1)

951

1335188

Jack Phillips
Hw 2 Part A

1) Proofs

a) $a \equiv b \pmod{n} \rightarrow b \equiv a \pmod{n}$

assume $a \equiv b \pmod{n}$.

By definition $n \mid (b-a)$, this means $n \mid (-1)(b-a)$, which is $n \mid (a-b)$. Meaning $b \equiv a \pmod{n}$

b) $a \equiv b \pmod{n}$, $b \equiv c \pmod{n} \rightarrow a \equiv c \pmod{n}$

This means that:

$n \mid (b-a)$ and $n \mid (c-b)$. Any number divisible by n added to another divisiable by n is also divisible by n. This gets you:

$n \mid (b-a) + (c-b) \Rightarrow n \mid (c-a)$.

This means $a \equiv c \pmod{n}$.

2)

a) $1234 \bmod 4321$

$\gcd(1234, 4321)$

$4321 = 1234(3) + 619$

$1234 = 619(1) + 615$

$619 = 615(1) + 4$

$615 = 4(153) + 3$

$4 = 3(1) + 1$

$3 = 3(1)$

$1 = 4 - 3(1)$

$1 = 4 - (615 - 4(153))$

$1 = 4(154) - 615$

$1 = (619 - 615)(154) - 615$

$1 = 619(154) - 615(155)$

$1 = 619(154) - (1234(1) - 619(1))(155)$

$1 = 619(309) - 1234(155)$

$1 = (4321 - 1234(3))(309) - 1234(155)$

$1 = 4321(309) - 1234(1082)$

$1 = 432(309) + 1234(-1082)$

$1 \equiv 1234(-1082) \bmod 4321$

Positive $= 3239$

b) 24140 mod 40902

gcd(24140, 40902)

40902 = 24140 + 16762

24140 = 16762 + 7378

16762 = 7378(2) + 2006

7378 = 2006(3) + 1360

2006 = 1360 + 646

1360 = 646(2) + 68

646 = 68(9) + 34

68 = 34(2) + 0 ← Not 1

$\boxed{\text{Does Not Exist}}$

c) 550 mod 1769

gcd(550, 1769) = 1

1769 = 550(3) + 119

550 = 119(4) + 74

119 = 74(1) + 45

74 = 45(1) + 29

45 = 29(1) + 16

29 = 16 + 13

16 = 13 + 3

13 = 3(4) + 1

3 = 3(1)

1 = 13 - 3(4)

1 = 13 - (16 - 13)(4)

1 = 13(5) - 16(4)

1 = (29 - 16)(5) - 16(4)

1 = 29(5) - 16(9)

1 = 29(5) - (45 - 29)(9)

1 = 29(14) - 45(9)

1 = (74 - 45)(14) - 45(9)

1 = 74(14) - 45(23)

1 = 74(14) - (119 - 74)(23)

1 = 74(37) - (119)(23)

1 = (550 - 119(4))(37) - 119(23)

1 = 550(37) - 119(171)

1 = 550(37) - (1769 - 550(3))(171)

1 = 550(550) - 1769(171)

$\boxed{1 \equiv (550)(550) \bmod 1769}$

3) reducible GF(2)

a) $x^3+1 = (x+1)(x^2+1) = x^3 + \underbrace{x + x^2}_{\text{always even}} + 1 \pmod 2$

b) $x^3+x^2+1 \Rightarrow$ Not reducible

c) $x^4+1 = (x^2+1)(x^2+1) = x^4 \underbrace{+2x^2}_{\text{even always}} + 1 \pmod 2$

4)

a) x^3-x+1 and x^2+1 over GF(2)
↳ Not reducible $\boxed{gcd = 1}$

b) $x^5+x^4+x^3+x^2+x+1$ and x^3+x^2+x+1 GF(3)

$(x+1)(x^4+x^2+x+1)$ $(x^2+1)(x+1)$

$\boxed{GCD = x+1}$

5) Not valid so calc the harder way :(

$Pr(1|k_1) = 1/4 + 1/2 = 3/4$

$Pr(1|k_2) = 1/2$

$P(1|k_3) = 0$

$P(2|k_1) = 1/4$

$P(2|k_2) = 1/4$

$P(2|k_3) = 1/4$

$P(3|k_1) = 0$

$P(3|k_2) = 1/4$

$P(3|k_3) = 1/4$

$P(4|k_1) = 0$

$P(4|k_2) = 0$

$P(4|k_3) = 1/2$

$P(1) = (\frac{1}{4})(\frac{1}{2}) + (1/2)(1/2) + (1/4)(\frac{1}{2}) =$
$1/8 + 1/4 + 1/8 = 1/2$

$P(2) = (1/4)(1/4) + (1/4)(1/4) + (1/2)(1/4)$
$= 1/16 + 1/16 + 1/8 = 2/8 = 1/4$

$P(3) = (1/4)(1/2) + (1/4)(1/4) = 1/8$

$P(4) = (1/4)(1/2) = 1/8$

$P(K_1|1) = (3/4)(1/2)/1/2 = 3/4$

$P(K_2|1) = (1/2)(1/4)/(1/2) = 1/4$

$P(K_3|1) = 0$

$P(K_1|2) = (1/4)(1/2)/(1/4) = 1/2$

$P(K_2|2) = (1/4)(1/4)/(1/4) = 1/4.$

$P(K_3|2) = (1/4)(1/4)/(1/4) = 1/4$

$P(K_1|3) = 0$

$P(K_2|3) = (1/4)(1/4)/(1/8) = 1/16/1/8 = 1/2$

$P(K_3|3) = (1/4)(1/4)/(1/8) = 1/2$

$P(K_1|4) = 0$

$P(K_2|4) = 0$

$P(K_3|4) = (1/2)(1/4)/(1/8) = 1$

$$\begin{aligned}
H(K|C) = -\Big(&1/2(3/4\log_2 3/4 + 1/4\log_2 1/4 + 0)\\
&+ 1/4(1/2\log_2 1/2 + 1/4\log_2 1/4 + 1/4\log_2 1/4)\\
&+ 1/8(0 + 1/2\log_2 1/2 + 1/2\log_2 1/2)\\
&+ 1/8(1\log_2 1)\Big)\\
= -(-.40564& - .375 - .125 - 0)\\
= \boxed{.90654}&
\end{aligned}$$