① Prove that

a) $a \equiv b \pmod n$ implies $b \equiv a \pmod n$

a is congruent to b modulo n, provided that n divides $a - b$

is $17 \equiv 5 \pmod 6$

b)

i $a - a = 0$ and $n \mid 0$, so $a \equiv a \pmod n$

ii: $a \equiv b \pmod n$ means that $a - b = nk$ for some $k \in \mathbb{Z}$. Therefore $b - a = -nk = n(-k)$; so $b \equiv a \pmod n$

iii If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then

$$a - b = nk$$
$$b - c = n'k$$

this we get $a - c = n(k + k')$ so $a \equiv c \pmod n$

② 1234 mod 43+1

24140 mod 4090 2

5 50 mod 1769

Ex. 8 mod 11

Euclidian algorithm	reverse Euclids
$11 = 8(1) + 3$	$3 = 11 - 8(1)$
$8 = 3(2) + 2$	$2 = 8 - 3(2)$
$3 = 2(1) + 1$	$1 = 3 - (2 \cdot 1)$
$2 = 1(2)$	

1234 mod 4321

Euclid algorithm

$4321 = 1234(3) + 619$
$1234 = 619(1) + 615$
$619 = 615(1) + 4$
$615 = 4(153) + 3$
$4 = 3(1) + 1$
$3 = 1(3)$

$\rho_0 = 0$
$\rho_1 = 1$
$\rho_2 = 0 - 1(3) \bmod 4321 = 4318$
$\rho_3 = 1 - 4318(1) \bmod 4321 = 4$
$\rho_4 = 4318 - 4(1) \bmod 4321 = 4314$
$\rho_5 = 4 - 4314(153) \bmod 4321 = 1075$
$\rho_6 = [4314 - 1075(1)] \bmod 4321 = 3239$

$-3 \bmod 4321$
$-4317 \bmod 4321$
$-660038 \bmod 4321$

$$\frac{-660038}{4321} = -152.75125 \Rightarrow 4321 \cdot .75$$

$$= -3246$$

3239 mod 4321 1234^{-1} is congruent to

$3239 \equiv 1234^{-1} \bmod 4321$

24140 mod 40902

Euclid

40902 = 24140 (1) + 16762
24140 = 16762 (1) + 7378
16,762 = 7378 (2) + 2006
7378 = 2006 (3) + 1360
2006 = 1360 (1) + 646
1360 = 646 (2) + 68
646 = 68 (9) + 34
68 = 34 (2) + 0

no multiplicative inverse.

③ 550 mod 1769

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

$p_0 = 0$
$p_1 = 1$
$p_2 = 0 - 1(3) \bmod 1769 \equiv 1766$
$p_3 = 1 - 1766(4) \bmod 1769 = 13$
$p_4 = 1766 - 13(1) \bmod 1769 = 175$
$p_5 = 13 - 175(1) \bmod 1769 = 29$
$p_6 = 175 - 29(1) \bmod 1769 = 1724$
$p_7 = 29 - 1724(1) \bmod 1769 = 74$
$p_8 = 1724 - 74(1) \bmod 1769 = 1650$
$p_9 = 74 - 1650(4) \bmod 1769 = 550$

1766 · 4 = 7064

3,493216507 = −1757
−1756 mod 1769 =

3.689089881
· 1769 = −1219 mod 1769

$550 \equiv 550^{-1} \bmod 1769$

3) determine reducible over GF(2)

a) reducible
b) irreducible
c) reducible

4)
a) x^3-x+1 and x^2+1 over GF(2)

(x^3-x+1) (x^2+1) $(x+1)\cdot(x)$

$x^3+x+x+1$

x^2+2x

$\rightarrow 2x+1$

$$\begin{array}{r} x+1 \\ x^2+1 \;\big|\; x^3-3x+1 \\ -(x^3+x) \\ \hline -4x+1 \end{array}$$

$$\begin{array}{r} -\frac{1}{4}x \\ -4x \;\big|\; x^2+1 \\ -(x^2) \\ \hline 1 \end{array}$$

$-4x$

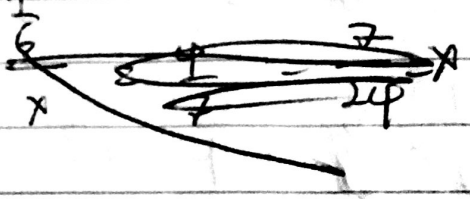
$gcd = x+1$

(5)

$$H(k|c) = -\text{Sum}(k \text{ in } K, c \text{ in } C) \cdot Pr(c) \cdot Pr(k|c) \cdot \log_2(Pr(k|c))$$

$Pr(1|k_1)$ $Pr(a) + Pr(c) = 3/4$
$Pr(1|k_2)$ $Pr(c) = 1/2$
$Pr(1|k_3)$ ϕ
$Pr(2|k_1)$ $Pr(b) = 1/4$
$Pr(2|k_2)$ $Pr(a) = 1/4$
$Pr(2|k_3)$ $Pr(b) = 1/4$
$Pr(3|k_1)$ ϕ
$Pr(3|k_2)$ $1/4$
$Pr(3|k_3)$ $1/4$
$Pr(4|k_1)$ ϕ
$Pr(4|k_2)$ ϕ
$Pr(4|k_3)$ $1/2$

$Pr(1) = (1/2 \cdot 3/4) + (1/4 \cdot 1/2) + 0$
$Pr(2) = (1/2 \cdot 1/4) + (1/4 \cdot 1/4) + (1/4 \cdot 1/4)$
$Pr(3) = 0 + (1/4 \cdot 1/4) + (1/4 \cdot 1/2)$
$Pr(4) = 0 + 0 + (1/4 \cdot 1/2)$
$Pr(1) = 1/2$
$Pr(2) = 1/4$
$Pr(3) = 3/16$
$Pr(4) = 1/8$



$Pr(k_1|1) = Pr(1|k_1) Pr(k_1) / Pr(1) = 3/4$
$Pr(k_1|2) = 1/4 \cdot 1/2 / 1/4 = 1/2$
$Pr(k_1|3) = \phi \cdot 1/2 / 3/16 = \phi$
$Pr(k_1|4) = \phi \cdot 1/2 / 1/8 = \phi$
$Pr(k_2|1) = 1/2 \cdot 1/4 / 1/2 = 1/4$
$Pr(k_2|2) = 1/4 \cdot 1/4 / 1/4 = 1/4$
$Pr(k_2|3) = 1/4 \cdot 1/4 / 3/16 = 1/3$
$Pr(k_2|4) = \phi \cdot 1/4 / 1/8 = \phi$
$Pr(k_3|1) = \phi \cdot 1/4 / 1/2 = \phi$
$Pr(k_3|2) = 1/4 \cdot 1/4 / 1/4 = 1/4$
$Pr(k_3|3) = 1/4 \cdot 1/4 / 3/16 = 1/3$
$Pr(k_3|4) = 1/2 \cdot 1/4 / 1/8 = 1$

1) $H(k|c) = -\sum_{k \in K, c \in C} P(c)\, P(k,k) \log_2 (P(k|c))$

$= -\left(\frac{1}{2}\left(\frac{3}{4}\log_2\left(\frac{3}{4}\right) + \frac{1}{4}\left(\log_2 \frac{1}{4}\right) + 0\log_2 0\right)\right) = .4054$

$+ \left(\frac{1}{4}\left(\frac{1}{2}\log_2 \frac{1}{2}\right) + \frac{1}{4}\left(\log_2 \frac{1}{2}\right) + \frac{1}{4}\left(\log_2 \frac{1}{4}\right)\right) = .375$

$+ \left(\frac{1}{16}\cdot\left(0\log_2 0\right) + \frac{1}{2}\left(\log_2 \frac{1}{2}\right) + \frac{1}{2}\left(\log_2 \frac{1}{2}\right)\right) = .1981$

$+ \left(\frac{1}{16}\cdot\left(0\log_2 0\right) + 0\log_2 0\right) + 1\log_2(1) = 0$

$\approx .9376 \quad .9376$