Workout Problems

Saturday, January 28, 2023 2:15 PM

1. Show whether or not the set of remainders Z_{18} forms a group with the modulo *addition* operator. Then show whether or not Z_{18} forms a group with the modulo *multiplication* operator.

group - {G, ∘}

- closure
  - a∘b = c, a,b,c in set
- associativity
  - (a∘b)∘c = a∘(b∘c)
- identity element
  - a∘i = a for all a in set
- inverse element
  - a∘b = i for all a,b in set

$(a+b) \bmod 18 = c \bmod 18$

$a+b \equiv c \bmod 18$

$Z_{18} = \{0, 1, 2, \ldots, 16, 17\}$

Modulo Addition Group

✓ - closure
  - $(a+b) \bmod 18 = c \bmod 18$
  - or $a+b \equiv c \bmod 18$
  - True for all $a+b = c < 18$
    - ex. $4+5 = 9$ where $9 \in Z_{18}$
  - True for $a+b = c > 18$
    - ex. $15+7 = 22$, although $22 \notin Z_{18}$, but we know $22 \bmod 18 = 4$ where $4 \in Z_{18}$

✓ - associativity
  - From lecture 5.3
    - $\lceil \ldots \rceil \bmod 18 = \lceil a+(b+c) \rceil \bmod 18$

- From lecture 5.5
  - $[(a+b)+c] \bmod 18 = [a+(b+c)] \bmod 18$ is true for all Z_n

✓ - identity element
  - $(a+i) \bmod 18 = a$ for all $a \in Z_{18}$
  - True for identity element $i = 0$
    - $(a+0) \bmod 18 = a \bmod 18 = a$

✓ - inverse elements
  - $(a+b) \bmod 18 = i$, for $a \in Z_{18}$ some $b \in Z_{18}$
  - True for identity element $i = 0$, where b is the additive inverse of a.
    - $(a + a.i(a)) \bmod 18 = 0$

      $(a + (18-a)) \bmod 18 = 0$

      $18 \bmod 18 = 0$

∴ Z_{18} forms a group w/ modulo addition operation

Modulo Multiplication Group

✓ - closure
  - $(a \cdot b) \bmod 18 = c \bmod 18$, $a, b, c \in Z_{18}$
  - or $a \cdot b \equiv c \bmod 18$
  - True for all $a \cdot b = c > 18$
    - ex. $3 \cdot 5 = 15 \in Z_{18}$
  - True for all $a \cdot b = c > 18$
    - ex. $5 \cdot 6 = 30 \notin Z_{18}$

      however $30 \bmod 18 = 12$

      and $12 \in Z_{18}$

✓ - associativity

✓ - associativity
  - From lecture 6.3
    - $[(w \cdot x) \cdot y] \bmod n = [w \cdot (x \cdot y)] \bmod n$
      for all Z_n

✓ - identity element
  - $(a \cdot i) \bmod 18 = a$, some i $\forall a \in Z_{18}$
    - True for identity element $i = 1$, which $\in Z_{18}$
    - $a \cdot 1 \bmod 18 = a$, $a = a$

✗ - inverse element (b)
  - $(a \cdot b) \bmod 18 = i$, some i $\forall a \in Z_{18}$ and some $b \in Z_{18}$
  - There doesn't exist some $i = 1$ $\forall a \in Z_{18}$, when b is the inverse element
    - $\forall a \in Z_{18}$ there does not exist a m.i. since 18 is not prime and then $\forall a$, not all a will be relatively prime

∴ Z_{18} does not form a group on the modulo multiplication operator

2. Is the set of all unsigned integers W a group under the $gcd(\cdot)$ operation? Why or why not?
Hint: Find the identity element for $\{W, gcd(\cdot)\}$

unsigned integer : { 0, 1, 2, ... , ~4 million }

gcd(x,y) mul(x,y)?

- identity element
  - a o i = a for all a in set
- inverse element
  - a o b = i for all a, b in set

gcd(a,0) = a

gcd(a,b) = 0

We know identy element for

We know identity element for gcd(·) is 0

- gcd(a, 0) = a always

Since i = a, there can be no inverse element

- gcd(a, b) = 0 cannot exist as no number can have a gcd of 0

∴ W is not a group under the gcd(·)

gcd(a, b) = 0

Impossible

3. Compute $gcd(10946, 19838)$ using Euclid's algorithm. Show all of the steps.

gcd(10946, 19838):

= gcd(19838, 10946) 19838 % 10946 = 8892

= gcd(10946, 8892) 10946 % 8892 = 2054

= gcd(8892, 2054) 8892 % 2054 = 676

= gcd(2054, 676) 2054 % 676 = 26

= gcd(676, 26) 676 % 26 = 0

= gcd(26, 0)

∴

gcd(10946, 19838) = 26

$$\begin{array}{r} 2^{3}\,8^{1}54 \\ -\quad 4 \\ \hline 8\,2\,6 \end{array}$$

4. Use the Extended Euclid's Algorithm to compute by hand the multiplicative inverse of 19 in Z_{35}. List all of the steps.

35 % 19 = 16

$19 \% 16 = 3$

$16 \% 3 = 1$

$\gcd(19, 35)$

$= \gcd(35, 19)$

$= \gcd(19, 16)$ | residue $16 = 1 \times 35 - 1 \times 19$

$= \gcd(16, 3)$ | residue $3 = 1 \times 19 - 1 \times 16$

$= 1 \times 19 - (1 \times 35 - 1 \times 19)$

$= 2 \times 19 - 1 \times 35$

$= \gcd(3, 1)$ | residue $1 = 1 \times 16 - 5 \times 3$

$= 1 \times 35 - 1 \times 19 - 5(2 \times 19 - 1 \times 35)$

$= 1 \times 35 - 1 \times 19 - 10 \times 19 + 5 \times 35$

$= 6 \times 35 - 11 \times 19$

a.i

$-11 + 35 = 24$

$m.i(19) \mod 35 = 24$

5. In the following, find the smallest possible integer x. Briefly explain (i.e. you don't need to list out all of the steps) how you found the answer to each. You should solve them *without* simply plugging in arbitrary values for x until you get the correct value:

   (a) $6x \equiv 3 \pmod{23}$ a) $x = 12$

   (b) $7x \equiv 11 \pmod{13}$ b) $x = 22$

   (c) $5x \equiv 7 \pmod{11}$ c) $x = 63$

Steps:

- $ax \equiv b \pmod{c}$
- $x \equiv b \cdot \frac{1}{a} \pmod{c}$: basic arithmetic

- $x \equiv b \cdot \frac{1}{a} \pmod{c}$: basic arithmetic
- we know $\frac{1}{a} = m.i(a)$
- $x \equiv b \cdot m.i(a) \pmod{c}$
- solve $m.i(a)$ using euclid extended algorithm
- then with $d = b \cdot m.i(a)$
- $x \equiv d \pmod{c}$
- $x \bmod c = d \bmod c$
- $\boxed{x = d = b \cdot m.i(a)}$

a) $6x \equiv 3 \pmod{23}$

$x \equiv 3 \cdot m.i(6) \pmod{23}$

$m.i(6) \bmod 23 =$

$\gcd(6, 23)$

$= \gcd(23, 6)$

$= \gcd(6, 5)$ | residue 5 $= 1 \times 23 - 3 \times 6$

$= \gcd(5, 1)$ | residue 1 $= 1 \times 6 - 1 \times 5$

$= 1 \times 6 - 1 \times 23 + 3 \times 6$

$= 4 \times 6 - 1 \times 23$

$23 \bmod 6 = 5$

$6 \bmod 5 = 1$

$5 \bmod 1 = 0$

$m.i(6) \bmod 23 = 4$

$x \equiv 3 \cdot m.i(6) \pmod{23}$

$x \equiv 12 \mod(23)$

$\boxed{x = 12}$

b) $7x \equiv 11 \pmod{13}$

$x \equiv 11 \cdot m.i(7) \pmod{13}$

$13 \% 7 = 6$

$7 \% 6 = 1$

$m.i(7) \mod(13)$

$\gcd(7, 13)$

$= \gcd(13, 7)$

$= \gcd(7, 6)$ | residue $6 = 1 \times 13 - 1 \times 7$

$= \gcd(6, 1)$ | residue $1 = 1 \times 7 - 1 \times 6$

$= 1 \times 7 - 1 \times 13 + 1 \times 7$

$= 2 \times 7 - 1 \times 13$

$m.i(7) = 2$ ←

$x \equiv 11 \cdot 2 \mod(3$

$\boxed{x = 22}$

c) $5x \equiv 7 \pmod{11}$

$x \equiv 7 \cdot m.i(5) \pmod{11}$

$11 \% 5 = 1$

gcd(5, 11):

gcd(11, 5)

gcd(5, 1) | residue 1 = 1x 11 − 2x 5

m.i(5): −2 = −2 + 11 = 9

x = 7 · 9 = 63