Math 110 Problem Set 1 Solutions

2.2 The ciphertext UCR was encrypted using the affine function $9x + 2$ mod 26. Find the plaintext.

Solution: Given y, we need to solve

$$\begin{aligned} y &\equiv 9x + 2 \bmod 26 \\ \Rightarrow y - 2 &\equiv 9x \bmod 26 \end{aligned}$$

Checking, we see that 3 is the inverse of 9 modulo 26, as 9*3 is 1 modulo 26. Thus, the above is solved by

$$x \equiv 3 * 9x \equiv 3 * (y - 2) \bmod 26$$

Let us apply this to UCR. We have $U = 20$, $C = 2$, $R = 17$. Thus, calculating:

$$\begin{aligned} 3 * (20 - 2) \equiv 54 \equiv 2 \bmod 26 \\ 3 * (2 - 2) \equiv 0 \bmod 26 \\ 3 * (17 - 2) \equiv 45 \equiv 19 \bmod 26 \end{aligned}$$

Thus, converting back, we see that the plaintext was CAT.

2.3 Encrypt *howareyou* using the affine function $5x + 7$ (mod 26). What is the decryption function? Check that it works.

Solution: Let's calculate this:

$$\begin{aligned} &h = 7: \ 5 * 7 + 7 \equiv 42 \equiv 16 \bmod 26 \\ &o = 14: \ 5 * 14 + 7 \equiv 77 \equiv 25 \bmod 26 \\ &w = 22: \ 5 * 22 + 7 \equiv 117 \equiv 13 \bmod 26 \\ &a = 0: \ 5 * 0 + 7 \equiv 7 \bmod 26 \\ &r = 17: \ 5 * 17 + 7 \equiv 92 \equiv 14 \bmod 26 \\ &e = 4: \ 5 * 4 + 7 \equiv 27 \equiv 1 \bmod 26 \\ &y = 24: \ 5 * 24 + 7 \equiv 127 \equiv 23 \bmod 26 \\ &o = 14: \ 5 * 14 + 7 \equiv 16 \bmod 26 \\ &u = 20: \ 5 * 20 + 7 \equiv 107 \equiv 3 \bmod 26 \end{aligned}$$

Thus, converting this to letters, we get *qznhobxqd*. Let us find the decryption function. Note that $5 * 5 \equiv 25 \equiv -1$ mod 26 so $-5 \equiv 21$ mod 26 is the inverse of 5 modulo 26. Thus, solving

$$\begin{aligned} y &\equiv 5x + 7 \bmod 26 \\ \Rightarrow x &\equiv 21(y - 7) \equiv 21y + 9 \end{aligned}$$

Let us use this do decrypt *qznhobxqd*.

$$\begin{aligned}
q = 16 :&\ \ 21 * 16 + 9 \equiv 345 \equiv 7 \bmod 26\\
z = 25 :&\ \ 21 * 25 + 9 \equiv 534 \equiv 14 \bmod 26\\
n = 13 :&\ \ 21 * 13 + 9 \equiv 282 \equiv 22 \bmod 26\\
h = 7 :&\ \ 21 * 7 + 9 \equiv 156 \equiv 0 \bmod 26\\
o = 14 :&\ \ 21 * 14 + 9 \equiv 303 \equiv 17 \bmod 26\\
b = 1 :&\ \ 21 * 1 + 9 \equiv 30 \equiv 4 \bmod 26\\
x = 23 :&\ \ 21 * 23 + 9 \equiv 492 \equiv 24 \bmod 26\\
q = 16 :&\ \ 21 * 16 + 9 \equiv 345 \equiv 7 \bmod 26\\
d = 3 :&\ \ 21 * 3 + 9 \equiv 72 \equiv 20 \bmod 26
\end{aligned}$$

Thus, we decrypt *qznhobxqd* to *howareyou*, as expected.

2.6 Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher (both are working mod 26). Is there any advantage to doing this, rather than using a single affine cipher? Why or why not?

Solution: There is no advantage. Say we use the affine function $ax + b$ (mod 26) followed by the affine function $cx + d$ (mod 26). In that case, at the end, x will be mapped to $c(ax+b)+d = acx+(bc+d)$ (mod 26), which is just another affine function. Hence we get no advantage from using two affine functions.

2.10 Suppose there is a language that has only the letters a and b. The frequency of the letter a is .1 and the frequency of b is .9. A message is encrypted using a Vigenère cipher (working mod 2 instead of mod 26). The ciphertext is $BABABAAABA$.

(a) Show that key length is probably 2.
(b) Using the information on the frequences of the letters, determine the key and decrypt the message.

Solution:
(a)Let us count the number of coincidences with various displacements.
Displacement of 1:

$$\begin{array}{l}BABABAAABA\\ BABABAAABA\end{array}$$

Hence, with a displacement of 1 we have 2 coincidences.
Displacement of 2:

$$\begin{array}{l}BABABAAABA\\ BABABAAABA\end{array}$$

Hence, with a displacement of 2 we have 7 coincidences.
Displacement of 3:

$$BABABAAABA$$
$$BABABAAABA$$

Hence, with a displacement of 3 we have 2 coincidences.
We see that if we displace by 4 or more we have an overlap of at most 6, so we have the maximal number of coincidences with a displacement of 2. Hence, the key length is probably 2.

(b) Let us look at the 1st, 3rd, 5th,... letters and see which letter occurs most frequently. We see that we have 4 Bs and 1 A. Since B occurs much more frequently in these letters, and the frequency of B in the language is .9, we conclude that the first number in our key is 0. Now, look at the 2nd, 4th,... letters. We have 5 As and no Bs. This implies that the second number in our key is 1. Thus, the key is $\{0, 1\} = \{A, B\}$ and the message decrypts to $BBBBBBABBB$.

2.11 Suppose you have a language with only the 3 letters a, b, c, and they occur with frequencies .7,.2,.1, respectively. The following ciphertext was encrypted by the Vigenère method (shifts are mod 3 instead of mod 26, of course):

$$ABCBABBBAC$$

Suppose you are told that the key length is 1, 2, or 3. Show that the key length is probably 2, and determine the most probable key.

Solution: Let us count the number of coincidences with displacements of 1, 2, or 3.
Displacement of 1:

$$ABCBABBBAC$$
$$ABCBABBBAC$$

Hence, with a displacement of 1 we have 2 coincidences.
Displacement of 2:

$$ABCBABBBAC$$
$$ABCBABBBAC$$

Hence, with a displacement of 2 we have 3 coincidences.
Displacement of 3:

$$ABCBABBBAC$$
$$ABCBABBBAC$$

Hence, with a displacement of 3 we have 1 coincidence.

Thus, we see that the key length is probably 2. Let us now determine the most probable key. The 1st, 3rd,... letters contain 3 As, 1 B and 1 C. Since A has the highest frequency, this would imply that the first number in the key is 0. The 2nd, 4th,... letters contain 4 Bs and 1 C. Thus, the second number in the key is likely 1. Hence, the most probable key is $\{0,1\} = \{A,B\}$.

3.1
(a) Find integers x and y such that $17x + 101y = 1$.
(b) Find 17^{-1} (mod 101).

Solution:
(a) Let us use the extended Euclidean algorithm.

$$\begin{aligned} 101 &= 5 * 17 + 16 \\ 17 &= 1 * 16 + 1 \end{aligned}$$

Thus, we have that

$$1 = 17 - 1 * 16 = 17 - (101 - 5 * 17) = 6 * 17 - 101.$$

Thus, a solution to our equation is $x = 16$ and $y = -1$.

(b) From above, we have that

$$17 * 6 \equiv 1 \pmod{101}$$

so we have that 17^{-1} (mod 101) is 6 (mod 101).

3.3
(a) Find all solutions of $12x \equiv 28 \pmod{236}$.
(b) Find all solutions of $12x \equiv 30 \pmod{236}$.

Solution:
(a) Note that 4 divides all of 12, 28 and 236. Thus, dividing by 4, we get the congruence

$$3x \equiv 7 \pmod{59}$$

It is clear from inspection that $3 * 20 \equiv 1 \pmod{59}$. Thus, we multiply both sides by 20 to get

$$x \equiv 20 * 7 \equiv 140 \equiv 22 \pmod{59}$$

Thus, the solution is $x \equiv 22 \pmod{59}$, which means that the solutions modulo 236 are 22, 81, 140, and 199.

(b) Note that 4 divides 12 and 236, but not 30. That implies that for any x, $12x$ modulo 236 is divisible by 4. Hence, there are no solutions.

3.4
(a) Use the Euclidean algorithm to compute $\gcd(30030, 257)$.
(b) Using the result of part (a) and the fact that $30030 = 2 * 3 * 5 * 7 * 11 * 13$, show that 257 is prime.

Solution:
(a) Let us apply the Euclidean algorithm:

$$\begin{aligned} 30030 &= 116 * 257 + 218 \\ 257 &= 1 * 218 + 39 \\ 218 &= 5 * 39 + 23 \\ 39 &= 1 * 23 + 16 \\ 23 &= 1 * 16 + 7 \\ 16 &= 2 * 7 + 2 \\ 7 &= 3 * 2 + 1 \\ 2 &= 2 * 1 + 0 \end{aligned}$$

Thus, the gcd is 1.

(b) If 257 is composite, it has a prime divisor that's at most $\sqrt{257} < 17$. Thus, it would have a prime divisor not greater than 13. But 30030 is the product of all the primes not greater than 13, and 257 has no factors in common with it. Hence, 257 is prime.

3.7
(a)Let p be prime. Suppose a and b are integers such that $ab \equiv 0$ (mod p). Show that either $a \equiv 0$ or $b \equiv 0$ (mod p).
(b) Show that if a, b, n are integers with $n|ab$ and $\gcd(a, n) = 1$, then $n|b$.

Solution:
(a) We have that $p|ab$ as $ab \equiv 0$ (mod p). Thus, by the Lemma in the textbook, we have that either $p|a$ or $p|b$. Thus, by definition, $a \equiv 0$ or $b \equiv 0$ (mod p).

(b) Since $\gcd(a, n) = 1$ we can write

$$ax + ny = 1$$

for some integers x and y using the Euclidian algorithm. Thus,

$$abx + nby = b$$

Now, n divides ab by the conditions of the problem, and clearly n divides nby. Thus, n divides the LHS of the above equation, and therefore $n|b$ as required.