Math 255 - Spring 2022
Some cryptography
10 points

This homework invites you to solve two number-theoretic problems that are inspired by mathematical cryptography.

The first problem is a simplified version of the index calculus attack, which is an attack on the discrete logarithm problem in $(\mathbb{Z}/p\mathbb{Z})^\times$ that is so powerful that it is no longer used in practice. Instead the "elliptic curve" version of the discrete logarithm problem is now used. The second problem is related to a different cryptographic scheme, RSA. It shows that if one already knows that n is a product of two distinct primes, then knowledge of these two primes is equivalent to knowledge of $\phi(n)$.

1. Let $n = 101$. The goal of this problem will be to compute $\log_3 17$ in $(\mathbb{Z}/101\mathbb{Z})^\times$.

   (a) We will first compute $\log_3 2$ in $(\mathbb{Z}/101\mathbb{Z})^\times$. We do this by following these steps:
   - Compute 2^7 and reduce your answer modulo 101.
   - Factor the new number that you obtained.
   - This should give you an equation satisfied by $\log_3 2$. Solve this equation.

   (b) What is $17^{-1} \pmod{101}$? Compute this number and call it b.

   (c) Use that $17b \equiv 1 \pmod{101}$ to get a relationship between $\log_3 2$ and $\log_3 17$. Using the value of $\log_3 2$ you computed in part (a), solve this equation for $\log_3 17$.

2. In this problem we will show how we can factor n given knowledge of the value of $\phi(n)$, under certain circumstances. This is a trick that it used to break the RSA cryptosystem when $\phi(n)$ is leaked or guessed. Throughout, suppose that n is a positive integer with $n = pq$, for p and q two distinct primes.

   (a) In this case what is $\phi(n)$?

   (b) From knowledge only of the values of n and $\phi(n)$, and knowledge of the fact that $n = pq$ is a product of two primes, explain how one can obtain the value of $p + q$.

   (c) From knowledge only of n and $\phi(n)$, and knowledge of the fact that $n = pq$ is a product of two primes, explain how one can obtain the values of p and q. Hint: What are the roots of the polynomial $x^2 - (p + q)x + n$?

   (d) Apply part (c) to factor the number $n = 4399$, which is of the form $n = pq$ for p and q two distinct primes, using the fact that $\phi(4399) = 4264$.