Cryptography and Network Security Homework 2a

Jacques Becker

October 9, 2018

Problem 1a: Prove that $a \equiv b (\text{mod } n)$ implies $b \equiv a (\text{mod } n)$

Assume $a \equiv b (\text{mod } n)$ is true. From the definition of modular congruence, we know that n divides the difference between a and b, so $n|(a-b)$. Since n divides $(a-b)$, it follows that n must also divide every integer multiple of $(a-b)$, so therefore $n|k(a-b)$, where $k \in \mathbb{Z}$. Suppose $k = -1$. We have that $n|-1(a-b)$, which is equivalent to $n|(b-a)$. This is the definition for modular congruence of b and a, so it must therefore be true that $b \equiv a (\text{mod } n)$.

Problem 2a: Prove that $a \equiv b (\text{mod } n)$ and $b \equiv c (\text{mod } n)$ imply $a \equiv c (\text{mod } n)$.

Suppose that $a \equiv b (\text{mod } n)$ and $b \equiv c (\text{mod } n)$. From the definition of modular congruence, we know that $(a-b)$ is a multiple of n, and $(b-c)$ is a multiple of n. So, $a - b = kn$ and $b - c = rn$, where $k, r \in \mathbb{Z}$. Adding these equations together, we get $(a-b)+(b-c) = kn + rn$, which simplifies to $a - c = n(k+r)$. From this, we see that $a - c$ is an integer multiple of n, so it must be true that $a \equiv c (\text{mod } n)$.

Problem 2a: Using the Extended Euclidean Algorithm, find the multiplicative inverse of 1234 mod 4321.

$$\begin{aligned}
4321 &= 3(1234) + 619 \\
1234 &= 1(619) + 615 \\
619 &= 1(615) + 4 \\
615 &= 153(4) + 3 \\
4 &= 1(3) + 1 \\
3 &= 3(1) + 0
\end{aligned}$$

So, the greatest common divisor of 1234 and 4321 is 1. The multiplicative inverse of 1234 must therefore exist.

$$\begin{aligned}
1 &= 4 - 3 \\
1 &= 4 - (615 - 153(4)) \\
1 &= 154(4) - 615 \\
1 &= 154(619 - 615) - 615 \\
1 &= 154(619) - 154(615) - 615 \\
1 &= 154(619) - 155(615) \\
1 &= 1 = 154(619) - 155(1234 - 619) \\
1 &= 154(619) - 155(1234) + 155(619) \\
1 &= 309(619) - 155(1234) \\
1 &= 309(4321 - 3(1234)) - 155(1234) \\
1 &= 309(4321) - 927(1234) - 155(1234) \\
1 &= 309(4321) - 1082(1234) \\
-309(4321) + 1 &= -1082(1234)
\end{aligned}$$

From this, we see that $-1082(1234)$ is equal to a multiple of 4321 plus one, so $x = -1082$ satisfies $1234x \equiv 1(\text{mod } 4321)$. Therefore, -1082 is the multiplicative inverse of 1234 mod 4321.

Problem 2b: Using the Extended Euclidean Algorithm, find the multiplicative inverse of 24140 mod 40902.

$$\begin{aligned}
40902 &= 1(24140) + 16762 \\
24140 &= 1(16762) + 7378 \\
16762 &= 2(7378) + 2006 \\
7378 &= 3(2006) + 1360 \\
2006 &= 1(1360) + 646 \\
1360 &= 2(646) + 68 \\
646 &= 9(68) + 34 \\
68 &= 2(34) + 0
\end{aligned}$$

Because 40902 and 24140 have a GCD 34, 24140 has no multiplicative inverse mod 40902.

Problem 2a: Using the Extended Euclidean Algorithm, find the multiplicative inverse of 550 mod 1769.

$$
\begin{aligned}
1796 &= 3(550) + 119 \\
550 &= 4(119) + 74 \\
119 &= 1(74) + 45 \\
74 &= 1(45) + 29 \\
45 &= 1(29) + 13 \\
16 &= 1(13) + 3 \\
13 &= 4(3) + 1 \\
3 &= 3(1) + 0
\end{aligned}
$$

The greatest common divisor of 1769 and 550 is 1, so the multiplicative inverse of 550 mod 1769 must exist.

$$
\begin{aligned}
1 &= 13 - 4(3) \\
1 &= 13 - 4(16 - 13) \\
1 &= 5(13) - 4(16) \\
1 &= 5(29 - 16) - 4(16) \\
1 &= 5(29) - 9(16) \\
1 &= 5(29) - 9(45 - 29) \\
1 &= 14(29) - 9(45) \\
1 &= 14(74 - 45) - 9(45) \\
1 &= 14(74) - 23(45) \\
1 &= 14(74) - 23(119 - 74) \\
1 &= 37(74) - 23(119) \\
1 &= 37(550 - 4(119)) - 23(119) \\
1 &= 37(550) - 171(119) \\
1 &= 37(550) - 171(1769 - 3(550)) \\
1 &= 550(550) - 171(1769) \\
171(1769) + 1 &= 550(550)
\end{aligned}
$$

Because 550(550) is equal to a multiple of 1769 plus one, we know that $x = 550$ satisfies $550x \equiv 1(\text{mod } 1769)$. Therefore, 550 is the multiplicative inverse of 550 mod 1796.

Problem 3: Determine which of the following are reducible over GF(2):
a. $x^3 + 1$
b. $x^3 + x^2 + 1$
c. $x^4 + 1$

$x^3 + 1$ is reducible over GF(2) because $x^3 + 1 = (x + 1)(x^2 + x + 1)(\text{mod } 2)$.
$x^3 + x^2 + 1$ is not reducible over GF(2).
$x^4 + 1$ is reducible over GF(2) because $x^4 + 1 = (x + 1)^4(\text{mod } 2)$.

Polynomials **a** and **c** are reducible over GF(2).

Problem 4: Determine the GCD of the following pair of polynomials:
a. $x^3 - x + 1$ and $x^2 + 1$ over GF(2)
b. $x^5 + x^4 + x^3 - x^2 - x + 1$ and $x^3 + x^2 + x + 1$ over GF(3)

a. $\text{GCD}(x^3 - x + 1, x^2 + 1) = 1$
b. $\text{GCD}(x^5 + x^4 + x^3 - x^2 - x + 1, x^3 + x^2 + x + 1) = (x + 1)$

Problem 5: For a cryptosystem P,K,C,E,D where:
P = {a, b, c} with:
PP(a) = 1/4
PP(b) = 1/4
PP(c) = 1/2

K = {K1, K2, K3} with:
PK(K1) = 1/2
PK(K2) = 1/4
PK(K3) = 1/4

C = {1, 2, 3, 4}

$$\begin{array}{lll} e_{k_1}(a) = 1 & e_{k_1}(b) = 2 & e_{k_1}(c) = 1 \\ e_{k_2}(a) = 2 & e_{k_2}(b) = 3 & e_{k_2}(c) = 1 \\ e_{k_3}(a) = 3 & e_{k_3}(b) = 2 & e_{k_3}(c) = 4 \end{array}$$

We know that $H(K|C) = -\sum_{k\in K, c\in C} p(c)p(k|c)\log_2 p(k|c)$. In order to compute this, we first need to compute the values of $p(c)$ for all $c \in C$ and the value of $p(k|c)$ for all key/ciphertext pairs. Begin by finding the values of $p(c)$:

$$p(1) = P_k(k_1) \cdot P_p(a) + P_k(k_1) \cdot P_p(c) + P_k(k_2) \cdot P_p(c) = \frac{1}{2} \cdot \frac{1}{4} + \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{2}$$
$$p(2) = P_k(k_1) \cdot P_p(b) + P_k(k_2) \cdot P_p(a) + P_k(k_3) \cdot P_p(a) = \frac{1}{2} \cdot \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{4} = \frac{1}{4}$$
$$p(3) = P_k(k_2) \cdot P_p(b) + P_k(k_3) \cdot P_p(a) = \frac{1}{4} \cdot \frac{1}{4} + \frac{1}{4} \cdot \frac{1}{4} = \frac{1}{8}$$
$$p(4) = P_k(k_3) \cdot P_p(c) = \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8}$$

Now that we have values for all $p(c)$, the values of all $p(k|c)$ must be computed. By Bayes' rule, $p(k|c) = p(c|k)\frac{p(k)}{p(c)}$, where $p(c|k) = \sum_{\{x|e_k(x)=c\}} P_p(x)$:

$$
\begin{aligned}
p(k_1|1) &= p(1|k_1)\frac{p(k_1)}{p(1)} = \left(\frac{1}{4}+\frac{1}{2}\right)\frac{1/2}{1/2} = \frac{3}{4} \\
p(k_1|2) &= p(2|k_1)\frac{p(k_1)}{p(2)} = \frac{1}{4}\cdot\frac{1/4}{1/4} = \frac{1}{2} \\
p(k_1|3) &= p(3|k_1)\frac{p(k_1)}{p(3)} = 0 \\
p(k_1|4) &= p(4|k_1)\frac{p(k_1)}{p(4)} = 0 \\
p(k_2|1) &= p(1|k_2)\frac{p(k_2)}{p(1)} = \frac{1}{2}\cdot\frac{1/4}{1/2} = \frac{1}{4} \\
p(k_2|2) &= p(2|k_2)\frac{p(k_2)}{p(2)} = \frac{1}{4}\cdot\frac{1/4}{1/4} = \frac{1}{4} \\
p(k_2|3) &= p(3|k_2)\frac{p(k_2)}{p(3)} = \frac{1}{4}\cdot\frac{1/4}{1/8} = \frac{1}{2} \\
p(k_2|4) &= p(4|k_2)\frac{p(k_2)}{p(4)} = 0 \\
p(k_3|1) &= p(1|k_3)\frac{p(k_3)}{p(1)} = 0 \\
p(k_3|2) &= p(2|k_3)\frac{p(k_3)}{p(2)} = \frac{1}{4}\cdot\frac{1/4}{1/4} = \frac{1}{4} \\
p(k_3|3) &= p(3|k_3)\frac{p(k_3)}{p(3)} = \frac{1}{4}\cdot\frac{1/4}{1/8} = \frac{1}{2} \\
p(k_3|4) &= p(4|k_4)\frac{p(k_4)}{p(4)} = \frac{1}{4}\cdot\frac{1/4}{1/8} = \frac{1}{2}
\end{aligned}
$$

Now, we can use these values to compute the conditional entropy $H(K|C)$:

$$
H(K|C) = -\sum_{i=1}^{3}\sum_{j=1}^{4} p(c_j)p(k_i|c_j)\log_2 p(k_i|c_j)
$$

$$
\begin{aligned}
H(K|C) =& [\frac{1}{2}\left(\frac{3}{4}\log_2\frac{3}{4}+\frac{1}{2}\log_2\frac{1}{2}\right)+ \\
& \frac{1}{4}\left(\frac{1}{4}\log_2\frac{1}{4}+\frac{1}{4}\log_2\frac{1}{4}+\frac{1}{2}\log_2\frac{1}{2}\right)+ \\
& \frac{1}{8}\left(\frac{1}{4}\log_2\frac{1}{4}+\frac{1}{2}\log_2\frac{1}{2}+\frac{1}{2}\log_2\frac{1}{2}\right)] \\
H(K|C) \approx& -[0.5(-0.811)+0.25(-1.5)+0.125(-1.5)] \\
H(K|C) \approx& 0.968
\end{aligned}
$$