CSCI 4100 Homework 4

Colin Goldberg

October 10, 2018

1. Prove that

   (a) $a \equiv b(\mod n)$ implies $b \equiv a(\mod n)$

   $$\begin{aligned} a &\equiv b(\mod n) \\ a - b &= kn \\ bla &= (-k)n \\ b &\equiv a(\mod n) \end{aligned}$$

   (b) $a \equiv b(\mod n)$ and $b \equiv c(\mod n)$ implies $a \equiv c(\mod n)$

   $$\begin{aligned} a &\equiv b(\mod n) \\ a - b &= kn \\ b &\equiv c(\mod n) \\ b - c &= jn \\ (a-b) + (b-c) &= kn + jn \\ a - c &= (k+j)n \\ a &\equiv c(\mod n) \end{aligned}$$

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

   (a) 1234 mod 4321

   (b) 24140 mod 40902

   (c) 550 mod 1769

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

   (a) $x^3 + 1$
   Reducible into $(x+1)(x^2+x+1)$

   (b) $x^3 + x^2 + 1$
   Not Reducible

(c) $x^4 + 1$
Reducible into $(x+1)^4$

4. Determine the GCD of the following polynomials:

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

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

5. Calculate $H(K|C)$

$$H(K) = -\sum_{k\in K} Pr(k)\log_2(Pr(k)) = -(-\frac{1}{2} - \frac{1}{2} - \frac{1}{2}) = \frac{3}{2}$$

$$H(P) = -\sum_{p\in P} Pr(p)\log_2(Pr(p)) = \frac{3}{2}$$

$$\begin{aligned}
Pr(1) &= Pr(a)Pr(k1) + Pr(c)Pr(k1) + Pr(c)Pr(k2) \\
&= \frac{1}{4}\frac{1}{2} + \frac{1}{2}\frac{1}{2} + \frac{1}{2}\frac{1}{4} = \frac{1}{2} \\
Pr(2) &= Pr(b)Pr(k1) + Pr(a)Pr(k2) + Pr(b)Pr(k3) \\
&= \frac{1}{4}\frac{1}{2} + \frac{1}{4}\frac{1}{4} + \frac{1}{4}\frac{1}{4} = \frac{1}{4} \\
Pr(3) &= Pr(b)Pr(k2) + Pr(a)Pr(k3) + Pr(a)Pr(k4) \\
&= \frac{1}{4}\frac{1}{4} + \frac{1}{4}\frac{1}{4} = \frac{1}{8} \\
Pr(4) &= Pr(c)Pr(k3) \\
&= \frac{1}{2}\frac{1}{4} \\
&= \frac{1}{8}
\end{aligned}$$

$$H(C) = -\sum_{c\in C} Pr(c)\log_2(Pr(c)) = -(-\frac{1}{2} - \frac{1}{2} - \frac{3}{8} - \frac{3}{8}) = \frac{7}{4}$$

$$H(K|C) = H(K) + H(P) - H(C) = \frac{3}{2} + \frac{3}{2} - \frac{7}{4} = \frac{5}{4} = 1.25$$