Billy Culver

1a) $a \equiv b \bmod n \rightarrow \frac{a-b}{n} = k$ an int

$\frac{b-a}{n} = -k$ also int

$b \equiv a \bmod n$

b) $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$

$a \bmod n \equiv b \equiv c \bmod n$

$a \equiv c \bmod n$

2)

a) $4321 = 3(1234) + 619$

$1234 = 1(619) + 615$

$619 = 1(615) + 4$

$615 = 153(4) + \boxed{1}$

$4 = 4(1) + 0$ ✓

$P_0 = 0$

$P_1 = 1$

$P_2 = 0 - 1(3) \bmod 4321 = 4318$

$P_3 = 1 - 4318(1) \bmod 4321 = 4$

$P_4 = 4318 - 4 \bmod 4321 = 4314$

$P5 = 4 - (4314)\,153 \bmod 4321 = 1075$

$P6 = 4314 - 1075(1) \bmod 4321 = \boxed{3239}$

b) $24140 \bmod 40902$

$40902 = 1(24140) + 16762$

$24140 = 1(16762) + 7378$

$16762 = 2(7378) + 2006$

$7378 = 3(2006) + 1360$

$2006 = 1(1360) + 646$

$1360 = 2(646) + 68$

$646 = 9(68) + \boxed{34}$ no inverse.

$68 = 2(34) + 0$

c) 550 mod 1769

$1769 = 3(550) + 119$
$550 = 4(119) + 74$
$119 = 1(74) + 45$
$74 = 1(45) + 29$
$45 = 1(29) + 16$
$29 = 1(16) + 13$
$16 = 1(13) + 3$
$13 = 4(3) + 1$
$3 = 3(1) + 0$

$P_0 = 0$
$P_1 = 1$
$P_2 = 0 - 1(3) \bmod 1769 = 1766$
$P_3 = 1 - 1766(4) \bmod 1769 = 13$
$P_4 = 1766 - 13(1) \bmod 1769 = 1753$
$P_5 = 13 - 1753(1) \bmod 1769 = 29$
$P_6 = 1753 - 29(1) \bmod 1769 = 1224$
$P_7 = 29 - 1224(1) \bmod 1769 = 74$
$P_8 = 1224 - 74(1) \bmod 1769 = 1650$
$P_9 = 74 - 1650(4) \bmod 1769 = \boxed{550}$

3a) Reducable

$GF(2) = \{x, x+1, x^2+x+1\}$

$$x+1 \overline{)\, x^3+0x^2+0x+1} \quad x^2 - x + 1$$

$x^3 + x^2$
$-x^2$
$-x^2 - x$
$x + 1$
$x + 1$
0

$(x+1)(x^2 - x + 1)$

b) irreducable

$$\frac{x^3+x^2+1}{x} = (x^2+x) + \frac{1}{x}$$

$$\frac{x^3+x^2+1}{x+1} = x^2 + \frac{1}{x+1}$$

$$\frac{x^3+x^2+1}{x^2+x+1} = x + \frac{x+1}{x^2+x+1}$$

c) $x^4+1 = (x^2+x+1)(x^2-x) + (x+1)$
(GF(2)) (Reducable) (GF(2))

$x^2 - x = x(x+1) - 2x = (x+1)x \bmod 2$

4a) $x^2+1 \overline{)\, x^3-x+1}$ $\quad x$

x^3+x

$-2x+1$

$x^3-x+1 = x(x^2+1) + (-2x+1)$

$= x(x^2+1) + 1$ $\quad$ (1)

$-1 \equiv 1 \mod 2$ in mod 2

b) $x^3+x^2+x+1 \overline{)\, x^5+x^4+x^3-x^2-x+1}$ $\quad x^2$

$x^5+x^4+x^3+x^2$

$-2x^2-x+1$

$-x+1 \equiv x+1 \mod 2$

$x^5+x^4+x^3-x^2-x+1 = x^3+x^2+x+1$ (x+1) $\quad$ x+1

5) $H(K|C) = H(K) + H(P) - H(E)$

$H(K) = H(P) = \frac{1}{4}\log\frac{1}{4} + \frac{1}{4}\log\frac{1}{4} + \frac{1}{2}\log\frac{1}{2} =$ 1.5

$H(C)$

1: $k_1 a + k_1 c + k_2 c = \frac{1}{2}$

2: $k_1 b + k_2 a + k_3 b = \frac{1}{4}$

3: $k_2 b + k_3 a + k_4 a = \frac{1}{8}$

4: $k_3 c + k_4 b + k_4 c = \frac{1}{8}$

$\frac{1}{2}\log\frac{1}{2} + \frac{1}{4}\log\frac{1}{4} + \frac{1}{8}\log\frac{1}{8} + \frac{1}{8}\log\frac{1}{8} = 1.75$

$3 - 1.75 =$ 1.25