HW 2 pt A

Nolan Pofi

1.
a).
To show $a \equiv b (\mod n)$ implies $b \equiv a (\mod n)$
First, if $n|(a-b)$ then $(a-b) = kn$ for some k which can be written as $a = b + kn$
Meaning $(a \mod n) =$ (remainder when $b + kn$ is divided by n) = (remainder when b is divided by n) $= (b \mod n)$.
Next, if $n|(-1)(b-a)$ then $(b-a) = kn$ for some k which can be written as $b = a + kn$ Meaning, $(b \mod n) =$ (remainder when $a + kn$ is divided by n) = (remainder when a is divided by n) $= (a \mod n)$.
Therefore $a \equiv b (\mod n)$ implies $b \equiv a (\mod n)$.

b).
To show $a \equiv b (\mod n)$ and $b \equiv c (\mod n)$ implies $a \equiv c (\mod n)$
First, if $n|(a-b)$ and $n|(b-c)$ then $(a-b) = kn$ and $(b-c) = ln$ for some k and l which can be written as $a = b + kn$ and $b = c + ln$
So, $(a \mod n) =$ (remainder when $b + kn$ is divided by n) = (remainder when b is divided by n) $= (b \mod n)$ and
$(b \mod n) =$ (remainder when $c + ln$ is divided by n) = (remainder when c is divided by n) $= (c \mod n)$
So, $a (\mod n) = b (\mod n) = c (\mod n)$
Therefore, $a \equiv c (\mod n)$

2.
a).

$4321 = (1234) \times 3 + 619$	$p_0 = 0$
$1234 = (619) \times 1 + 615$	$p_1 = 1$
$619 = (615) \times 1 + 4$	$p_2 = 0 - 1(3) \mod 4321 = 4318$
$615 = (4) \times 153 + 3$	$p_3 = 1 - 4318(1) \mod 4321 = 4$
$4 = (3) \times 1 + 1$	$p_4 = 4318 - 4(1) \mod 4321 = 4314$
$3 = (1) \times 3 + 0$	$p_5 = 4 - 4314(153) \mod 4321 = 1075$
	$p_6 = 4314 - 1075(1) \mod 4321 = 3239$

Inverse = 3239

b).
$40902 = (24140) \times 1 + 16762$
$24140 = (16762) \times 1 + 7378$
$16762 = (7378) \times 2 + 2006$
$7378 = (2006) \times 3 + 1360$
$1360 = (1360) \times 1 + 646$
$1360 = (646) \times 2 + 68$
$646 = (68) \times 9 + 64$
$68 = (34) \times 2 + 0$
Gcd(40902,24140) $\neq 1$ therefore no inverse exists

c).

$1769 = (550) \times 3 + 119$	$p_0 = 0$
$550 = (119) \times 4 + 74$	$p_1 = 1$
$119 = (74) \times 1 + 45$	$p_2 = 0 - 1(3) \mod 1769 = 1766$
$74 = (45) \times 1 + 29$	$p_3 = 1 - 1766(4) \mod 1769 = 13$
$45 = (29) \times 1 + 16$	$p_4 = 1766 - 13(1) \mod 1769 = 1753$
$29 = (16) \times 1 + 13$	$p_5 = 13 - 1753(1) \mod 1769 = 29$
$16 = (13) \times 1 + 3$	$p_6 = 1753 - 29(1) \mod 1769 = 1724$
$13 = (3) \times 4 + 1$	$p_7 = 29 - 1724(1) \mod 1769 = 74$
$3 = (1) \times 3 + 0$	$p_8 = 1724 - 74(1) \mod 1769 = 1650$
	$p_9 = 74 - 1650(4) \mod 1769 = 550$

Inverse = 550

3.
a).
$\frac{x^3+1}{x+1} = (x^2 + x + 1)$
$x^3 + 1$ reduces to $(x + 1)(x^2 + x + 1)$

b).
$(x^3 + x^2 + 1)$ is not divisible by x can tell by looking
$\frac{x^3+x^2+1}{x+1} = (x^2) + 1$ remainder exists so it isn't divisble by x + 1
therefore it is irreducible over GF(2).

c).
$\frac{x^4+1}{x+1} = x^3 + x^2 + x + 1$
$x^4 + 1$ reduces to $(x + 1)(x^3 + x^2 + x + 1)$

4.
a).
$x^3 - x + 1$ over GF(2) $= x^3 + x + 1$
$\gcd((x^3 + x + 1), (x^2 + 1))$
$x^3 + x + 1 = (x)(x^2 + 1) + 1$ remainder of one
Therefore $\gcd((x^3 + x + 1), (x^2 + 1))$ =1

b).
Over GF(3) $x^5 + x^4 + x^3 + 2x^2 + 2x + 1$
gcd$((x^5 + x^4 + x^3 + 2x^2 + 2x + 1), (x^3 + x^2 + x + 1))$
$(x^5 + x^4 + x^3 + 2x^2 + 2x + 1) = (x^2)(x^3 + x^2 + x + 1) + (x^2 + 2x + 1)$
gcd$((x^3 + x^2 + x + 1), (x^2 + 2x + 1))$
$(x^3 + x^2 + x + 1) = (x + 2)(x^2 + 2x + 1) + (2x + 2)$
gcd$((x^2 + 2x + 1), (2x + 2))$
$(x^2 + 2x + 1) = (x + x)(2x + 2) + (x + 1)$
gcd$((2x + 2), (x + 1))$
$2x + 2 = (2)(x + 1) + 0$ remainder of zero
Therefore gcd$((x^5 + x^4 + x^3 + 2x^2 + 2x + 1), (x^3 + x^2 + x + 1))$ = (x+1)

5.
$P_c(1) = (\frac{1}{4} * \frac{1}{2}) + (\frac{1}{2} * \frac{1}{2}) + (\frac{1}{2} * \frac{1}{4}) = .5$
$P_c(2) = (\frac{1}{4} * \frac{1}{2}) + (\frac{1}{4} * \frac{1}{4}) + (\frac{1}{4} * \frac{1}{4}) = .25$
$P_c(3) = (\frac{1}{4} * \frac{1}{4}) + (\frac{1}{4} * \frac{1}{4}) = .125$
$P_c(1) = (\frac{1}{2} * \frac{1}{4}) = .125$

Method 1:
$H(K|C) = H(K) + H(P) - H(C)$

$H(K) = -(\frac{1}{2}\log_2\frac{1}{2} + {}^{1}\log_2\frac{1}{4} + \frac{1}{4}\log_2\frac{1}{4}) = 1.5$
$H(P) = -(\frac{1}{4}\log_2\frac{1}{4} + \frac{1}{4}\log_2\frac{1}{4} + \frac{1}{2}\log_2\frac{1}{2}) = 1.5$
$H(C) = -(.5\log_2 .5 + .25\log_2 .25 + .125\log_2 .125 + .125\log_2 .125) = 1.75$

$H(K|C) = 1.5 + 1.5 - 1.75 = 1.25$

Method 2:
Pr(1—k1) = Pr(a) + Pr(c) = $\frac{3}{4}$
Pr(1—k2) = Pr(c) = $\frac{1}{2}$
Pr(1—k3) = 0
Pr(1—k4) = 0
Pr(2—k1) = Pr(b) = $\frac{1}{4}$
Pr(2—k2) = Pr(a) = $\frac{1}{4}$
Pr(2—k3) = Pr(b) = $\frac{1}{4}$
Pr(2—k4) = 0
Pr(3—k1) = 0
Pr(3—k2) = Pr(b) = $\frac{1}{4}$
Pr(3—k3) = Pr(a) = $\frac{1}{4}$
Pr(3—k4) = 0
Pr(4—k1) = 0
Pr(4—k2) = 0
Pr(4—k3) = Pr(c) = $\frac{1}{2}$
Pr(4—k4) = 0

Pr(k1—1) = Pr(1—k1) Pr(k1) / Pr(1) = $\frac{3}{4}$

Pr(k1—2) = Pr(2—k1) Pr(k1) / Pr(2) = $\frac{1}{2}$
Pr(k1—3) = Pr(3—k1) Pr(k1) / Pr(3) = 0
Pr(k1—4) = Pr(4—k1) Pr(k1) / Pr(4) = 0
Pr(k2—1) = Pr(1—k2) Pr(k2) / Pr(1) = $\frac{1}{4}$
Pr(k2—2) = Pr(2—k2) Pr(k2) / Pr(2) = $\frac{1}{4}$
Pr(k2—3) = Pr(3—k2) Pr(k2) / Pr(3) = $\frac{1}{2}$
Pr(k2—4) = Pr(4—k2) Pr(k2) / Pr(4) = 0
Pr(k3—1) = Pr(1—k3) Pr(k3) / Pr(1) = 0
Pr(k3—2) = Pr(2—k3) Pr(k3) / Pr(2) = $\frac{1}{4}$
Pr(k3—3) = Pr(3—k3) Pr(k3) / Pr(3) = $\frac{1}{2}$
Pr(k3—4) = Pr(4—k3) Pr(k3) / Pr(4) = 1
Pr(k4—1) = Pr(1—k4) Pr(k4) / Pr(1) = 0
Pr(k4—2) = Pr(2—k4) Pr(k4) / Pr(2) = 0
Pr(k4—3) = Pr(3—k4) Pr(k4) / Pr(3) = 0
Pr(k4—4) = Pr(4—k4) Pr(k4) / Pr(4) = 0

H(K—C) = -Sum_(k in K, c in C) Pr(c) Pr(k—c) $\log_2$(Pr(k—c)) = $-(.5(\frac{3}{4}\log_2\frac{3}{4}+\frac{1}{4}\log_2\frac{1}{4}+\frac{1}{4}\log_2\frac{1}{4}+0\log_2 0)+.25(\frac{1}{2}\log_2\frac{1}{2}+\frac{1}{4}\log_2\frac{1}{4}+\frac{1}{4}\log_2\frac{1}{4}+0\log_2 0)+.125(0\log_2 0+\frac{1}{2}\log_2\frac{1}{2}+\frac{1}{2}\log_2\frac{1}{2}+0\log_2 0)+.125(0\log_2 0+0\log_2 0+1\log_2 1+0\log_2 0)) = 1.156$