Liam Donohoe
RCSID: donohl
RIN: 661634267

Crypto HW2.a

1. A. Prove a = b (mod n) implies b = a (mod n).

First, we start with the assumption that a, and b are both integers, and that a = b (mod n). Assuming both of these are true, then, a - b = k * n for some integer k. Using this equation, we can rewrite it as b - a = (-k) * n, showing that b = a (mod n) as well, proving that a = b (mod n) implies b = a (mod n).

B. Prove a = b (mod n) and b = c (mod n) implies a = c (mod n).

We start by assuming that a, b, and c are integers, and we are also given a = b (mod n) and, b = c (mod n). Similarly to the previous proof, we get the equation a - b = k * n for some k, from the first statement, and we can also obtain b - c = p * n for some p, from the second statement. If we add these statements together, we get the following; a - b + b - c = k * n + p * n. Simplifying this equation, we arrive at; a - c = (k + p) * n. This equation represents a = c (mod n), proving that a = b (mod n) and b = c (mod n) imply a = c (mod n).

2. Multiplicative Inverse using Extended Euclidean Algorithm

a. 1234 mod 4321

Q	Smaller Value	Larger Value	Vector for Small	Vector for Large
3	1234	4321	(1, 0)	(0, 1)
1	619	1234	(0, 1)	(1, -3)
1	615	619	(1, -3)	(-1, 4)
153	4	615	(-1, 4)	(2, -7)
1	3	4	(2, -7)	(-307, 1075)
3	1	3	(-307, 1075)	(309, -1082)
0	0	1	(309, **-1082**)	----------

Multiplicative inverse of 1234 mod 4321 = -1082.

b. 24140 mod 40902

Q	Smaller Value	Larger Value	Vector for Small	Vector for Large
1	24140	40902	(1, 0)	(0, 1)
1	16762	24140	No need to fill	In the rest
2	7378	16762	Of the table.	
3	2006	7378		
1	1360	2006		
2	646	1360		
9	68	646		
2	34	68		
	0	34		

Reduces to 0, and second value is not 1, therefore there is no multiplicative inverse.

c. 550 mod 1769

Q	550	1769	(1, 0)	(0, 1)
3	119	550	(0, 1)	(1, -3)
4	74	119	(1, -3)	(-4, 13)
1	45	74	(-4, 13)	(5, -16)
1	29	45	(5, -16)	(-9, 29)
1	16	29	(-9, 29)	(14, -45)
1	13	16	(14, -45)	(-23, 74)
1	3	13	(-23, 74)	(39, -119)
4	1	3	(37, -119)	(-171, 550)

The multiplicative inverse of 550 mod 1769 = 550.

3. Determine which of the following are reducible over GF(2)
   a. $x^3 + 1 \Rightarrow (x+1)(x^2 + x + 1)$
   b. $x^3 + x^2 + 1 \Rightarrow$ Not Reducible
   c. $x^4 + 1 \Rightarrow (x + 1)^4$

4. Determine the GCD of the following pair of polynomials

a. $x^3 - x + 1$ and $x^2 + 1$ over GF(2) => $x^3 - x + 1$ is not reducible, therefore there is no GCD between the polynomials (besides 1).
   $f(0) = 0 - 0 + 1 = 1$
   $f(1) = 1 - 1 + 1 = 1$
   0 is not obtainable.

b. $x^5 + x^4 + x^3 - x^2 - x + 1$ and $x^3 + x^2 + x + 1$ over GF(3) => Both are reducible
   $f_1(0) = 1$ $f_2(0) = 1$
   $f_1(1) = 1$ $f_2(1) = 1$
   $f_1(2) = 0$ $f_2(2) = 0$
   As both equations are equal to 0 when x = 2, we know we have a solution at x - 2 = 0.
   In GF(3) this is equivalent to x-1, so we can use this to reduce the polynomials.
   $f_1(x) = (x + 1)(x^4 + x^3 + x^2 - x - 1)$
   $f_2(x) = (x + 1)(x^2 + 1)$.
   Therefore, GCD of these equations is (x + 1).

5. This cryptosystem is not valid, so we will use the equation,
$H(K|C) = - \text{Sum}_{(k \text{ in } K,\ c \text{ in } C)} Pr(c) Pr(k|c) \log_2(Pr(k|c))$
$Pr(k|c) = Pr(c|k) Pr(k) / Pr(c)$

$P(1) = ½$
$P(2) = ¼$
$P(3) = ⅛$
$P(4) = ⅛$

$P(1|K_1) = ¾$, $P(2|K_1) = ¼$, $P(3|K_1) = 0$, $P(4|K_1) = 0$
$P(1|K_2) = ½$, $P(2|K_2) = ¼$, $P(3|K_2) = ¼$, $P(4|K_2) = 0$
$P(1|K_3) = 0$, $P(2|K_3) = ¼$, $P(3|K_3) = ¼$, $P(4|K_3) = ½$
$P(1|K_4) = 0$, $P(2|K_4) = 0$, $P(3|K_4) = ¼$, $P(4|K_4) = ¾$

$P(K_1|1) = ¾$, $P(K_1|2) = ½$, $P(K_1|3) = 0$, $P(K_1|4) = 0$,
$P(K_2|1) = ¼$, $P(K_2|2) = ¼$, $P(K_2|3) = ½$, $P(K_2|4) = 0$,
$P(K_3|1) = 0$, $P(K_3|2) = ¼$, $P(K_3|3) = ½$, $P(K_3|4) = 1$,
$P(K_4|1) = 0$, $P(K_4|2) = 0$, $P(K_4|3) = 0$, $P(K_4|4) = 0$.

Now, using the above formula for H(K|C), we get;
$½ * (¾\log_2(¾) + ½\log_2(½)) + (¼ * (½ \log_2(½)) + (¼\log_2(¼)) + (¼ \log_2(¼))) + (⅛ * (½\log_2(½) + (½\log_2(½)) + (⅛ * \log_2 1) =$
$= \mathbf{0.6277}$