1 A Number Theoretic Warm-Up

Answer each of the following questions with brief justification.

(a) What is the last digit of $15^{2021}$?
(b) What is the inverse of 3 modulo 20?
(c) For how many values of $a \pmod{10}$ does $a^{-1}$ exist modulo 10?

2 CRT Decomposition

In this problem we will find $3^{302} \pmod{385}$.

(a) Write 385 as a product of prime numbers in the form $385 = p_1 \times p_2 \times p_3$.
(b) Use Fermat’s Little Theorem to find $3^{302} \pmod{p_1}$, $3^{302} \pmod{p_2}$, and $3^{302} \pmod{p_3}$.
(c) Let $x = 3^{302}$. Use part (b) to express the problem as a system of congruences (modular equations $\pmod{385}$). Solve the system using the Chinese Remainder Theorem. What is $3^{302} \pmod{385}$?

3 Sparsity of Primes

A prime power is a number that can be written as $p^i$ for some prime $p$ and some positive integer $i$. So, $9 = 3^2$ is a prime power, and so is $8 = 2^3$. $42 = 2 \cdot 3 \cdot 7$ is not a prime power.

Prove that for any positive integer $k$, there exists $k$ consecutive positive integers such that none of them are prime powers.
Hint: This is a Chinese Remainder Theorem problem. We want to find \( x \) such that \( x + 1, x + 2, \ldots, x + k \) are all not powers of primes. We can enforce this by saying that \( x + 1 \) through \( x + k \) each must have two distinct prime divisors.

4 Baby Fermat

Assume that \( a \) does have a multiplicative inverse \( \text{mod} \ m \). Let us prove that its multiplicative inverse can be written as \( a^k \) (\( \text{mod} \ m \)) for some \( k \geq 0 \).

(a) Consider the infinite sequence \( a, a^2, a^3, \ldots \) (\( \text{mod} \ m \)). Prove that this sequence has repetitions. (\textbf{Hint:} Consider the Pigeonhole Principle.)

(b) Assuming that \( a^i \equiv a^j \) (\( \text{mod} \ m \)), where \( i > j \), what is the value of \( a^{i-j} \) (\( \text{mod} \ m \))?

(c) Prove that the multiplicative inverse can be written as \( a^k \) (\( \text{mod} \ m \)). What is \( k \) in terms of \( i \) and \( j \)?

5 Euler’s Totient Function

Euler’s totient function is defined as follows:

\[
\phi(n) = |\{i : 1 \leq i \leq n, \gcd(n, i) = 1\}|
\]

In other words, \( \phi(n) \) is the total number of positive integers less than or equal to \( n \) which are relatively prime to it. We develop a general formula to compute \( \phi(n) \).

(a) Let \( p \) be a prime number. What is \( \phi(p) \)?

(b) Let \( p \) be a prime number and \( k \) be some positive integer. What is \( \phi(p^k) \)?

(c) Show that if \( \gcd(m, n) = 1 \), then \( \phi(mn) = \phi(m)\phi(n) \). (\textbf{Hint:} Use the Chinese Remainder Theorem.)

(d) Argue that if the prime factorization of \( n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \), then

\[
\phi(n) = n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}.
\]

6 Using RSA

Kevin and Bob decide to apply the RSA cryptography so that Kevin can send a secret message to Bob.

1. Assuming \( p = 3, q = 11, \) and \( e = 7 \), what is \( d \)? Calculate the exact value.

2. Following part (a), what is the original message if Bob receives 4? Calculate the exact value.
7 Breaking RSA

Eve is not convinced she needs to factor $N = pq$ in order to break RSA. She argues: "All I need to know is $(p - 1)(q - 1)$... then I can find $d$ as the inverse of $e$ mod $(p - 1)(q - 1)$. This should be easier than factoring $N."$ Prove Eve wrong, by showing that if she knows $(p - 1)(q - 1)$, she can easily factor $N$ (thus showing finding $(p - 1)(q - 1)$ is at least as hard as factoring $N$).

8 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where $p, q, r$ are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod{N}$. 