1. $A = \{0, 1\}$

- boolean and

0&1 = 0 ✓

It is closure, 0 & 1 = 1 & 0 (associativity)

identity element : 1

1 & 1 = 1

0 & 1 = 0 ✓

inverse element : 1 & 1 = 1

Cannot Form a Group

0 & ? = 0 — can't be 1

- boolean or

0 || 1 = 1 ✓

It's closure, 0 or 1 = 1 or 0

identity element: 0

1 or 0 = 1

0 or 0 = 0

inverse element:

There's no inverse element that can or with 1 to get 0.

Cannot Form a Group

- boolean xor

0 xor 1 = 1 ✓

It's closure, 0 xor 1 = 1 xor 0

identity element : 0

0 xor 0 = 0

1 xor 0 = 1

Can Form a Group

inverse element : 0 xor 0 = 0

1 xor 1 = 0 it is itself.

累了，用饭团外卖搞劳自己

2. No. GCD(w1, x), GCD(w2, x) .....

closure : the greatest common divider of any two unsigned number will be an unsigned integer.

Associativity: GCD(w1, x) = GCD(x, w1) ✓

identity element: 0, GCD(w, 0) would be w

inverse element : The smallest number of gcd is 1, which can't be 0. So No.

3.

If it switch, it became $\{R, \times, +\}$

1. Closure with additive + ?

$a+b = b+a$ ✓

2. associativity with additional +

$(a+b)+c = a+(b+c)$ ✓

3. distribute over operator +

$(a+b)\times c = a\times c + b\times c$

$a\times(b+c) = a\times b + a\times c$

} Ring property

4. closure with multiplicate

$ab = ba$

5. associativity with ×

$a(bc) = (ab)c$

6. identity element : 1

$a\times 1 = a$

$b\times 1 = b$

7. inverse element : it power -1.

$a\times a^{-1} = 1$

$b\times b^{-1} = 1$

Yes, it would still be Ring

累了，用饭团外卖搞劳自己

4. Z_{97}

$\gcd(\overline{4}, \overline{97})^{\overline{4}}$

$= \gcd(\overline{97}, \overline{4}) = \gcd(\overline{4}, 5)$ | residue $5 = \overline{1\times 97} - \overline{2\times 4}$

$= \gcd(5, 2)$ | $2 = \overline{1\times 4} - 9\times 5$

$= \overline{1\times 4} - 9\times(\overline{1\times 97} - \overline{2\times 4})$

$= \gcd(2, 1)$

residue $1 = 1\times 5 - 2\times 2$

$= 1\times(\overline{1\times 97} - \overline{2\times 4}) - 2\times(\overline{1\times 4} - 9\times(\overline{1\times 97} - \overline{2\times 4}))$

$= (\overline{1\times 97} - \overline{2\times 4}) - 2\times(\overline{1\times 4} - \overline{9\times 97} + \overline{18\times 4})$

$= \overline{1\times 97} - \overline{2\times 4} - \overline{2\times 4} + \overline{18\times 97} - \overline{39\times 4}$

$= \overline{19\times 97} + \overline{(-43)\times 4}$

$= \boxed{\overline{54}\times 4} + \overline{19\times 97}$

5. (a) $28x \equiv 34 \pmod{37}$

$x = \frac{1}{28} \cdot 34 \pmod{37}$

MI of 28 in Z_{37} is 4

gcd(37, 28)

= gcd(28, 9) $9 = 1\times37 - 1\times28$

= gcd(9, 1) $1 = 1\times28 - 3\times9$

$= 1\times28 - 3\times(1\times37 - 1\times28)$

$= 1\times28 - 3\times37 + 3\times28$

$= 4\times28 + (-3)\times37$

$= \boxed{4}\times28 + 34\times37$

$x = 4 \cdot 34 \pmod{37}$

$= 136 \pmod{37} = \boxed{25}$

b) $19x \equiv 42 \pmod{43}$

$x = \frac{1}{19}\, 42 \pmod{43}$

gcd(43, 19)

= gcd(19, 5) $5 = 1\times43 - 2\times19$

= gcd(5, 4) $4 = 1\times19 - 3\times5$

$= 1\times19 - 3\times(1\times43 - 2\times19)$

= gcd(4, 1) $1 = 1\times5 - 1\times4$

$= 1\times5 - 1\times19 + 3\times(1\times43 - 2\times19)$

$= 1\times5 - 1\times19 + 3\times43 - 6\times19$

$= 1\times43 - 2\times19 - 1\times19 + 3\times43 - 6\times19$

$= 4\times43 - 9\times19 = 4\times43 + 34\times19$

MI of 19 is 34

$x = 34\times42 \pmod{43}$

$= 1428 \pmod{43}$

$= \boxed{9}$

c) $54x \equiv 69 \pmod{79}$

gcd(54, 79)

= gcd(79, 54)

= gcd(54, 25) $25 = 1\times79 - 1\times54$

= gcd(25, 4) $4 = 1\times54 - 2\times25 = 1\times54 - 2\times(1\times79 - 1\times54)$

= gcd(4, 1) $1 = 1\times25 - 6\times4$

$= 1\times79 - 1\times54 - 6\times(1\times54 - 2\times(1\times79 - 1\times54))$

$= 1\times79 - 1\times54 - 6\times(1\times54 - 2\times79 + 2\times54)$

$= 1\times79 - 1\times54 - 6\times54 + 12\times79 - 12\times54$

$= 13\times79 - 19\times54$

$= 13\times79 + \boxed{60}\times54$

$x = 60\times69 \pmod{79}$

$= 4140 \pmod{79}$

$= \boxed{32}$

d) $153x = 182 \pmod{271}$

$\gcd(271, 153)$

$= \gcd(153, 118)$ $\quad 118 = 1\times271 - 1\times153$

$= \gcd(118, 35)$ $\quad 35 = 1\times153 - 1\times118$

$= 1\times153 - 1\times271 + 1\times153$

$= 2\times153 - 1\times271$

$= \gcd(35, 13)$ $\quad 13 = 1\times118 - 3\times35$

$= 1\times271 - 1\times153 - 3\times(2\times153 - 1\times271)$

$= 1\times271 - 1\times153 - 6\times153 + 3\times271$

$= 4\times271 - 7\times153$

$= \gcd(13, 9)$ $\quad 9 = 1\times35 - 2\times13$

$= 1\times35 - 2\times(4\times271 - 7\times153)$

$= 1\times35 - 8\times271 + 14\times153$

$= 2\times153 - 1\times271 - 8\times271 + 14\times153$

$= 16\times153 - 9\times271$

$= \gcd(9, 4)$ $\quad 4 = 1\times13 - 1\times9$

$= 4\times271 - 7\times153 - 16\times153 + 9\times271$

$= 13\times271 - 25\times153$

$= \gcd(4, 1)$ $\quad 1 = 1\times9 - 2\times4$

$= 16\times153 - 9\times271 - 2\times(13\times271 - 25\times153)$

$= 16\times153 - 9\times271 - 26\times271 + 50\times153$

$= \boxed{66}\times153 - 35\times271$

$x = 66\times182 \pmod{271}$

$= 12012 \pmod{271}$

$= \boxed{88}$

累了，用饭团外卖搞劳自己

e) $672x = 836 \pmod{997}$

$\gcd(672, 997)$ $\quad 325 = 1\times997 - 1\times672$

$= \gcd(997, 672)$ $\quad 22 = 1\times672 - 2\times325$

$= \gcd(672, 325)$

$= 1\times672 - 2\times(1\times997 - 1\times672)$

$= 1\times672 - 2\times997 + 2\times672$

$= 3\times672 - 2\times997$

$= \gcd(325, 22)$ $\quad 17 = 1\times325 - 14\times22$

$= 1\times997 - 1\times672 - 14\times(3\times672 - 2\times997)$

$= 1\times997 - 1\times672 - 42\times672 + 28\times997$

$= 29\times997 - 43\times672$

$= \gcd(22, 17)$ $\quad 5 = 1\times22 - 1\times17$

$= 3\times672 - 2\times997 - 29\times997 + 43\times672$

$= 46\times672 - 31\times997$

$= \gcd(17, 5)$ $\quad 2 = 1\times17 - 3\times5$

$= 29\times997 - 43\times672 - 3\times(46\times672 - 31\times997)$

$= 29\times997 - 43\times672 - 138\times672 + 93\times997$

$= 122\times997 - 181\times672$

$= \gcd(5, 2)$ $\quad 1 = 1\times5 - 2\times2$

$= 46\times672 - 31\times997 - 2\times(122\times997 - 181\times672)$

$= 46\times672 - 31\times997 - 244\times997 + 362\times672$

$= \boxed{408}\times672 - 275\times997$

$= \gcd(2, 1)$

$x = 408\times836 \pmod{997}$

$= 341088 \pmod{997}$

$= \boxed{114}$

6. $(54x^{10}-62x^9-84x^8+70x^7-75x^6+x^5-50x^3+84x^2+65x+78)+(-67x^9+44x^8-26x^7-37x^6+61x^5+68x^4+22x^3+74x^2+87x+38)$

$=54x^{10}-62x^9-84x^8+70x^7-75x^6+x^5-50x^3+84x^2+65x+78-67x^9+44x^8-26x^7-37x^6+61x^5+68x^4+22x^3+74x^2+87x+38$

$=54x^{10}-62x^9-67x^9-84x^8+44x^8+70x^7-26x^7-76x^6-37x^6+62x^5+68x^4-50x^3+22x^3+84x^2+74x^2+65x+87x+78+38$

$=54x^{10}+49x^9+49x^8+44x^7+65x^6+62x^5+68x^4+61x^3+69x^2+63x+27$

累了，用饭团外卖搞劳自己

7. GF(11)

$(8x^3+6x^2+8x+1)\times(3x^3+9x^2+7x+5)$

$=24x^6+18x^5+24x^4+3x^3+72x^5+54x^4+72x^3+9x^2+56x^4+42x^3+56x^2+7x+40x^3+30x^2+40x+5$

$=2x^6+90x^5+134x^4+151x^3+95x^2+47x+5$

$=2x^6+2x^5+2x^4+3x^3+7x^2+3x+5$

8.

a). $(x^2+x+1) \times (x^2+x) \bmod (x^3+x+1)$

$= (x^4+x^3+x^2+x^3+x^2+x) \bmod (x^3+x+1)$

$= (x^4+x) \bmod (x^3+x+1)$

$= x - \frac{x^2}{x^3+x+1} = -x^2$

$= \boxed{x^2}$

$$\begin{array}{r} x \\ x^3+x+1 \overline{)\, x^4+x} \\ x^4+x^2+x \\ \hline -x^2 \end{array}$$

b). $x^2 - (x^2+x+1) \bmod (x^3+x+1)$

$= -x-1 \bmod (x^3+x+1)$

$= -x-1 = \boxed{x+1}$

c) $\dfrac{x^2+x+1}{x^2+1} \mod (x^3+x+1)$

$= \boxed{1+\dfrac{x}{x^2+1}}$

$$
\begin{array}{r|l}
 & 1+\dfrac{x}{x^2+1} \\
\cline{2-2}
x^2+1 & x^2+x+1 \\
 & x^2+1 \\
\cline{2-2}
 & x
\end{array}
$$