Graded Homework 4

Kimberly Mandery

10/24/2018

1. (20 points) 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

block XJHRF(shift 1-5)	whena	block TNZHM(shift 6-10)	ngryc
block ZGAHI(shift 11-15)	ountt	block UETXZ(shift 16-20)	enbef
block JNBWN(shift 21-25)	oreyo	block UTRHE(shift 0-4)	uspea
block POMDN(shift 5-9)	kifve	block BJMAU(shift 10-14)	ryang
block GORFA(shift 15-19)	ryanh	block OIZOC(shift 20-24)	undre
block C(shift 25)	d		

   "When angry, count ten before you speak. If very angry, an hundred"

2. (20 points) Let $\{p_1, p_2, \ldots, p_r\}$ 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. (This proof of the infinitude of primes appears in Euclid's *Elements*. Prime numbers have been studied for thousands of years.)

   Proof: Suppose N can be written as a product of primes in the set $\{p_1, p_2, \ldots p_j\}$ such that

$$N = p_1 p_2 \ldots p_j$$

   . We can observe that

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

   from $N = p_1 p_2 \cdots p_r + 1$. Since two consecutive numbers only differ by 1, there is no prime we can multiply $N-1$ by in order to obtain $p_1, p_2, \ldots p_j$. Thus, there must exist a $p_j* \in \{p_1, p_2, \ldots p_j\}$ where $p_j* \notin \{p_1, p_2, \ldots, p_r\}$. This works for both finite and infinite sets of primes.

3. (20 points) Find all values of x between 0 and $m-1$ that are solutions of the following congruences.

   (a) $x + 17 \equiv 23 \pmod{37}$
   $x \equiv (23 - 17) \pmod{37}$
   $x \equiv 6 \pmod{37}$
   The solution is $x = 6$.

   (b) $x^2 \equiv 3 \pmod{11}$
   $5^2 \equiv 3 \pmod{11}$
   $6^2 \equiv 3 \pmod{11}$
   The solutions $x = 5, 6$ were found by trial and error.

   (c) $x^2 \equiv 2 \pmod{13}$
   No solutions in the interval from 0 to 13 give such an equivalency.

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

   $$x \equiv 3 \pmod{7} \qquad\qquad x \equiv 4 \pmod{9}.$$

   [Hint Note that every solution of the first congruence looks like $x = 3 + 7y$ for some y. Substitute this into the second congruence and solve for y; then use that to get x.]

   Using the hint from above and the Euclidean Algorithm, we can use x=9 and y=7 to get $9 \equiv 7(1) + 2$. We can repeat the algorithm using x=7 and y=2 to obtain $7 \equiv 2(3) + 1$. Since we obtained 1 for a remainder we can stop. Rearranging both we obtain $2 \equiv 9 - 7(1)$ and $1 \equiv 7 - 2(3)$. Combining these two equations, we get $1 \equiv 7 - (9 - 7(1))(3)$ which is equal to $7 + 9(-3) + 7(3)$. Combining like terms, we get $7(4) + 9(-3)$. To finish, we must consider which mod to use and can do the following by using the Chinese Remainder Theorem. Since we combined 7 and 9, the mod is now $7 * 9$, or 63. The final combination is $4(7*4) + 3(9*-3) mod(9*7) \equiv 112 - 81 mod(63) \equiv 31$