AFRICAN INSTITUTE FOR MATHEMATICAL SCIENCES

(AIMS RWANDA, KIGALI)

Name: Darix SAMANI SIEWE	Assignment Number: 2
Course: Algebra and Cryptography	Date: March 8, 2025

Exercise 1

1. Let N bet the product of two distinct primes. shows that N is not a Carmichael numbers.

   definition of carmicheal numner a composite number n is a carmichael number if for every integer b that is copime to n, the congruence $b^{n-1} \equiv 1 \pmod{n}$.

   let's prove that $N = p \times q$ is Not a Carmichael Number

   Proof. Let $N = p \times q$, where p and q are distinct primes. A Carmichael number satisfies $\lambda(N) \mid (N-1)$, where $\lambda(N) = \operatorname{lcm}(p-1, q-1)$.

   Case 1: If $p = 2$, then $\lambda(N) = q - 1$. We require $q - 1 \mid 2q - 1$. However:

   $$2q - 1 = 2(q - 1) + 1,$$

   and $q - 1 \geq 2$ cannot divide 1. Thus, $\lambda(N) \nmid (N - 1)$.

   Case 2: If p and q are odd primes, $\lambda(N) = \operatorname{lcm}(p-1, q-1)$ is even, while $N-1 = pq-1$ is also even. However, $\operatorname{lcm}(p-1, q-1)$ typically exceeds the factorization of $pq - 1$, making $\lambda(N) \nmid (N - 1)$.

   In both cases, $\lambda(N) \nmid (N - 1)$, so N cannot be a Carmichael number. □

2. Let G be a cyclic group of order n. Consider two generators g1 and g2 of the group G. Show that $gcd(dlog_{g1}, (g2), n) = 1$.

   let's proof that : $\gcd(\operatorname{dlog}_{g_1}(g_2), n) = 1$

   Let G be a cyclic group of order n, and let g_1 and g_2 be generators of G. By definition, there exists an integer $k = \operatorname{dlog}_{g_1}(g_2)$ such that:

   $$g_2 = g_1^k.$$

   Since g_2 is a generator of G, its order is n. If $\gcd(k, n) = d > 1$, then the order of g_2 would be $\frac{n}{d} < n$, contradicting the fact that g_2

3. Let p be prime and $n \geq 1$. How many elements of even order do we have in $(Z/p^n Z)$?

   Let p be an odd prime and $n \geq 1$. The multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic of order:

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1).$$

   Since p is odd, $p-1$ is even, so $\phi(p^n)$ is even. In a cyclic group of even order, exactly half of the elements have even order. Thus, the number of elements of even order is:

$$\boxed{\frac{p^{n-1}(p-1)}{2}}.$$

4. Use the Eratosthene's sieve to find the (5000000 + n)-th prime number where n is your birthday (mmddyy). How many prime number do we have between 225 and 226?