(d) The rational number with decimal expansion 3.14592.

• If $x = 3.14592$ then $(10^5 - 10^2)x = 314592 - 314 = 314278$ so $x = \frac{314278}{99900} = 3.14592$.

(e) The period of the repeating decimal 9/41 and its expansion. [Hint: See 1(b).]

• The period is the order of 10 modulo 41, which we calculated in 1(b) to be 5.

• Then the repeating part is $\frac{9}{41}(10^5 - 1) = 21951$, so $\frac{9}{41} = 0.227018978125$.

(f) The period of the repeating decimal 4/23.

• The period is the order of 10 modulo 23. This order divides $\varphi(23) = 22$.

• Since $10^{22/2} \equiv 10^{11} \equiv -1 \pmod{23}$ and $10^{22/11} \equiv 10^2 \equiv 8 \pmod{23}$, the order must be 22.

• Indeed, one can evaluate $\frac{4}{23} = 0.1739130434782608695652$.

(g) The period of the repeating decimal 7/89.

• The period is the order of 10 modulo 89, which was calculated in 1(e) as 44.

• Indeed, one can evaluate $\frac{7}{89} = 0.4494382022471910112359550561797772808988764$.

(h) All primes $p$ such that $\frac{1}{p}$ has a repeating decimal expansion of period 5.

• If $\frac{1}{p}$ has period 5, then $p$ must divide $10^5 - 1 = 9 \cdot 11111 = 3^2 \cdot 41 \cdot 271$.

• Since $\frac{1}{3}$ has period 1, we see that $p = 41, 271$. Indeed, $\frac{1}{41} = 0.02439$ and $\frac{1}{271} = 0.00369$.

(i) All primes $p$ such that $\frac{1}{p}$ has a repeating decimal expansion of period 6.

• If $\frac{1}{p}$ has period 6, then $p$ must divide $10^6 - 1 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$.

• Since $\frac{1}{3}$ has period 1, $\frac{1}{11} = 0.09$ has period 2, and $\frac{1}{37} = 0.027$ has period 3, we see that $p = 7, 13$.

• Indeed, $\frac{1}{7} = 0.142857$ and $\frac{1}{13} = 0.076923$.

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 $m$.

• By Euler’s Theorem, since $\varphi(2027) = 2026 = 2 \cdot 1013$, we need to show that $2^2$ and $2^{1013}$ are not congruent to 1 modulo $m$.

• We clearly have $2^2 \equiv 4 \pmod{m}$ and successive squaring yields $2^{1013} \equiv -1 \pmod{m}$. Since neither of these is 1 (mod $m$), we see that 2 is a primitive root.

(b) Find all the solutions to the congruence $x^2 \equiv 3 \pmod{m}$, given that $3 \equiv 2^{282} \pmod{m}$.

• We can solve the congruence by taking discrete logarithms to the base 2.

• From the given information we know that $3 \equiv 2^{282} \pmod{2027}$, so taking logarithms yields the equality $2 \log_2(x) \equiv 282 \pmod{2026}$. (Remember that discrete logarithms yield congruences modulo $\varphi(m)$ in general.)
• Cancelling the factor of 2 yields \( \log_2(x) \equiv 141 \pmod{1013} \), which has the two solutions \( \log_2 x = 141, 1154 \pmod{2026} \).

• Then \( x \equiv 2^{141}, 2^{1154} \pmod{m} \). Equivalently, this is \( x = 78, 1730 \pmod{m} \).

(c) Find all the solutions to the congruence \( x^5 \equiv 1 \pmod{m} \).

• We can solve the congruence by taking discrete logarithms to the base 2.

• This yields \( 5 \log_2(x) \equiv 0 \pmod{2026} \). Since 5 is relatively prime to 2026, it is a unit, so multiplying by its inverse yields \( \log_2(x) \equiv 0 \pmod{2026} \).

• Hence we only get the solution \( \log_2(x) \equiv 0 \pmod{2026} \), so that \( x \equiv 2^0 = 1 \pmod{m} \).

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

• By writing down all 26 possible shifts of this message, we see there is only one that makes sense, the shift backward by 6 letters. Alternatively, one could use a frequency analysis: the letter K appears 4 times, more than any other letter, which suggests that it decrypts to e.

• Either way, the decrypted message is huskiesarethebestdogs, which is unarguably true.

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

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

• Here is an encryption table:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10| 11| 12| 13| 14| 15| 16| 17| 18| 19| 20| 21| 22| 23| 24| 25|
| 0 | 14| 17| 20| 23| 0 | 3 | 6 | 9 | 12| 15| 18| 21| 24| 1 | 4 | 7 | 10| 13| 16| 19| 22| 25| 2 | 5 | 8 |

• So the ciphertext is UBJQYBZ.

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.

• We see \( 3^{-1} \equiv 9 \pmod{26} \) since we have \( 3 \cdot 9 \equiv 1 \pmod{26} \), so the decryption function is \( f^{-1}(x) = 9(x - 11) \equiv 9x + 5 \pmod{26} \).

• Making a table like the one in part (a), or simply evaluating the function on each letter, yields the decoded message thatsafline.

(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).

• From the formula \( f^{-1}(x) = a^{-1}(x - b) \) we see that \( a^{-1} \) must exist modulo 26, so it must be a unit. Thus, including the case \( a = 1 \), there are \( \phi(26) = 12 \) possible values for \( a \).

• Once \( a \) is chosen we may pick any value for \( b \), so in total there are \( 12 \cdot 26 = 312 \) possible affine encryption functions.

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

• Obviously it is easy to break since by part (c) there are only 312 possible decodings of any possible message, and this is a small enough number that it is possible to do decodings by hand.

• Also, since it is an example of a substitution cipher, it can also be easily broken using the same techniques (e.g., frequency analysis).
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 $999\ldots9$.

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

- We have $1/13 = 0.076923$ and indeed $076 + 923 = 999$.
- Likewise, $4410/9091 = 0.4850951490$ and indeed $48509 + 51490 = 99999$.

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

- Since $d/p$ has even period $2k$, we know that $p$ divides $10^{2k} - 1 = (10^k - 1)(10^k + 1)$.
- Furthermore, since the period is not $k$, $p$ does not divide $10^k - 1$.
- Since $10^k - 1$ and $10^k + 1$ are relatively prime (their difference is 2, which does not divide either term), we conclude that $p$ must divide $10^{2k} + 1$, as claimed.

(c) Suppose that $d/p = 0.a_1a_2\cdots a_k b_1b_2\cdots b_k$. 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 $\frac{(10^k + 1)d}{p} = A + B(10^k - 1)$]

- If $d/p = 0.a_1 a_2 \cdots a_k b_1 b_2 \cdots b_k$ then we have $(10^{2k} - 1) \cdot \frac{d}{p} = a_1 a_2 \cdots a_k b_1 b_2 \cdots b_k = 10^k A + B$.
- Then dividing both sides by $10^k - 1$ yields the expression $\frac{(10^k + 1)d}{p} = A + B \cdot \frac{10^k}{10^k - 1}$ from the hint.
- But now, because the left-hand side is an integer by part (a), the right-hand side must also be an integer, and therefore $10^k - 1$ must divide $A + B$.

(d) With notation as in part (b), deduce that $A + B = 10^k - 1 = 999\ldots9$. [Hint: How large can $A + B$ be?]

- Observe that $A + B$ is positive and less than $2(10^k - 1)$ because $A$ and $B$ are both at most $10^k - 1$ (and they cannot both be equal to $10^k - 1$).
- Therefore we have $0 < A + B < 2(10^k - 1)$. But since $A + B$ is a multiple of $10^k - 1$ by part (b), the only possibility is to have $A + B = 10^k - 1 = 999\ldots9$ as claimed.

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 $\varphi$.

- Since $N = pq$ we have $q = N/p$.
- Substitute into the equation for $\varphi$: we obtain $\varphi = (p - 1)(N/p - 1)$.
- This is equivalent to the quadratic equation $p^2 - (N - \varphi + 1)p + N = 0$, whose roots are $p, q = \frac{(N - \varphi + 1) \pm \sqrt{(N - \varphi + 1)^2 - 4N}}{2}$

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

- If we know the factorization of $N$ then we certainly can compute $\varphi(N) = (p - 1)(q - 1)$.
- Conversely, by part (a), if we know $N$ and $\varphi(N)$, then we can compute $p$ and $q$.

(c) Given the information that $N$ is a product of two primes, where $N = 8130390764015866244802763$ and $\varphi(N) = 8130390764010072092213320$ find the prime factors of $N$.

- We can simply use the formula from (a), since if $N = pq$ then $\varphi(N) = (p - 1)(q - 1)$.
- This gives $p, q = \frac{5794152589444 \pm 1025007889578}{2} = 2384572349933, 3409580239511$