MATH/CSCI 408 Name: ____________________

CRYPTOGRAPHY PRIORITY MISSION 02 SOLUTIONS

Deadline: Thursday, 27 October 2016 at 11:59pm

Archer, Lana, and Ray get ambushed while on a mission after getting hit by tranquilizer darts in the jungle (from the henchman of the evil villain known as the "Annihilator.")

1. Ray wakes up first but is feeling woozy and has hallucinations in which Mallory is demanding that he computes the following Legendre symbols. Help him out so that he can focus on walking back to the escape vehicle (be sure to justify your answers).
   a. $\left(\frac{137}{151}\right) = 1$
   b. $\left(\frac{151}{137}\right) = 1$
   c. $\left(\frac{271}{151}\right) = -1$
   d. $\left(\frac{151}{271}\right) = 1$

2. Lana wakes up in a cell to find that the Annihilator standing before her. It turns out that the Annihilator is actually an evil mathematician, and she asks Lana to prove that there are infinitely many prime numbers. Help Lana out by following these steps:
   a. Prove that for any natural number n, that $\gcd(n, n+1) = 1$. [Hint: start by supposing that an integer a is such that $a \mid n$ and $a \mid (n+1)$. What does that mean in terms of the definitions? Then, notice that $1 = n + 1 - n$. How can you rewrite this using the definitions you just wrote?]

   Suppose $a \mid n$ and $a \mid (n+1)$. Then there exist integers k and l such that $ka = n$ and $la = n + 1$. Note that $1 = n + 1 - n = la - ka = (l - k)a$ meaning that $a \mid 1$, or that $a = 1$ must be true. Thus, $\gcd(n, n+1) = 1$.

   b. Now suppose there are only finitely many primes $p_1, p_2, \cdots, p_N$ for a natural number N (for the sake of contradiction). Consider the number which is the product of all the primes plus one, or $p_1 p_2 \cdots p_N + 1$. What can you say using part a. of this problem?

   Suppose there are only finitely many primes $p_1, p_2, \cdots, p_N$ for a natural number N. Consider the number which is the product of all the primes plus one, or $p_1 p_2 \cdots p_N + 1$. By part a. we know that $\gcd(p_1, p_2, \cdots, p_N, p_1, p_2, \cdots, p_N + 1) = 1$. We have two cases. Case 1: if $p_1, p_2, \cdots, p_N + 1$ is prime, then we have found another prime that is not in the original list, which is a contradiction. Case 2: if $p_1, p_2, \cdots, p_N + 1$ is not prime, then a prime factor p divides it, but p also divides $p_1, p_2, \cdots, p_N$, which is a contradiction to the gcd condition. Thus, our original assumption is false, and there are infinitely many primes.

3. Archer also wakes up in a cell but finds several of the Annihilator's henchmen demanding that he uses the Euclidean algorithm to find the greatest common divisor of 16891 and 589. Krieger (who is still in communication with Archer via a hidden ear piece) tells Archer that the answer is 19, but the henchmen aren't satisfied until Archer shows all of

his work. Help him out.

$$\begin{aligned}16891 &= 589(28) + 399\\ 589 &= 399(1) + 190\\ 399 &= 190(2) + 19\\ 190 &= 19(10) + 0\end{aligned}$$

so the gcd is 19.

4. Pam and Cheryl are waiting on the escape vehicle, wondering what is taking so long. They get bored and start computing the following:
   a. $\varphi(23) = 22$

   b. $\varphi(32) = 16$

   c. $\varphi(p) = p - 1$ where p is a prime number. This is because a prime number is defined to only have factors of p and 1, so all numbers up to p are relatively prime.

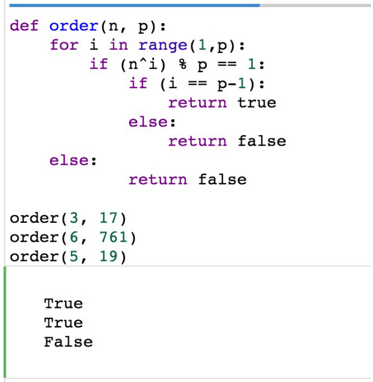
   d. $8^{278} \bmod 13 \equiv (8^{12})^{23} \cdot 8^2 \equiv 1 \cdot 64 \bmod 13 \equiv 12 \bmod 13$

   e. $7^{496} \bmod 32 = (7^{16})^{31} \equiv 1 \bmod 32$

5. Out of nowhere, Babou jumps out and attacks the Annihilator. Do the following while Lana and Archer escape:

   a. Find a primitive root of $p = 17$, and show you you verify that it is a primitive root. 3 is a primitive root because $3^{16} \equiv 1 \bmod 17$ and $3^i \not\equiv 1 \bmod 17$ for all $i \in \{1, 2, \cdots 15\}$.

   b. Write a SageMath program to check if an integer n is a primitive root of a given prime p. Be sure to provide an example of n being a primitive root and an example where it isn't.
   (Code by Hailey Crouse)



```
def order(n, p):
    for i in range(1,p):
        if (n^i) % p == 1:
            if (i == p-1):
                return true
            else:
                return false
    else:
            return false

order(3, 17)
order(6, 761)
order(5, 19)
```

```
    True
    True
    False
```

6. Now that the Annihilator is defeated (via ocelot), her henchmen want to divide up her treasure (in the form of x gold bricks that she had in a vault). 149 henchmen start to divide up the treasure evenly, but realize that there are 3 gold bars left over, so they get in a fight. Two henchmen are critically wounded and taken to the hospital.

   a. Before the remaining 147 henchmen get in a fight again, you jump in because you believe a peaceful solution is the best solution. Explain to the henchmen how you can use the Chinese Remainder Theorem to guarantee that the x gold bricks can be divided evenly as long (as there are enough gold bricks).
   First note that $\gcd(149, 147) = 1$. We can set up the following equivalences and guarantee a solution using the Chinese Remainder Theorem:

   $$x \equiv 3 \bmod 149$$
   $$x \equiv 0 \bmod 147$$

   b. Use SageMath's `crt(a,b,m,n)` to show what the minimum number of gold bricks x must be.
   `crt(3,0,149,147) = 10731`