Cassell Teng
HW 2 Theory Part A

1 (a) $a \equiv b \pmod n \rightarrow b \equiv a \pmod n$

↳ $a - b = nk \rightarrow b - a = -nk = n(-k) \rightarrow b \equiv a \pmod n$

(b) $a \equiv b \pmod n$ & $b \equiv c \pmod n \rightarrow a \equiv c \pmod n$

$(a - b = nk) + (b - c = nk') = a - c = nk + nk'$

$= n(k + k')$

$a \equiv c \pmod n$

2. (a) $1234 \bmod 4321$

$4321 = 3(1234) + 619$ $\quad p_0 = 0$

$1234 = 1(619) + 615$ $\quad p_1 = 1$

$619 = 1(615) + 4$ $\quad p_2 = 0 - 1(3) \bmod 4321 = 4318$

$615 = 153(4) + 3$ $\quad p_3 = 1 - 4318(1) \bmod 4321 = 4$

$4 = 1(3) + 1$ $\quad p_4 = 4318 - 4(1) \bmod 4321 = 4314$

$3 = 3(1) + 0$ $\quad p_5 = 4 - 4314(153) \bmod 4321 = 1075$

$p_6 = 4314 - 1075(1) \bmod 4321 = 3239$

$1234(3239) = 1 + 925(4321) \equiv 1 \bmod 4321$

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

(b) $24140 \bmod 40902$

$40902 = 1(24140) + 16762$

$24140 = 1(16762) + 7378$

$16762 = 2(7378) + 2006$

$7378 = 3(2006) + 1360$

$2006 = 1(1360) + 646$

$1360 = 2(646) + 68$

$646 = 9(68) + 34$

$68 = 2(34) + 0 \rightarrow$ No multiplicative inverse

(c) $550 \bmod 1769$

$1769 = 3(550) + 119$ $\quad p_0 = 0$

$550 = 4(119) + 74$ $\quad p_1 = 1$

$119 = 1(74) + 45$ $\quad p_2 = 0 - 1(3) \bmod 1769 = 1766$

$74 = 1(45) + 29$ $\quad p_3 = 1 - 1766(4) \bmod 1769 = 13$

$45 = 1(29) + 16$ $\quad p_4 = 1766 - 13(1) \bmod 1769 = 1753$

$29 = 1(16) + 13$ $\quad p_5 = 13 - 1753(1) \bmod 1769 = 29$

$16 = 1(13) + 3$ $\quad p_6 = 1753 - 29(1) \bmod 1769 = 1724$

$13 = 4(3) + 1$ $\quad p_7 = 29 - 1724(1) \bmod 1769 = 74$

$3 = 3(1) + 0$ $\quad p_8 = 1724 - 74(1) \bmod 1769 = 1650$

$p_9 = 74 - 1650(4) \bmod 1769 = 550$

$(550)^2 = 1 + 171(1769) = 1 \bmod 1769$ $\quad 550 \equiv 550^{-1} \bmod 1769$

3. (a) x^3+1

$f(0)=1 \rightarrow x+1$ is a factor $\rightarrow$ Reducible

$f(1)=1+1=0$

(b) x^3+x^2+1

$f(0)=1$

$f(1)=1+1+1=1 \rightarrow$ Irreducible.

(c) x^4+1

$f(0)=1 \rightarrow$ Reducible.

$f(1)=1+1=0$

4. (a) x^3-x+1 & x^2+1 GF(2)

$x^3-x+1 \mod x^2+1$:

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

$x^2+1 \mod x+1$:

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

GCD

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

$x^5+x^4+x^3-x^2-x+1 \mod x^3+x^2+x+1$:

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

$x^3+x^2+x+1 \mod x^2-x+1$:

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

$x^2-x+1 \mod x+1$:

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

GCD = 1

5. $P = \{a, b, c\}$: $P_p(a) = \frac{1}{4}$ $P_p(b) = \frac{1}{4}$ $P_p(c) = \frac{1}{2}$

$K = (k_1, k_2, k_3)$: $P_k(k_1) = \frac{1}{2}$ $P_k(k_2) \frac{1}{4}$ $P_k(k_3) \frac{1}{4}$

$C = \{1, 2, 3, 4\}$

$E_1(P)$:	a	b	c
k_1	1	2	1
k_2	2	3	1
k_3	3	2	4
k_4	3	4	4

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

$H(P) = \frac{1}{4}\log_2 4 + \frac{1}{4}\log_2 4 + \frac{1}{2}\log_2 2 = 1.5$

$H(K) = \frac{1}{2}\log_2 2 + \frac{1}{4}\log_2 4 + \frac{1}{4}\log_2 4 = 1.5$

$P_r(C=1) = \frac{1}{2}\left(\frac{1}{4} + \frac{1}{2}\right) + \frac{1}{4}\left(\frac{1}{2}\right) = \frac{1}{2}$

$P_r(C=2) = \frac{1}{2}\left(\frac{1}{4}\right) + \frac{1}{4}\left(\frac{1}{4}\right) + \frac{1}{4}\left(\frac{1}{2}\right) = \frac{5}{16}$

$P_r(C=3) = \frac{1}{4}\left(\frac{1}{4}\right) + \frac{1}{4}\left(\frac{1}{4}\right) = \frac{1}{8}$

$H(C) = -\frac{1}{2}\log_2\left(\frac{1}{2}\right) - \frac{5}{16}\log_2\left(\frac{5}{16}\right) - \frac{1}{8}\log_2\left(\frac{1}{8}\right) = 1.3994$

$H(K|C) = 1.5 + 1.5 - 1.3994 = 1.6006$