Cryptography HW 2

1. Prove

    1.

$$
\begin{array}{l}
a \equiv b \mod n \to b \equiv a \mod n \\
\text{Assume } a \equiv b \mod n, \text{ then show } b \equiv a \mod n \\
\text{By definition, } \exists e \in \mathbb{Z} \text{ s.t. } a = e \cdot n + b \\
b = -e \cdot n + a \\
\therefore \text{By definition of mod, } b \equiv a \mod n.
\end{array}
$$

    2.

$$
\begin{array}{l}
a \equiv b \mod n \wedge b \equiv c \mod n \to a \equiv c \mod n \\
\text{Assume } a \equiv b \mod n \wedge b \equiv c \mod n, \text{then show } a \equiv c \mod n \\
\text{By definition of modulus, } a \cdot i + b = n, b \cdot j + c = n \\
\text{We must find } k \text{ s.t. } a \cdot k + c = n \\
b = \dfrac{n-c}{j} \\
a \cdot i + \dfrac{n-c}{j} = n \\
a \cdot ij + n - c = nj \\
n \equiv 0 \mod n. \text{ Therefore we can exclude it from our formula.} \\
\Rightarrow ak + c = n \\
\therefore a \equiv c \mod n.
\end{array}
$$

2. Using extended Euclidean algorithm find the multiplicative inverse of:

    1.

$$
\begin{gathered}
1234 \cdot a^{-1} \equiv 1 \mod 4321 \\
1 = 1234x + 4321y \\
1234x + 4321y \equiv 1 \mod 4321 \\
1234x \equiv 1 \mod 4321 \\
4321 = 3(1234) + 619 \\
1234 = 1(619) + 615 \\
619 = 1(615) + 4 \\
615 = 153(4) + 3 \\
4 = 1(3) + 1 \\
3 = 3(1) + 0 \\
1 = 4 - 3 \\
4 = 619 - 615 \\
619 = 4321 - 3(1234) \\
615 = 1234 - 619 \Rightarrow (-1)(4321) + (4)(1234) \\
4 = (4321 - 3(1234)) - ((-1)(4321) + (4)(1234)) \Rightarrow 4 = (2)(4321) + (-7)(1234) \\
3 = 615 - 153(4) \Rightarrow 3 = (4(1234) + (-1)(4321)) + (-153)(2(4321) + (-7)(1234)) \\
3 = (1075)(1234) + (-307)(4321) \\
1 = (2(4321) + (-7)(1234)) - (1075(1234) + (-307)(4321)) \Rightarrow 1 = (-1082)(1234) + (309)(4321) \\
\Rightarrow x = -1082.
\end{gathered}
$$

    2. The multiplicative inverse does not exist, as 24140 and 40902 are not co-prime.

$$
24140 \cdot a^{-1} \equiv 1 \mod 40902
$$

    3.

$$550 \cdot a^{-1} \equiv 1 \mod 1769$$
$$a^{-1} = 550$$

3. Determine which of the following are reducible over GF(2) 1.

$$x^3 + 1 \equiv (x+1)(x^2+x+1) = x^3 + 2x^2 + 2x + 1 \equiv x^3 + 1 \mod 2$$

   2. Irreducible:

$$x^3 + x^2 + 1$$

   3.

$$x^4 + 1 \equiv (x^2+1)(x^2+1) = x^4 + 2x^2 + 1 \equiv x^4 + 1 \mod 2$$

4. Determine the GCD of the following pair of polynomials:

   1.

$$x^3 - x + 1 \text{ and } x^2 + 1 \text{ over } GF(2)$$
$$x^2 + 1 = (x+1)^2$$

   The greatest common divisor is $x + 1$.

   2.

$$x^5 + x^4 + x^3 - x^2 - x + 1 \text{ and } x^3 + x^2 + x + 1 \text{ over } GF(3)$$

5. Crypto-system:

$$H(K|C) = H(K) + H(P) - H(C)$$
$$H(X) = -\sum_{i=1}^{n} p(X = x_i) \log_2 p(X = x_i)$$
$$H(K) = -(\frac{1}{4}log_2(\frac{1}{4}) + \frac{1}{4}log_2(\frac{1}{4}) + \frac{1}{2}log_2(\frac{1}{2})) = \frac{3}{2}$$
$$H(P) = -(\frac{1}{4}log_2(\frac{1}{4}) + \frac{1}{4}log_2(\frac{1}{4}) + \frac{1}{2}log_2(\frac{1}{2})) = \frac{3}{2}$$
$$p(1) = \sum_{k \in K} p(1|k)p(k) = (\frac{2}{3})(\frac{1}{2}) + (\frac{1}{3})(\frac{1}{4}) = \frac{5}{12}$$
$$p(2) = (\frac{1}{3})(\frac{1}{2}) + (\frac{1}{3})(\frac{1}{4}) + (\frac{1}{3})(\frac{1}{4}) = \frac{1}{3}$$
$$p(3) = (\frac{1}{3})(\frac{1}{4}) + (\frac{1}{3})(\frac{1}{4}) = \frac{1}{6}$$
$$H(C) = -((\frac{5}{12}\log_2(\frac{5}{12})) + \frac{1}{3}\log_2(\frac{1}{3}) + \frac{1}{6}\log_2(\frac{1}{6})) \approx 1.485$$
$$\therefore H(K|C) = 2 \cdot \frac{3}{2} - 1.485 = 1.515$$