

$$① a) a \equiv b \pmod{n}$$

$$a = qn + b$$

$$a - b = qn$$

$$b - a = (-q)n$$

$$b = (-q)n + a$$

$$\boxed{b \equiv a \pmod{n}}$$

$$b) a \equiv b \pmod{n} \quad b \equiv c \pmod{n}$$

$$a = qn + b$$

$$b = kn + c$$

$$c = b - kn$$

$$a - c = qn + b - b + kn$$

$$a - c = (q + k)n$$

$$a = (q + k)n + c$$

$$\boxed{a \equiv c \pmod{n}}$$

$$② a) 1234 \text{ mod } 4321$$

$$4321 = 1234 \times 3 + 619$$

$$1234 = 619 \times 1 + 615$$

$$619 = 615 \times 1 + 4$$

$$615 = 4 \times 153 + 3$$

$$4 = 3 \times 1 + 1$$

$$1 = 4 - 3$$

$$1 = 4 - 615 + 4 \times 153$$

$$1 = 4 \times 154 - 615$$

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

$$1 = 619 \times 154 - 615 \times 154 - 615$$

$$1 = 619 \times 154 - 615 \times 155$$

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

$$1 = 619 \times 154 - 1234 \times 155 + 619 \times 155$$

$$1 = 619 \times 309 - 1234 \times 155$$

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

$$1 = 4321 \times 309 - 927 \times 1234 - 1234 \times 155$$

$$1 = -1082 \times 1234$$

$$\boxed{3,239}$$



b)  $24140 \text{ mod } 40902$

$$40902 = 24140 \times 1 + 16762$$

$$24140 = 16762 \times 1 + 7378$$

$$16762 = 7378 \times 2 + 2006$$

$$7378 = 2006 \times 3 + 1360$$

$$2006 = 1360 \times 1 + 646$$

$$1360 = 646 \times 2 + 68$$

$$646 = 68 \times 9 + 34$$

$$68 = 34 \times 2 + 0$$

No Solution

c)  $550 \text{ mod } 1769$

$$1769 = 550 \times 3 + 119$$

$$550 = 119 \times 4 + 74$$

$$119 = 74 \times 1 + 45$$

$$74 = 45 \times 1 + 29$$

$$45 = 29 \times 1 + 16$$

$$29 = 16 \times 1 + 13$$

$$16 = 13 \times 1 + 3$$

$$13 = 3 \times 4 + 1$$

550

$$1 = 13 - 3 \times 4$$

$$1 = 13 - (16 - 13) \times 4$$

$$1 = 13 - 16 \times 4 + 13 \times 4$$

$$1 = 13 \times 5 - 16 \times 4$$

$$1 = (29 - 16) \times 5 - 16 \times 4$$

$$1 = 29 \times 5 - 16 \times 5 - 16 \times 4$$

$$1 = 29 \times 5 - 9 \times 16$$

$$1 = 29 \times 5 - 9 \times (45 - 29)$$

$$1 = 29 \times 5 - 9 \times 45 + 9 \times 29$$

$$1 = -9 \times 45 + 14 \times 29$$

$$1 = -9 \times 45 + 14 \times (74 - 45)$$

$$1 = -9 \times 45 + 14 \times 74 - 14 \times 45$$

$$1 = -23 \times 45 + 14 \times 74$$

$$1 = -23 \times (119 - 74) + 14 \times 74$$

$$1 = -23 \times 119 + 23 \times 74 + 14 \times 74$$

$$1 = -23 \times 119 + 37 \times 74$$

$$1 = -23 \times 119 + 37 \times (550 - 119 \times 4)$$

$$1 = -23 \times 119 + 37 \times 550 - 148 \times 119$$

$$1 = 37 \times 550 - 171 \times 119$$

$$1 = 37 \times 550 - 171 \times (1769 - 550 \times 3)$$

$$1 = 37 \times 550 - 171 \times 1769 + 513 \times 550$$



- ③ a) reducible  
b) irreducible  
c) reducible

④ a)  $f = qg + r$

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

$$\boxed{1}$$

$$\begin{array}{r} x \\ x^2+1 \overline{) x^3+x+1} \\ \underline{x^3+x} \phantom{+1} \\ 0 \end{array}$$

b)  $x^5 + x^4 + x^3 + 2x^2 + 2x + 1$

$$\begin{array}{r} x^3+x^2+x+1 \overline{) x^5+x^4+x^3+2x^2+2x+1} \\ \underline{x^5+x^4+x^3+x^2} \phantom{+1} \\ x^2+2x+1 \end{array}$$

$$x^5 + x^4 + x^3 + 2x^2 + 2x + 1 = (x^3 + x^2 + x + 1)(x^2) + (x^2 + 2x + 1)$$

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

$$\begin{array}{r} x+2 \\ x^2+2x+1 \overline{) x^3+x^2+x+1} \\ \underline{x^3+2x^2+x} \phantom{+1} \\ 2x^2+1 \\ \underline{2x^2+x+2} \\ 2x+2 \end{array}$$

$$x^2 + 2x + 1 = (2x + 2)(2x + 2) + 0$$

$$\boxed{2x+2}$$

$$\begin{array}{r} 2x+2 \\ 2x+2 \overline{) x^2+2x+1} \\ \underline{x^2+x} \phantom{+1} \\ x+1 \\ \underline{x+1} \\ 0 \end{array}$$



$$\textcircled{5} H(P) = \left( \frac{1}{4} \log_2 \frac{1}{4} + \frac{1}{4} \log_2 \frac{1}{4} + \frac{1}{2} \log_2 \frac{1}{2} \right) = 1.5$$

$$H(K) = 1.5$$

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

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

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

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

$$H(c) = - \left( \frac{1}{2} \log_2 \frac{1}{2} + \frac{1}{4} \log_2 \frac{1}{4} + \frac{1}{8} \log_2 \frac{1}{8} + \frac{1}{8} \log_2 \frac{1}{8} \right) = 1.75$$

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

$$H(K|C) = 1.5 + 1.5 - 1.75 = \boxed{1.25}$$