Homework 2 Solutions

- **Group Members: Yu Wang(wangy52 661834351)**
- **Collaborators: no**

Problem 1

(a)

If $a \equiv b \mod n$, then $\exists t \in \mathcal{Z}$ ($\mathcal{Z}$ is a set containing all integer numbers) such that $a = t \cdot n + b$.
We now have $b - t \cdot n = a$ which means $(b - t \cdot n) \mod n = b \mod n = a \mod n$, that is $b \equiv a \mod n$

(b)

If $a \equiv b \mod n$ and $b \equiv c \mod n$ then $\exists t, k \in \mathcal{Z}$ such that

$$\begin{aligned} a + tn &= b \\ c + kn &= b. \end{aligned} \tag{1-1}$$

Then

$$\begin{aligned} &a + tn = c + kn \\ \Rightarrow &a = c + (k - t)n \\ \Leftrightarrow &a \equiv c \mod n. \end{aligned} \tag{1-2}$$

Problem 2

(a)

4321	1234	Q	(1,0)	(0,1)
4321- 3*1234=619	1234	3	(1,0)-3*(0,1)=(1,-3)	(0,1)
619	1234-1*619=615	1	(1,-3)	(0,1)-1*(1,-3)=(-1,4)
619-1*615=4	615	1	(1,-3)-1*(-1,4)=(2,-7)	(-1,4)
4	615-153*4=3	153	(2,-7)	(-1,4)-153*(2,-7)=(-307,1075)
4-1*3=1	3	1	(2,-7)-(-307,1075)=(309,-1082)	(-307,1075)

We now have

$$1 = 309 * 4321 - 1082 * 1234. \tag{2-1}$$

Apply module 4321 to both side, we have

$$1 = \underbrace{-1082}_{1234^{-1}} * 1234 \mod 4321. \tag{2-2}$$

So

$$1234^{-1} \mod 4321 = -1082 \mod 4321 = \boxed{3239} \mod 4321. \tag{2-3}$$

(b)

40902	24140	Q	(1, 0)	(0, 1)
16762	24140	1	(1, -1)	(0, 1)
16762	7378	1	(1, -1)	(-1,2)
2006	7378	2	(3,-5)	(-1,2)
2006	1360	3	(3,-5)	(-10,17)
646	1360	1	(13,-22)	(-10,17)
646	68	2	(13,-22)	(-36,61)
34	68	9	(337,-571)	(-36,61)
34	0	2	(337,-571)	(-710,1203)

We see reminder to be 0, which means 24150 is $\boxed{\text{NOT multiplicative inversable in GF(40902)}}$.

(c)

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

We have

$$1 = -171 * 1769 + 550 * 550 \mod 1769 = 550 * 550 \mod 1769 \tag{2-4}$$

So, $550^{-1} \mod 1769 = \boxed{550} \mod 1769$.

Problem 3

(a)

Let $f(x) = x^3 + 1$.

$f(1) = 1 + 1 = 0$, which means $x + 1$ is one of the factor of $f(x)$. Apply the polynomial division, $x^3 + 1 = (x + 1)(x^2 + x + 1)$. So $f(x) = x^3 + 1$ is $\boxed{\text{NOT}}$ an irreducible polynomial over GF(2).

(b)

Let $f(x) = x^3 + x^2 + 1$.

$f(1) = 1 + 1 + 1 = 1 \neq 0$ and $f(0) = 0 + 0 + 1 \neq 0$, so $f(x) = x^3 + x^2 + 1$ $\boxed{\text{IS}}$ an irreducible polynomial.

(c)

Let $f(x) = x^4 + 1$.

Because $f(1) = 1 + 1 = 0$, $x + 1$ is one of the factor of $f(x)$. Apply the polynormial division, $x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1)$. So $f(x) = x^4 + 1$ is $\boxed{\text{NOT}}$ an irreducible polynormial over GF(2).

Problem 4

(a)

In GF(2), $x^3 - x + 1 = x^3 + x + 1$.
Apply $GCD(a, b) = GCD(\mod (a, b), b)$.

$$(x^3 + x + 1)/(x^2 + 1) = x \cdots 1, \tag{4-1}$$

so $GCD(x^3 + x + 1, x^2 + 1) = GCD(1, x^2 + 1) = \boxed{1}$

(b)

If GF(3), $x^5 + x^4 + x^3 - x^2 - x + 1 = x^5 + x^4 + x^3 + 2x^2 + 2x + 1$.

$$(x^5 + x^4 + x^3 + 2x^2 + 2x + 1)/(x^3 + x^2 + x + 1) = x^2 \cdots x^2 + 2x + 1, \tag{4-2}$$

so $GCD(x^5 + x^4 + x^3 + 2x^2 + 2x + 1, x^3 + x^2 + x + 1) = GCD(x^2 + 2x + 1, x^3 + x^2 + x + 1)$.

$$(x^3 + x^2 + x + 1)/(x^2 + 2x + 1) = x + 2 \cdots 2x + 2, \tag{4-3}$$

so $GCD(x^2 + 2x + 1, x^3 + x^2 + x + 1) = GCD(x^2 + 2x + 1, 2x + 2)$.

$$(x^2 + 2x + 1)/(2x + 2) = 2x + 2 \cdots 0, \tag{4-4}$$

so $GCD(x^5 + x^4 + x^3 + 2x^2 + 2x + 1, x^3 + x^2 + x + 1) = \boxed{\text{2x + 2}}$.

Problem 5

The formula for conditional entropy is

$$H(K|C) = \sum_k \sum_c p(k, c) \log \frac{p(c)}{p(k, c)}. \tag{5-1}$$

Our task turns to compute $p(c)$ and $p(k, c)$.

1. $p(c)$

$$\begin{aligned}
Pr(C = 1) =& Pr(P = a, K = k1) + Pr(P = c, K = k1) + Pr(P = c, K = k2) \\
=& 1/4 * 1/2 + 1/2 * 1/2 + 1/2 * 1/4 = 1/2 \\
Pr(C = 2) =& Pr(P = b, K = k1) + Pr(P = a, K = k2) + Pr(P = b, K = k3) \\
=& 1/4 * 1/2 + 1/4 * 1/4 + 1/4 * 1/4 = 1/4 \\
Pr(C = 3) =& Pr(P = b, K = k2) + Pr(P = a, K = k3) + Pr(P = a, K = k4) \\
=& 1/4 * 1/4 + 1/4 * 1/4 + 1/4 * 0 = 1/8 \\
Pr(C = 4) =& Pr(P = c, K = k3) + Pr(P = b, K = k4) + Pr(P = c, K = k4) \\
=& 1/2 * 1/4 + 1/4 * 0 + 1/2 * 0 = 1/8
\end{aligned}$$

2. $p(k, c)$

$$
\begin{aligned}
&Pr(K = k1, C = 1) = Pr(K = k1, P = a) + Pr(K = k1, P = c) = 1/2 * 1/4 + 1/2 * 1/2 = 3/8 \\
&Pr(K = k1, C = 2) = Pr(K = k1, P = b) = 1/2 * 1/4 = 1/8 \\
&Pr(K = k1, C = 3) = Pr(K = k1, C = 4) = 0 \\
&Pr(K = k2, C = 1) = Pr(K = k2, P = c) = 1/4 * 1/2 = 1/8 \\
&Pr(K = k2, C = 2) = Pr(K = k2, P = a) = 1/4 * 1/4 = 1/16 \\
&Pr(K = k2, C = 3) = Pr(K = k2, P = b) = 1/4 * 1/4 = 1/16 \\
&Pr(K = k2, C = 4) = 0 \\
&Pr(K = k3, C = 1) = 0 \\
&Pr(K = k3, C = 2) = Pr(K = k3, P = b) = 1/4 * 1/4 = 1/16 \\
&Pr(K = k3, C = 3) = Pr(K = k3, P = a) = 1/4 * 1/4 = 1/16 \\
&Pr(K = K3, C = 4) = Pr(K = k3, P = c) = 1/4 * 1/2 = 1/8 \\
&Pr(K = K4, C = 1) = Pr(K = k4, C = 2) = Pr(K = k4, C = 3) = Pr(K = k4, C = 4) = 0
\end{aligned}
$$

Now we have all the building blocks to compute the conditional entropy.

$$
\begin{aligned}
H(K|C) = &\sum_k \sum_c p(k, c) \log \frac{p(c)}{p(k, c)} \\
=&3/8 \log \frac{1/2}{3/8} + 1/8 \log \frac{1/4}{1/8} + 1/8 \log \frac{1/2}{1/8} + 1/16 \log \frac{1/4}{1/16} \\
&+ 1/16 \log \frac{1/8}{1/16} + 1/16 \log \frac{1/4}{1/16} + 1/16 \log \frac{1/8}{1/16} + 1/8 \log \frac{1/8}{1/8} \\
=&\boxed{0.9056}
\end{aligned}
\tag{5-2}
$$