Cryptography & Network Security I - Fall 2018

Homework 2 Theory Part A

Charles Schmitter

October 9, 2018

Q1. Prove that:

(a) $a \equiv b(\mathbf{mod} n)$ implies $b \equiv a(\mathbf{mod} n)$.

We begin with assuming $a \equiv b(\mathbf{mod} n)$. This means $a - b$ is a multiple of n. In math terms this is equivalent to: $a - b = c * n$ where c is a constant in the set of all integers. Now, we must prove $b - a$ is a multiple of n to solve the proof. We rearrange $a - b = c * n$ to $b - a = -c * n$, again where $-c$ is in the set of all integers. Therefore, we have proved $b - a$ is a multiple of n, which is equivalent to $b \equiv a(\mathbf{mod} n)$. Thus, our proof has been complete: $a \equiv b(\mathbf{mod} n)$ does in fact imply $b \equiv a(\mathbf{mod} n)$.

(b) $a \equiv b(\mathbf{mod} n)$ and $b \equiv c(\mathbf{mod} n)$ implies $a \equiv c(\mathbf{mod} n)$.

We begin by following some of the logic from part (a) and assume that $a - b$ and $b - c$ are multiples of n. This can be written in mathematical terms as $a - b = x * n$ and $b - c = y * n$ where x and y are both in the set of all integers. For this proof to be completed, we must prove that $a - c$ is a multiple of n. We can substitute in the aforementioned equations into $a - c$ like so: $a - c = (x * n + b) - (b - y * n)$. If we reduce this equation down, we find that $a - c = (x + y) * n$ where $x + y$ is in the set of all integers. Therefore, $a - c$ is a multiple of n, which is equivalent to $a \equiv c(\mathbf{mod} n)$. Thus, we have proven that $a \equiv b(\mathbf{mod} n)$ and $b \equiv c(\mathbf{mod} n)$ implies $a \equiv c(\mathbf{mod} n)$.

Q2. Using extended Euclidean algorithm to find the multiplicative inverse of:

(a) 1234 mod 4321:

Euclidean Algorithm	Solved For Remainders
$4321 = 1234(3) + 619$	$619 = 4321 - 1234(3)$
$1234 = 619(1) + 615$	$615 = 1234 - 619(1)$
$619 = 615(1) + 4$	$4 = 619 - 615(1)$
$615 = 4(153) + 3$	$3 = 615 - 4(153)$
$4 = 3(1) + 1$	$1 = 4 - 3(1)$
$3 = 1(3)$	N/A

Therefore, $gcd(1234, 4321) = 1$. Now, on to the extended Euclidean algorithm. We start with the last equation under the 'Solved for Remainders' column, substitute in $3 = 615 - 4(153)$ for 3 in that equation, and combine like terms. We continue this process until we find the following

equation: $1 = 309(4321) - 1082(1234)$. We can then deduce that the multiplicative inverse is -1082. We can **mod** this by 4321 to retrieve the postiive answer: 3239. This checks out as $1234 * 3239\textbf{mod}4321 \equiv 1$.

(b) 24140 mod 40902:

Euclidean Algorithm
$40902 = 24140(1) + 16762$
$24140 = 16762(1) + 7378$
$16762 = 7378(2) + 2006$
$7378 = 2006(3) + 1360$
$2006 = 1360(1) + 646$
$1360 = 646(2) + 68$
$646 = 68(9) + 34$
$68 = 34(2)$

Since 34 is the GDC, and not 1, no multiplicative inverse exists.

(c) 550 mod 1769:

Euclidean Algorithm	Solved For Remainders
$1769 = 550(3) + 119$	$119 = 1769 - 550(3)$
$550 = 119(4) + 74$	$615 = 1234 - 619(1)$
$119 = 74(1) + 45$	$4 = 619 - 615(1)$
...	...
$16 = 13(1) + 3$	$3 = 16 - 13(1)$
$13 = 3(4) + 1$	$1 = 13 - 3(4)$
$3 = 1(3)$	N/A

Therefore, $gcd(550, 1769) = 1$. Now, on to the extended Euclidean algorithm. We follow the process from before; start with the last equation under the 'Solved for Remainders' column, substitute the second to last equation in, combine like terms, and repeat. We continue this process until we find the following equation: $1 = -27(550) + 8(1769)$. We can then deduce that the multiplicative inverse is -27. We can **mod** this by 1769 to retrieve the postiive answer: 1742. This checks out as $550 * 1742\textbf{mod}1769 \equiv 1$.

Q3. Determine which of the following are reducible over $GF(2)$:

(a) $x^3 + 1$:
$f(0) = 1\%2 = 1$
$f(1) = 2\%2 = 0$
Therefore, (a) is reducible.

(b) $x^3 + x^2 + 1$:
$f(0) = 0 + 0 + 1 = 1\%2 = 1$
$f(1) = 1 + 1 + 1 = 3\%2 = 1$
Therefore, (b) is irreducible.

(c) $x^4 + 1$:
$f(0) = 0 + 1 = 1\%2 = 1$
$f(1) = 1 + 1 = 2\%2 = 0$
Therefore, (c) is reducible.

Q4. Determine the GCD of the polynomials:

(a) $x^3 - x + 1$ and $x^2 + 1$ over $GF(2)$

We will denote the first function as $f(x)$ and the second as $g(x)$.

x	$f(x)$
0	1
1	1

x	$g(x)$
0	1
1	$2\%2 = 0$

We can see that $f(x)$ has no roots, and thus no factors, meaning the GCD between these two polynomials is 1.

(b) $x^5 + x^4 + x^3 - x^2 - x + 1$ and $x^3 + x^2 + x + 1$ over $GF(3)$

We will denote the first function as $f(x)$ and the second as $g(x)$.

x	$f(x)$
0	1
1	2
2	$51\%3 = 0$

x	$g(x)$
0	1
1	$4\%3 = 1$
2	$15\%3 = 0$

We can see that $f(x)$ and $g(x)$ share the root $x = 2$, so they have a common factor of $x - 2$. Converted to the finite field $GF(3)$ gives us the factor $x + 1$. The GCD of these two polynomials over $GF(3)$ is $x + 1$.

Q5. Find $H(K|C)$ of the cryptosystem:

First, we find the probabilities of each ciphertext ($Pr(C)$). Then we can compute the probabilities of each ciphertext given a key ($Pr(C|K)$). Then, we can compute the probabilities of each key given a ciphertext ($Pr(K|C)$). Finally, we can compute entropy as the negation of the summation of $Pr(C) * Pr(K|C) * log_2(Pr(K|C))$. This comes out to be:

$$\begin{gathered}\tfrac{1}{2} * (\tfrac{3}{4} log_2(\tfrac{3}{4}) + \tfrac{1}{4} log_2(\tfrac{1}{4})) \\ + \tfrac{1}{4} * (\tfrac{1}{2} log_2(\tfrac{1}{2}) + \tfrac{1}{4} log_2(\tfrac{1}{4}) + \tfrac{1}{4} log_2(\tfrac{1}{4})) \\ + \tfrac{1}{8} * (\tfrac{1}{2} log_2(\tfrac{1}{2}) + \tfrac{1}{2} log_2(\tfrac{1}{2})) \\ = -0.4055 - 0.375 - 0.125 = -0.9055\end{gathered}$$

By applying the final negation, we receive our final answer: 0.9055.