1 Let $a, b, n \in \mathbb{Z}$.

Assume $a \equiv b \pmod{n}$, show $b \equiv a \pmod{n}$

Since $a \equiv b \pmod{n}$, $\exists k_1 \in \mathbb{Z}$ such that $a - b = k_1 n$

Want to find some $k_2 \in \mathbb{Z}$ such that $b - a = k_2 n$

Because the subtraction operation is symmetric, observe $a - b = b - a$. Therefore, we have

$$a - b = b - a = k_1 n$$

So choose $k_2 = k_1$ and see that, since $\exists k_2 \in \mathbb{Z}$ such that $b - a = k_2 n$, $b \equiv a \pmod{n}$, and the property holds. ∎

Let $a, b, c, n \in \mathbb{Z}$. Assume $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Show $a \equiv c \pmod{n}$.

Since $a \equiv b \pmod{n}$, $\exists k_1 \in \mathbb{Z}$ such that $a - b = k_1 n$.

Since $b \equiv c \pmod{n}$, $\exists k_2 \in \mathbb{Z}$ such that $b - c = k_2 n$.

We want to find some $k_3 \in \mathbb{Z}$ such that $a - c = k_3 n$.

Proceed by adding these two equations:

$$\begin{aligned} a - b &= k_1 n \\ b - c &= k_2 n \\ \hline a - c &= n(k_1 + k_2) \end{aligned}$$

By choosing $k_3 = (k_1 + k_2)$, see that $a \equiv c \pmod{n}$, and the transitivity property holds. ∎

2 Find multiplicative inverse w/ EEC:

a) $1234 \bmod 4321$

Want: int y such that $1234y \equiv 1 \pmod{4321}$

Start w/ Euclidean alg:

$4321 = 1234(3) + 619$

$1234 = 619(1) + 615$

$619 = 615(1) + 4$

$615 = 4(153) + 3$

$4 = 3(1) + 1 \implies \gcd(1234, 4321) = 1$

$3 = 1(3) + 0$

$1 = 4 - 3(1) \implies 3 = 615 - 4(153)$

$= 4 - (615 - 4(153))$

$= 4(154) - 615 \implies 4 = 619 - 615$

$= 154(619 - 615) - 615$

$= 619(154) - (155)615 \implies 615 = 1234 - 619$

$= 619(154) - 155(1234 - 619)$

$= 619(309) - 1234(155) \implies 619 = 4321 - 1234(3)$

$= 309(4321 - 1234(3)) - 1234(155)$

$1 = 4321(309) - 1234(1082)$

∴ since $4321x \equiv 0 \pmod{4321}$ for any x, see that:

$1234^{-1} \pmod{4321} \equiv -1082 \equiv \boxed{3239 \pmod{4321}}$

b) $24140 \bmod 40902$

$40902 = 24140(1) + 16762$

$24140 = 16762(1) + 7378$

$16762 = 7378(2) + 2006$

$7378 = 2006(3) + 1360$

$2006 = 1360(1) + 646$

$1360 = 646(2) + 68$

$646 = 68(9) + \boxed{34}$

$68 = 34(2) + 0$

$\therefore$ $\gcd(24140, 40902) = 34$

since 24140, 40902 are not relatively prime, 24140^{-1} does not exist mod 40902.

c) 550 mod 1769

$1769 = 550(3) + 119$

$550 = 119(4) + 74$

$119 = 74(1) + 45$

$74 = 45(1) + 29$

$45 = 29(1) + 16$

$29 = 16(1) + 13$

$16 = 13(1) + 3$

$13 = 3(4) + 1$ $\Rightarrow \gcd(550, 1769) = 1$

$3 = 1(3) + 0$

$1 = 13 - 3(4)$ $\Rightarrow 3 = 16 - 13(1)$

$= 13 - 4(16 - 13)$

$= 13(5) - 16(4)$ $\Rightarrow 13 = 29 - 16(1)$

$= 5(29 - 16) - 16(4)$

$= 29(5) - 16(9)$ $\Rightarrow 16 = 45 - 29$

$= 29(5) - 9(45 - 29)$

$= 29(14) - 45(9)$ $\Rightarrow 29 = 74 - 45$

$= 14(74 - 45) - 45(9)$

$= 74(14) - 45(23)$ $\Rightarrow 45 = 119 - 74$

$= 74(14) - 23(119 - 74)$

$= 74(37) - 119(23)$ $\Rightarrow 74 = 550 - 119(4)$

$= 37(550 - 119(4)) - 119(23)$

$= 550(37) - 119(171)$ $\Rightarrow 119 = 1769 - 550(3)$

$= 550(37) - 171(1769 - 550(3))$

$1 = 550(550) - \underbrace{1769(171)}_{\equiv 0 \pmod{1769}}$

$\Rightarrow$ 550 is its own multiplicative inverse mod 1769.

3 determine which are reducible over GF(2)

a) $x^3+1 = (x+1)(x^2-x+1)$ $\Rightarrow$ reducible

b) x^3+x^2+1 in GF(2), this polynomial has no roots. Therefore, it is irreducible.

[Thm: if deg[x] = 2 or 3, then f(x) is reducible in F(x) iff f(x) has a zero in F]

since (b) has no roots in GF(2), it is irreducible.

https://math.dartmouth.edu/archive/m31w05/public_html/Reducibility.pdf

c) $x^4+1 = (x+1)^4$ $\Rightarrow$ reducible over GF(2), not $\mathbb{Q}$

4 find GCD:

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

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

$$-x^3 \qquad +x$$

$$+1$$

$\Rightarrow (x(x^2+1) = x^3+x)$

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

$\therefore GCD(x^3-x+1,\ x^2+1)$ over $GF(2) = 1$

b)

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

x^2

$-(x^5+x^4+x^3+x^2)$

$-2x^2-x+1$

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

$-2x$

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

$-x^2+0x+1$

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

$2x-1$

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

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

$-2x+1$

$-(-2x+1)$

0

$\therefore \gcd(x^3+x^2+x+1,\ x^5+x^4+x^3-x^2-x+1) = 2x-1$ over $GF(3)$

5 Cryptosystem $\{P, K, C, E, D\}$ where:

$P = \{a, b, c\}$ with:

$P_p(a) = \frac{1}{4}$ $\quad P_p(b) = \frac{1}{4}$ $\quad P_p(c) = \frac{1}{2}$

$K = (k_1, k_2, k_3)$ with:

$P_K(k_1) = \frac{1}{2}$ $\quad P_K(k_2) = \frac{1}{4}$ $\quad P_K(k_3) = \frac{1}{4}$

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

$e_{k_1}(a) = 1$ $\quad e_{k_1}(b) = 2$ $\quad e_{k_1}(c) = 1$

$e_{k_2}(a) = 2$ $\quad e_{k_2}(b) = 3$ $\quad e_{k_2}(c) = 1$

$e_{k_3}(a) = 3$ $\quad e_{k_3}(b) = 2$ $\quad e_{k_3}(c) = 4$

$e_{k_4}(a) = 3$ $\quad e_{k_4}(b) = 4$ $\quad e_{k_4}(c) = 4$

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

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

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

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

$P_p(a|1) = \frac{\left(\frac{1}{2} \cdot \frac{1}{4}\right)}{\left(\frac{1}{2}\right)} = \frac{1}{4}$ $\quad P_p(b|1) = 0$ $\quad P_p(c|1) = \frac{\left(\frac{1}{2} \cdot \frac{1}{2}\right) + \left(\frac{1}{2} \cdot \frac{1}{4}\right)}{\frac{1}{2}} = \frac{3}{4}$

$P_p(a|2) = \frac{1}{4}$ | $P_p(b|2) = \frac{3}{4}$ | $P_p(c|2) = 0$

$P_p(a|3) = \frac{1}{2}$ | $P_p(b|3) = \frac{1}{2}$ | $P_p(c|3) = 0$

$P_p(a|4) = 0$ | $P_p(b|4) = 0$ | $P_p(c|4) = 1$

$$H(P) = -\left(\frac{1}{4}\log_2\frac{1}{4} + \frac{1}{4}\log_2\frac{1}{4} + \frac{1}{2}\log_2\frac{1}{2}\right) = \frac{3}{2}$$

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

$$H(C) = -\left(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{4}\log_2\frac{1}{4} + \frac{1}{8}\log_2\frac{1}{8} + \frac{1}{8}\log_2\frac{1}{8}\right) = \frac{7}{4}$$

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

$$= \frac{3}{2} + \frac{3}{2} - \frac{7}{4} = \boxed{\frac{5}{4}}$$

} => assumes cryptosystem is correct, which it isn't

$H(K|C)$ for an "incorrect" cryptosystem, following model posted to Piazza:

$$H(K|C) = -\left(\frac{1}{2}\left(\frac{1}{4}\log_2\frac{1}{4} + 0\log_2 0 + \frac{3}{4}\log_2\frac{3}{4}\right) +\right.$$

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

$$\left.\frac{1}{8}\left(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2} + 0\log_2 0\right) +\right.$$

$$\frac{1}{8}\left(0\log_2 0 + 0\log_2 0 + 1\log_2 1\right)\Big)$$

$$H(K|C) \approx 0.7334$$