Crypto Homework 4

Noah Wong

October 2018

1.) Using a cipher wheel, decrypt the following message, which was encrypted by rotating 1 clockwise for the first letter, then 2 clockwise for the second letter, etc.

XJHRF TNZHM ZGAHI UETXZ JNBWN
UTRHE POMDN BJMAU GORFA OIZOC C

This message translates to "When angry count ten before you speak if very angry an hundred".

2.) Let $\{p_1, p_2, \cdots, p_r\}$ be a set of prime numbers, and let

$$N = p_1 p_2 \cdots p_r + 1$$

Prove that N is divisible by some prime not in the original set. Use this fact to deduce that there must be infinitely many prime numbers.

Proof. We prove that there are infinitely many prime numbers by contradiction. So assume there are finitely many prime numbers, thus we can list them as

$$p_1, p_2, p_3, \dots p_k.$$

Define a number N as

$$N = p_1 p_2 \cdots p_r + 1,$$

this N is not divisible by any prime in our list. $N = p_1(p_2 p_3 \cdots p_k) + 1$, so dividing by p_1 gives us a remainder of 1, $p_1 \not| N$. Similarly dividing by p_2 gives a remainder of 1 so $p_2 \not| N$, as well as $p_3 \not| N, \cdots, p_k \not| N$. Thus none of the primes in the list are a divisor of N. By the fundamental theorem of arithmetic N must divide at least one prime. So there exists a prime that divides N not in our list. This is a contradiction of the assumption that there are finitely many primes. Thus there must be infinitely many primes.

□

3.) Find all values of x between 0 and $m - 1$ that are solutions of the following congruences.
(a) $x + 17 \equiv 23 \pmod{37}$

$$x \equiv 23 - 17 \pmod{37}$$

$$x \equiv 6 \pmod{37}$$

(b)$x^2 \equiv 3 \pmod{11}$

$$x \equiv 5 \pmod{11} \text{ and } x \equiv 6 \pmod{11}$$

For this problem we just squared every number $1, \dots, 10$ and found which one returned 3.

(c) $x^2 \equiv 2 \mod 13$
There is no x in which this equation holds. We also just squared each number and found which one returned 2 in this case there were none.

(d) Find a single value x that simultaneously solves the two congruences.

$$x \equiv 3 \pmod 7 \; x \equiv \quad \pmod 9$$

First we use the Euclidean algorithm to find the linear combination of 9 and 7.

$$9 = 7(1) - 2$$
$$7 = 2(3) - 1$$

Then rearranging this equations.

$$1 = 7 - (9 - 7)(3)$$
$$1 = 7(4) + 9(-3)$$

Next we multiply the linear combination of $7(4)$ by 4 and multiply $9(-3)$ by 3 and take the sum modulo $9 * 7$.

$$4(7)(4) + 3(9)(-3) \equiv 112 - 81 \equiv 31 \pmod{61}$$

So our answer is $x = 31$.