Jack Dates

① (a) By definition $a \equiv b \bmod n \rightarrow a = kn + b$ for some $k \in \mathbb{Z}$
$\rightarrow b = (-k)n + a$. Since $-k \in \mathbb{Z}$ by definition $b \equiv a \bmod n$

(b) By definition $a \equiv b \bmod n \rightarrow a = kn + b$, $k \in \mathbb{Z}$ and $b \equiv c \bmod n \rightarrow b = ln + c$, $l \in \mathbb{Z}$. Substituting b gives $a = (k+l)n + c$.
Since $k + l \in \mathbb{Z}$ $a \equiv c \bmod n$

② (a)

$4321 = 3 \cdot 1234 + 619$	$1 - 3 \cdot 0 = 1$	$0 - 3 \cdot 1 = -3$
$1234 = 1 \cdot 619 + 615$	$0 - 1 \cdot 1 = -1$	$1 - 1(-3) = 4$
$619 = 1 \cdot 615 + 4$	$1 - 1(-1) = 2$	$-3 - 1(4) = -7$
$615 = 153 \cdot 4 + 3$	$-1 - 153(2) = -307$	$4 - (153)(-7) = 1075$
$4 = 1 \cdot 3 + 1$	$2 - 1(-307) = 309$	$-7 - 1(1075) = -1082$
$3 = 3 \cdot 1 + 0$		$-1082 \% 4321 = 3239$

(b)

$40902 = 1 \cdot 24140 + 16762$	$1 - 1 \cdot 0 = 1$	$0 - 1 \cdot 1 = -1$
$24140 = 1 \cdot 16762 + 7378$	$0 - 1 \cdot 1 = -1$	$1 - 1(-1) = 2$
$16762 = 2 \cdot 7378 + 2006$	$1 - 2(-1) = 3$	$-1 - 2 \cdot 2 = -5$
$7378 = 3 \cdot 2006 + 1360$	$-1 - 3 \cdot 3 = -10$	$2 - 3(-5) = 17$
$2006 = 1 \cdot 1360 + 646$	$3 - 1(-10) = 13$	$-5 - 1 \cdot 17 = -22$
$1360 = 2 \cdot 646 + 68$	$-10 - 2 \cdot 13 = -36$	$17 - 2(-22) = 61$
$646 = 9 \cdot 68 + 34$	$13 - 9(-36) = 337$	$-22 - 9 \cdot 61 = -571$
$68 = 2 \cdot 34 + 0$	gcd $\neq 1$, no modular inverse	

(c)

$1769 = 3 \cdot 550 + 119$	$1 - 3 \cdot 0 = 1$	$0 - 3 \cdot 1 = -3$
$550 = 4 \cdot 119 + 74$	$0 - 4 \cdot 1 = -4$	$1 - 4(-3) = 13$
$119 = 1 \cdot 74 + 45$	$1 - 1(-4) = 5$	$-3 - 1 \cdot 13 = -16$
$74 = 1 \cdot 45 + 29$	$-4 - 1 \cdot 5 = -9$	$13 - 1(-16) = 29$
$45 = 1 \cdot 29 + 16$	$5 - 1(-9) = 14$	$-16 - 1 \cdot 29 = -45$
$29 = 1 \cdot 16 + 13$	$-9 - 1 \cdot 14 = -23$	$29 - 1(-45) = 74$
$16 = 1 \cdot 13 + 3$	$14 - 1(-23) = 37$	$-45 - 1 \cdot 74 = -119$
$13 = 4 \cdot 3 + 1$	$-23 - 4 \cdot 37 = -171$	$74 - 4(-119) = 550$
$3 = 3 \cdot 1 + 0$		550

③ (a) $x^3 + 1 \equiv (x^2 + x + 1)(x + 1)$

(b) $x^3 + x^2 + 1$ is not reducible

(c) $x^4 + 1 \equiv (x^2 + 1)(x^2 + 1)$

4 a) $x^3 - x + 1 \equiv x^3 + x + 1$ which is irreducible, so the gcd is 1

b) $x^3 + x^2 + x + 1 \equiv (x+1)(x^2+1)$

$x^5 + x^4 + x^3 + 2x^2 + 2x + 1 \equiv (x+1)(x^4 + x^2 + x + 1)$

so gcd is $x+1$

5 $P(C)$:

$P(1) = \frac{1}{2}\frac{1}{4} + \frac{1}{2}\frac{1}{2} + \frac{1}{4}\frac{1}{2} = \frac{1}{2}$ NOTE: $P(k_4) = 0$

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

$P(3) = \frac{1}{4}\frac{1}{4} + \frac{1}{4}\frac{1}{4} = \frac{1}{8}$

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

$P(C|K)$:

$P(1\|k_1) = \frac{1}{4} + \frac{1}{2} = \frac{3}{4}$	$P(1\|k_2) = \frac{1}{2}$	$P(1\|k_3) = 0$
$P(2\|k_1) = \frac{1}{4}$	$P(2\|k_2) = \frac{1}{4}$	$P(2\|k_3) = \frac{1}{4}$
$P(3\|k_1) = 0$	$P(3\|k_2) = \frac{1}{4}$	$P(3\|k_3) = \frac{1}{4}$
$P(4\|k_1) = 0$	$P(4\|k_2) = 0$	$P(4\|k_3) = \frac{1}{2}$

$P(K|C)$:

$P(k_1\|1) = \frac{3}{4}\frac{1}{2}\cdot 2 = \frac{3}{4}$	$P(k_2\|1) = \frac{1}{2}\frac{1}{4}\cdot 2 = \frac{1}{4}$	$P(k_3\|1) = 0$
$P(k_1\|2) = \frac{1}{4}\frac{1}{2}\cdot 4 = \frac{1}{2}$	$P(k_2\|2) = \frac{1}{4}\cdot\frac{1}{4}\cdot 4 = \frac{1}{4}$	$P(k_3\|2) = \frac{1}{4}\cdot\frac{1}{4}\cdot 4 = \frac{1}{4}$
$P(k_1\|3) = 0$	$P(k_2\|3) = \frac{1}{4}\cdot\frac{1}{4}\cdot 8 = \frac{1}{2}$	$P(k_3\|3) = \frac{1}{4}\cdot\frac{1}{4}\cdot 8 = \frac{1}{2}$
$P(k_1\|4) = 0$	$P(k_2\|4) = 0$	$P(k_4\|4) = \frac{1}{2}\cdot\frac{1}{4}\cdot 8 = 1$

$$H(K|C) = \frac{1}{2}\left(\frac{3}{4}\log_2\frac{4}{3} + \frac{1}{4}\log_2 4\right) + \frac{1}{4}\left(\frac{1}{2}\log_2 2 + \frac{1}{4}\log_2 4 + \frac{1}{4}\log_2 4\right) + \frac{1}{8}\left(\frac{1}{2}\log_2 2 + \frac{1}{2}\log_2 2\right) + \frac{1}{8}(\log_2 1)$$

$$= \frac{1}{2}\left(\frac{3}{4}\log_2\frac{4}{3} + \frac{1}{2}\right) + \frac{1}{4}\left(\frac{3}{2}\right) + \frac{1}{8}(1) + 0$$

$$= \frac{3}{8}\log_2\frac{4}{3} + \frac{3}{4} = \boxed{.9056}$$