Josh Barthelmess (cryptography)

(1)

(a) $a \equiv b \bmod n \Rightarrow \frac{a-b}{n} = k$ where k is an integer

$\frac{a-b}{n} = k \Rightarrow \frac{b-a}{n} = -k$ ← also an integer

$\therefore$ $\boxed{b \equiv a \bmod n}$

(b) from above $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$

$\Rightarrow a \bmod n \equiv c \bmod n \Rightarrow \boxed{a \equiv c \bmod n}$

↗ transitive property

(2)

(a)

0: $4321 = 3(1234) + 619$ $\quad \rho_0 = 0$

1: $1234 = 1(619) + 615$ $\quad \rho_1 = 1$

2: $619 = 1(615) + 4$ $\quad \rho_2 = 0 - (1) \bmod 4321 \equiv 4318$

3: $615 = 153(4) + 3$ $\quad \rho_3 = 1 - 4318 \bmod 4321 \equiv 4$

4: $4 = 1(3) + 1$ $\quad \rho_4 = 4318 - 4 \bmod 4321 \equiv 4314$ multiplicative inverse

$\rho_5 = 4 - (4314)^{153} \bmod 4321 \equiv 1075$

$\rho_6 = 4314 - 1075 \bmod 4321 = \boxed{3239}$

L>

(2) (b)

0: $40902 = 1(24140) + 16762$

1: $24140 = 1(16762) + 7378$

2: $16762 = 2(7378) + 2006$

3: $7378 = 3(2006) + 1360$

4: $2006 = 1(1360) + 646$

5: $1360 = 2(646) + 68$

6: $646 = 9(68) + 34$ ← No multiplicative inverse

7: $68 = 2(34) + 0$

(c)

0: $1769 = 3(550) + 119$

1: $550 = 4(119) + 74$

2: $119 = 1(74) + 45$

3: $74 = 1(45) + 29$

4: $45 = 1(29) + 16$

5: $29 = 1(16) + 13$

6: $16 = 1(13) + 3$

7: $13 = 4(3) + 1$ ← need ρ_9

$\rho_0 = 0$

$\rho_1 = 1$

$\rho_2 = 0 - (1)3 \bmod 1769 \equiv 1766$

$\rho_3 = 1 - (1766)4 \bmod 1769$

$\equiv 13$

$\rho_4 = 1766 - 13 \bmod 1769 \equiv 1753$

$\rho_5 = 13 - 1753 \bmod 1769 \equiv 29$

$\rho_6 = 1753 - 29 \bmod 1769 \equiv 1724$

$\rho_7 = 29 - 1724 \bmod 1769 \equiv 74$

$\rho_8 = 1724 - 74 \bmod 1769 \equiv 1650$

$\rho_9 = 74 - 4(1650) \bmod 1769 \equiv \boxed{550}$

(3) (a)

reducible by $\boxed{x+1}$ ✓

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

$x^2 - x + 1$

$x^3 + x^2$

$-x^2$

$-x^2 - x$

$x + 1$

$x + 1$

$\boxed{10}$

(b)

irreducible by any odd factors in GF(7)

$(x+1,\ x^2+x+1)$

(c)

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

$$x^2 - x = x(x+1) - 2x = \boxed{(x+1)x \bmod 2}$$

4

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

$x^3 + x$

$-2x + 1$

$x^3 - x + 1 = x(x^2+1) - 2x + 1$

$= x(x^2+1) + \boxed{1} \mod 2$

$\boxed{1}$ ← gcd

(b)

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

$x^5 + x^4 + x^3 + x^2$

$-2x^2 - x + 1$

$x^5 + x^4 + x^3 - x^2 - x + 1 =$

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

$= x^2(x^3 + x^2 + x + 1) + \boxed{x + 1}$

$\boxed{x+1}$ ← gcd

(5)

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

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

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

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

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

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

$H(E) = -1\cdot\left(2\cdot\frac{1}{8}\log_2\left(\frac{1}{8}\right) + \frac{1}{2}\log_2\left(\frac{1}{2}\right) + \frac{1}{4}\log_2\left(\frac{1}{4}\right)\right)$

$= 1.75$

$H(K|C) = 3 - 1.75 = \boxed{1.25}$