Jhonin Cim HW1 →

1a) $633 = 5(153) + 21$

$153 = 7(21) + 6$

$21 = 3(6) + 3$

$6 = 2(3)$

$\boxed{GCD = 3}$

b) $52 = 3(15) + 7 \rightarrow 7 = 52 - 3(15)$

$15 = 2(7) + 1$

$7 = 7(1)$

$GCD = 1$

$1 = 15 - 2(7)$

$3 = 3(15) - 6(7)$

$3 = 3(15) - 6(52 - 3(15))$

$3 = 3(15) - 6(52) + 18(15)$

$3 = -6(52) + 21(15)$

$\boxed{a = -6}$

$\boxed{b = 21}$

2a) $5a + 23 = 6 \bmod 499$

$5a = -17 \bmod 499$

$5a = 482 \bmod 499$

$a = 5^{-1}(482) \bmod 499$

$a = 5^{-1}$

$\gcd(499, 5) = 1$

$\gcd(5, 4) = 1$

$499 = 99(5) + 4$

$5 = (1)(4) + 1$

$4 = (4)(1)$

↓ gcd

$\gcd(4, 1) = 1$

$5x + 499y = 1$

↓

$1 = 5 - (1)(4) \qquad 4 = 499 - 99(5)$

$1 = 5 - (499) - 99(5)$

$1 = 5 - 499 + 99(5)$

$1 = (100)(5) - 499$

$x = 100$

$y = -1$

$x \equiv 100 \bmod 499$

$a = 100 \bmod 499 \times 482 \bmod 499$

$a = 48200 \bmod 499$

$\boxed{a = 296 \bmod 499}$

b) $9a \equiv -78 \bmod 81$

$9a \equiv 3 \bmod 81$

$a = 9^{-1}(3 \bmod 81)$

$x = 9^{-1}$

No solution

~~mod gcd(81,~~ $\gcd(81, 9) = 9 \neq 1$ ×

c. $b - 3a = 4 \bmod 37$

$-3b + 39a = -12 \bmod 37$

$+ \quad 30a + 3b = 0 \bmod 37$

$69a = -12 \bmod 37$

$69a = 25 \bmod 37$

$a = 69^{-1}(25 \bmod 37)$

$\gcd(69, 37) = 1$

$\gcd(37, 32) = 1$

$\gcd(32, 5) = 1$

$\gcd(5, 2) = 1$

$\gcd(2, 1) = 1$

$69 = (1)(37) + 32 \quad 32 = 69 - (1)37$

$37 = (1)32 + 5 \quad 5 = 37 - (1)(32)$

$32 = 6(5) + 2 \rightarrow 2 = 32 - 6(5)$

$5 = 2(2) + 1$

$2 = 2(1)$

$1 = 5 - 2(2)$

$1 = 5 - 2(32 - 6(5))$

$1 = 5 - 2(32) + 12(5)$

$1 = 13 - 2(69 - 37) + 13(37 - 32)$

$1 = 13 - 2(69) + 2(37) + 13(37) + 13(37)$

$1 = 13 - 2(69) + 15(37) + 13(69 - 37)$

$1 = 13(69) - 2(37)$

$1 = -15(69) + 28(37)$

$a = -15(25) \bmod 37$

$-32 \bmod 37$

$960 \bmod 37 + 3b = 0 \bmod 37$

$3b = -960 \bmod 37$

$3b = 2 \bmod 37$

$b = 3^{-1}(2) \bmod 37$

$\gcd(37, 3) = 1$

$\gcd(3, 1) = 1$

$b = -12 \bmod 37$

$37 = 12(3) + 1$

$1 = 37 - 12(3)$

$-12(2) \bmod 37 = -24 \bmod 37$

$\equiv 13 \bmod 37$

$a = 32 \bmod 37$

$b = 13 \bmod 37$

3a) - $\gcd(a,b) = \gcd(b,a)$ b/c of commutative property of GCD

- $\gcd(b,a) = \gcd(a, b \bmod a)$

$\gcd(a,b')$ due to substitution

- Thus if it is given that $\gcd(a,b)=1$ b/c they are relatively prime, $\gcd(a,b') = \gcd(a,b) = 1$ so a, b' must be relatively prime

b) - If $a|c$ there exists some $d \in \mathbb{Z}$ such that $ad = c$

- If $b|c$ there exists some $f \in \mathbb{Z}$ such that $bf = c$

- If $\gcd(a,b) = ax + by = 1$ for some $x, y \in \mathbb{Z}$

- $d(ax+by) = d(1)$

$adx + bdy = d(1-1) = 1 \ominus 1$

$c = b$

$cx + bdy = d$

$bfx + bdy = d$

$b(fx + dy) = d$

$c = ad = ab(fx+dy)$

$\therefore ab|c$

4a) $(a \ominus b) \oplus (b \ominus a)$

$= ((a-b) + (b-a)) \bmod n$

$= 0 \bmod n = 0$

Thus $(a \ominus b) \oplus (b \ominus a) = 0$

b) Assume $a \otimes b = 0 \rightarrow b \neq 0 \wedge a \neq 0$

- because negating $p \rightarrow q$ statement requires negating q. (proof by contradiction).
- If $b \neq 0 \wedge a \neq 0$, then $a \otimes b \neq 0$.
- This contradicts our true assumption of $a \otimes b = 0$.
- $\therefore$ $a \otimes b = 0 \rightarrow a = 0$ or $b = 0$.

5a) (counterexample) $a \oplus b$

~~$2 \oplus (n-2) = 0$ is not invertible~~

$2 \oplus (n-2) = (2 + n - 2) \bmod n$ not invertible.

$= n \bmod n = 0$

Counterexample: $a \ominus b$

$1 \ominus 1 = (1-1) \bmod n = 0 \bmod n$

Not invertible.

b) $a \otimes b$ is invertible

- $a \otimes b = (a \cdot b) \bmod n$
- $(a \otimes b) \otimes (b^{-1} \otimes a^{-1})$

↓

- $(a \cdot b \cdot b^{-1} \cdot a^{-1}) \bmod n = 0$

$= 1 \bmod n = 1$ $\therefore$

c). $a \otimes b$ is invertible

- [illegible]
- $a \otimes b = a \otimes b^{-1}$
- $(a \otimes b^{-1})^{-1} = (b \otimes a^{-1})$
- $(a \otimes b^{-1}) \otimes (b \otimes a^{-1}) =$

$(a \times b^{-1} \times b \times a^{-1}) \bmod n = 1 \bmod n$

$= 1$

$\therefore$ $a \otimes b$ is invertible.