HW 2.1

Tuesday, October 9, 2018 9:39 AM

1.

   a. Assume that a ≡ b mod n
      i. a ≡ b mod n is true if and only if a-b is evenly devisible by n
      ii. For all integers, - (a - b) = (b - a) by algebra
      iii. It is also true that if (a - b) is evenly divisible by n then - (a - b) must also be evenly divisibly by n
      iv. (b - a) must be evenly divisible by n
      v. Thus b ≡ a mod n
      vi. QED

   b. Assume that a ≡ b mod n and b ≡ c mod n
      i. a ≡ b mod n is true if and only if a-b is evenly devisible by n
      ii. b ≡ c mod n is true if and only if b-c is evenly devisible by n
      iii. If (a - b) is evenly divisible by n then (a - b) = k(n) for some integer k
      iv. If (b - c) is evenly divisible by n then (b - c) = j(n) for some integer j
      v. k(n) + j(n) = (k + j)n = [(a - b) + (b - c)]n = (a - c)n
      vi. This (a - c) is evenly divisible by n
      vii. Thus a ≡ c mod n
      viii. QED

2. Finding multiplicative inverses
   a. 1234 mod 4321
      i. 4321 = (1234) 3 + 619
      ii. 1234 = (619) 1 + 615
      iii. 619 = (615) 1 + 4
      iv. 615 = (4) 153 + 3
      v. 4 = 3 + 1

      vi. 1 = 4 - 3 by using step v
      vii. 1 = 4 - (615 - (4) 153) by substituting step iv
         1) 1 = 4 - 615 + (4)153
         2) 1 = 4 + (4)153 - 615
         3) 1 = (4)154 - 615
      viii. 1 = (619 - 615)154 - 615 by substituting step iii
         1) 1 = ((619)154 - (615)154) - 615
         2) 1 = (619)154 - (615)154 - (615)1
         3) 1 = (619)154 - (615)155
      ix. 1 = (619)154 - ((1234 - (619)1)155 by substituting step ii
         1) 1 = (619)154 - (1234)155 + (619)155
         2) 1 = (619)154 + (619)155 - (1234)155
         3) 1 = (619)309 - (1234)155
      x. 1 = ((4321 - (1234)3)309 - (1234)155 by substituting step i
         1) 1 = (4321)309 - (1234)927 - (1234)155
      xi. 1 = (4321)309 - (1234)1082

   b. 24140 mod 40902
      i. 40902 = (24140) 1 + 16762

ii. 24140 = (16762) 1 + 7378
iii. 16762 = (7378) 2 + 2006
iv. 7378 = (2006) 3 + 1360
v. 2006 = (1360) 1 + 646
vi. 1360 = (646) 2 + 68
vii. 646 = (68) 9 + 34
viii. 68 = (34) 2 + 0

ix. The gcd is not 0, thus there is not an inverse

c. 550 mod 1769
   i. 1769 = (550) 3 + 119
   ii. 550 = (119) 4 + 74
   iii. 119 = (74)1 + 45
   iv. 74 = (45)1 + 29
   v. 45 = (29)1 + 16
   vi. 29 = (16)1 + 13
   vii. 16 = (13)1 + 3
   viii. 13 = (3) 4 + 1

   ix. 1 = 13 - (3)4 by using step viii
   x. 1 = 13 - ((16)1 - (13)1) by substituting step vii
      1) 1 = (13)1 - (16)1 + (13)1
      2) 1 = (13)1 + (13)1 - (16)1
      3) 1 = (13)2 - (16)1
   xi. 1 = ((29)1 - (16)1)2 - 16 by substituting step vi
      1) 1 = ((29)1 - (16)1)2 - 16
      2) 1 = (29)2 - (16)2 - (16)1
      3) 1 = (29)2 - (16)3
   xii. 1 = (29)2 - ((45)1 - (29)1)3 by substituting step v
      1) 1 = (29)2 - ((45)3 - (29)3)
      2) 1 = (29)2 - (45)3 + (29)3
      3) 1 = (29)2 + (29)3 - (45)3
      4) 1 = (29)5 - (45)3
   xiii. 1 = ((74)1 - (45)1)5 - (45)3 by substituting step iv
      1) 1 = (74)5 - (45)5 - (45)3
      2) 1 = (74)5 - (45)8
   xiv. 1 = (74)5 - ((119)1 - (74)1)8 by substituting step iii
      1) 1 = (74)5 - ((119)8 - (74)8)
      2) 1 = (74)5 - (119)8 + (74)8
      3) 1 = (74)5 + (74)8 - (119)8
      4) 1 = (74)13 - (119)8
   xv. 1 = ((550)1 - (119)4)13 - (119)8 by substituting step ii
      1) 1 = (550)13 - (119)52 - (119)8
      2) 1 = (550)13 - (119)60
   xvi. 1 = (550)13 - ((1769)1 - (550)3)60 by substituting step i
      1) 1 = (550)13 - ((1769)60 - (550)180)
      2) 1 = (550)13 - (1769)60 + (550)180
      3) 1 = (550)13 + (550)180 - (1769)60
   xvii. 1 = (550)193 - (1769)60

3. Reducibility
   a. $x^3 + 1$ is reducible by $x + 1$ because $x^3 + 1 / x + 1 = x^2 + x + 1$

b. $x^3 + x^2 + 1$ is irreducible
c. $x^4 + 1$ is reducible by $x + 1$ because $x^4 + 1 / x + 1 = x^3 + x^2 + x + 1$

4. Polynomial gcd
   a. $Gcd(x^3 - x + 1, x^2 + 1)$
      i. $x^3 - x + 1 = (x^2 + 1)x + 1$
      ii. $(x^2 + 1) = (1)(x^2 + 1) + 0$
      iii. Thus gcd is 1

   b. $Gcd(x^5 + x^4 + x^3 - x^2 - x + 1, x^3 + x^2 + x^1 + 1)$
      i. $x^5 + x^4 + x^3 - x^2 - x + 1 = (x^3 + x^2 + x^1 + 1)x^2 + (-x + 1)$
      ii. $(x^3 + x^2 + x^1 + 1) = (-x + 1)x^2 + (x + 1)$
      iii. $(-x + 1) = (x + 1) + x$
      iv. $(x + 1) = (x) + 1$
      v. $x = (1)x + 0$
      vi. Thus gcd is 1

5. $H(K|C) = H(K) + H(P) - H(C) = 1.5 + 1.5 - 1.75 = 1.25$
   a. $H(K) = -((1/2)\log_2(1/2) + (1/4)\log_2(1/4) + (1/4)\log_2(1/4))$
      i. $-((1/2)(-1) + (1/4)(-2) + (1/4)(-2))$
      ii. $-(-(1/2) - (2/4) - (2/4)) = 1.5$
   b. $H(P) = -((1/4)\log_2(1/4) + (1/4)\log_2(1/4) + (1/2)\log_2(1/2))$
      i. $-((1/4)(-2)) + (1/4)(-2) + (1/2)(-1))$
      ii. $-(-(2/4) - (2/4) - (1/2)) = 1.5$
   c. $H(C) = -((1/2)\log_2(1/2) + (1/4)\log_2(1/4) + (1/8)\log_2(1/8) + (1/8)\log_2(1/8))$
      i. $-((1/2)(-1) + (1/4)(-2) + (1/8)(-3) + (1/8)(-3))$
      ii. $-(-(1/2) - (2/4) - (3/8) - (3/8)) = 1.75$

         1) $P_C(c_1) = (1/2)(1/4) + (1/2)(1/2) + (1/4)(1/2) = (1/8) + (2/8) + (1/8) = (1/2)$
         2) $P_C(c_2) = (1/4)(1/4) + (1/2)(1/4) + (1/4)(1/4) = (1/16) + (2/16) + (1/16) = (1/4)$
         3) $P_C(c_3) = (1/4)(1/4) + (0)(1/4) + (1/4)(1/4) = (1/16) + (1/16) = (1/8)$
         4) $P_C(c_4) = (0)(1/4) + (1/4)(1/2) + (0)(1/2) = (1/8)$