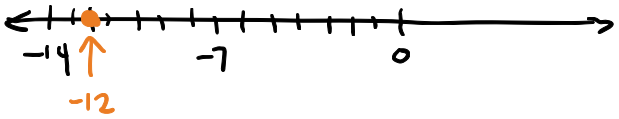
Math 234

Modular Arithmetic and $\mathbf{Z}_n$



Day 24

1. (a) What is the value of 23 (mod 7)?

$23 \equiv 2 \pmod 7$ ↑ congruent

$\{0, 1, 2, 3, 4, 5, 6\}$

(b) What is the value of -12 (mod 7)?

$-12 = -14 + 2$ so $-12 \equiv 2 \pmod 7$

(c) Is it true that 23 (mod 7) $= -12$ (mod 7)?

Yes, since $2 = 2$

(d) Is it true that $23 \equiv 12 \pmod 7$?

No. $2 \neq 5$

23 is 2 more than a multiple of 7, but 12 is 5 more than a multiple of 7

2. Using the facts that $46 \equiv 7 \pmod{13}$ and $17 \equiv 4 \pmod{13}$, using modular arithmetic to efficiently find an integer $0 \leq d \leq 12$ such that

multiples of 13: 13, 26, 39, 52

(a) $63 \equiv d \pmod{13}$. Note that $63 = 46 + 17$.

$63 \equiv 7 + 4 = 11 \pmod{13}$

$63 = (4)13 + 11$

(b) $29 \equiv d \pmod{13}$. Note that $29 = 46 - 17$.

$29 \equiv 7 - 4 = 3 \pmod{13}$

$29 = 2(13) + 3$

(c) $782 \equiv d \pmod{13}$. Note that $782 = 46 \times 17$.

$782 \equiv 7 \cdot 4 = 28 \equiv 2 \pmod{13}$

$782 = 13(60) + 2$
$= 780 + 2$

(d) $143 \equiv d \pmod{13}$. Note that $143 = (2 \times 46) + (3 \times 17)$.

$143 \equiv (2 \times 7) + (3 \times 4) = 14 + 12 = 26 \equiv 0 \pmod{13}$

So $143 \equiv 0 \pmod{13}$

$143 = 11 \cdot 13$

3. Find the units digit of 7^{2022}. Then do the same for 37^{2022}.

mod 10!

Find a pattern:

$7^0 = 1$

$7^1 = 7$

$7^2 = 49 \equiv 9 \pmod{10}$

$7^3 \equiv 3 \pmod{10}$

$7^4 \equiv 1 \pmod{10}$

$9 \cdot 7 = 63$
So $9 \cdot 7 \equiv 3 \pmod{10}$
$7^2 \cdot 7 \equiv 3 \pmod{10}$

$2022 = 4 \cdot 505 + 2$

$7^{2022} = 7^{4 \cdot 505 + 2} = (7^4)^{505} \cdot 7^2$

$\equiv 1^{505} \cdot 7^2 \pmod{10}$

$\equiv 1 \cdot 9$

$7^{2022} \equiv 9 \pmod{10}$

$f: S \times S \to S$

4. Recall that a **binary operation** on a set S is a function from $S \times S$ to S. Determine whether each of the functions below is a binary operation, and if so, identify set set S.

   (a) The logical *or* operation, as in $r \vee s$, where r and s are logical true/false values.

   $S = \{\text{true, false}\}$ $\quv: S \times S \to S$

   $S \times S = \{(T,T),(T,F),(F,T),(F,F)\}$

   Yes!

   (b) The logical *and* operation, as in $r \wedge s$, where r and s are logical true/false values.

   again, $S = \{\text{true, false}\}$ $\quad \wedge: S \times S \to S$ Yes!

r	s	r→s
T	T	T
T	F	F
F	T	T
F	F	T

   (c) The logical implication operation, as in $r \to s$, where r and s are logical true/false values.

   Yes, also a binary operation.

   (d) The numerical less than operation, as in $r < s$, where r and s are real numbers.

   $< : \mathbb{R} \times \mathbb{R} \to \{\text{true, false}\}$ NOT a binary operation

5. Let $\cdot$ be the usual multiplication operation for real numbers in some set S.

   (a) If $S = \mathbf{R}$, is $\cdot$ a binary operation?

   Yes, since the product of two real numbers is a real number.

   (b) If $S = \mathbf{R}^+$, is $\cdot$ a binary operation?

   Yes

   (c) If $S = \mathbf{Z}$, is $\cdot$ a binary operation?

   Yes

   (d) If $S = \mathbf{Z}^-$ (negative integers), is $\cdot$ a binary operation?

   No, since the product of two negative integers is positive.

—CLASS ENDED HERE—

6. Let $+$ be the usual addition operation on real numbers.

   (a) If $A = \{x \mid x > 0\}$, is A closed under $+$?

   Yes: if $x, y \in A$ then $x > 0$ and $y > 0$, so $x + y > 0$ and $x + y \in A$

   (b) If $A = 2\mathbf{Z}$, the set of even integers, is A closed under $+$?

   If $a, b \in A$ then $a = 2k$ and $b = 2m$ for $k, m \in \mathbb{Z}$

   then $a + b = 2k + 2m = 2(k+m) \in A$

   (c) If $A = \{n \in \mathbf{Z} \mid n \text{ is odd}\}$, is A closed under $+$?

   No. Counterexample: $a = 1$, $b = 3$ are in A but $a + b = 2 \notin A$

   (d) If $A = \mathbf{Q}$, is A closed under $+$?

   If $a, b \in \mathbb{Q}$, then $a = \frac{r}{s}$ and $b = \frac{p}{q}$ for $r, s, p, q \in \mathbb{Z}$

   (e) If $A = \mathbf{R} - \mathbf{Q}$, is A closed under $+$?

   then $a + b = \frac{qr + ps}{sq} \in \mathbb{Q}$

   No counterexamples: $\sqrt{2} + (-\sqrt{2}) = 0$

   $\pi + (1 - \pi) = 1$

Properties satisfied by the integers ($\mathbb{Z}$)

- Closed under addition ($+$) and multiplication ($\cdot$)
- **Commutative properties:** $a+b=b+a$ and $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{Z}$
- **Associative properties:** $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathbb{Z}$
- **Distributive property:** $a \cdot (b+c) = a \cdot b + a \cdot c$ for all $a, b, c \in \mathbb{Z}$
- **Identities:** additive identity 0: $a+0=a \quad \forall\, a \in \mathbb{Z}$
  multiplicative identity 1: $a \cdot 1 = a \quad \forall\, a \in \mathbb{Z}$
- **Additive inverses:** $\forall\, a \in \mathbb{Z}$, there exists $b = -a$ such that $a+b=0$

EXAMPLE: integers mod 5 $\quad \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ with $+$ and $\cdot$ modulo 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_5$ with $+$ and $\cdot$ mod 5 is:

$\mathbb{Z}_5$ is a Commutative ring

- Closed under $+$ and $\cdot$
- $+$ and $\cdot$ are commutative: $a+b=b+a$ and $a \cdot b = b \cdot a$
- $+$ and $\cdot$ are associative: $(a+b)+c = a+(b+c)$

  and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Distributive: $a \cdot (b+c) = a \cdot b + a \cdot c$

example:

$3 \cdot (4+2) = 3 \cdot 1 = 3$

$3 \cdot 4 + 3 \cdot 2 = 2 + 1 = 3$

- Additive identity: 0

  Multiplicative identity: 1
- Additive inverses:

a	$-a$
0	0
1	4
2	3
3	2
4	1

example

$1+2\sqrt{2} \in S$

$\frac{3}{4} - \frac{5}{2}\sqrt{2} \in S$

$3+10\sqrt{2} \in S$

7. Let $S = \{q + r\sqrt{2} \mid q, r \in \mathbf{Q}\}$ with the usual addition and multiplication of real numbers. Complete the following to establish that S is a commutative ring.

(a) Show that $+$ and $\cdot$ are commutative.

Let $a = q+r\sqrt{2}$ and $b = u+v\sqrt{2}$. Then:

$$a+b = (q+r\sqrt{2})+(u+v\sqrt{2}) = q+u+(r+v)\sqrt{2} = (u+v\sqrt{2})+(q+r\sqrt{2}) = b+a$$

so $+$ is commutative

Also:

$$a\cdot b = (q+r\sqrt{2})\cdot(u+v\sqrt{2}) = (qu+2rv)+(qv+ru)\sqrt{2} = (u+v\sqrt{2})\cdot(q+r\sqrt{2}) = b\cdot a$$

so $\cdot$ is commutative

(b) Show that $+$ and $\cdot$ are associative.

Let $a = q+r\sqrt{2}$, $b = u+v\sqrt{2}$, and $c = x+y\sqrt{2}$. Then:

$$(a+b)+c = \left[(q+r\sqrt{2})+(u+v\sqrt{2})\right]+(x+y\sqrt{2}) = q+u+x+(r+v+y)\sqrt{2} = (q+r\sqrt{2})+\left[(u+v\sqrt{2})+(x+y\sqrt{2})\right] = a+(b+c)$$

so $+$ is associative

Also:

$$(a\cdot b)\cdot c = \left[(q+r\sqrt{2})\cdot(u+v\sqrt{2})\right]\cdot(x+y\sqrt{2}) = \left[qu+2rv+(qv+ru)\sqrt{2}\right](x+y\sqrt{2}) = (qux+2rvx+2qvy+2ruy)+(qvx+rux+quy+2rvy)\sqrt{2}$$

$$= (q+r\sqrt{2})\cdot\left[ux+2vy+(vy+vx)\sqrt{2}\right] = (q+r\sqrt{2})\cdot\left[(u+v\sqrt{2})\cdot(x+y\sqrt{2})\right] = a\cdot(b\cdot c)$$

so $\cdot$ is associative

(c) Show that $+$ distributes over $\cdot$.

$$(q+r\sqrt{2})\cdot\left[(u+v\sqrt{2})+(x+y\sqrt{2})\right] = (q+r\sqrt{2})\cdot\left[u+x+(v+y)\sqrt{2}\right] = qu+qx+2rv+2ry+(ru+rx+qv+qy)\sqrt{2}$$

$$= \left[qu+2rv+(ru+qv)\sqrt{2}\right]+\left[qx+2ry+(rx+qy)\sqrt{2}\right]$$

$$= (q+r\sqrt{2})\cdot(u+v\sqrt{2})+(q+r\sqrt{2})\cdot(x+y\sqrt{2})$$

(d) Show that S contains an additive identity and a multiplicative identity.

Additive identity: $(0+0\sqrt{2})+(q+r\sqrt{2}) = q+r\sqrt{2}$

Multiplicative identity: $(1+0\sqrt{2})\cdot(q+r\sqrt{2}) = q+r\sqrt{2}$

for all $q, r \in \mathbb{Q}$.

(e) Show that each element of S has an additive inverse.

If $q+r\sqrt{2} \in S$, then $-q+(-r)\sqrt{2} \in S$,

and $(q+r\sqrt{2})+(-q+(-r)\sqrt{2}) = 0+0\sqrt{2}$.

8. Let S be the set of all 2×2 matrices of real numbers. Let $+$ be the usual matrix addition from linear algebra, and define a new "componentwise" multiplication $\star$ as follows:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \star \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae & bf \\ cg & dh \end{bmatrix}$$

(a) Are $+$ and $\star$ commutative? Yes!

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} = \begin{bmatrix} e+a & f+b \\ g+c & h+d \end{bmatrix} = \begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae & bf \\ cg & dh \end{bmatrix} = \begin{bmatrix} ea & fb \\ gc & hd \end{bmatrix} = \begin{bmatrix} e & f \\ g & h \end{bmatrix} * \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

(b) Are $+$ and $\star$ associative? Yes!

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) + \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} x & y \\ z & w \end{bmatrix} \right)$$

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) * \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} * \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} * \begin{bmatrix} x & y \\ z & w \end{bmatrix} \right)$$

(c) Do $+$ and $\star$ satisfy the distributive property? Yes!

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} x & y \\ z & w \end{bmatrix} \right) = \begin{bmatrix} a(e+x) & b(f+y) \\ c(g+z) & d(h+w) \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} x & y \\ z & w \end{bmatrix}$$

(d) Is there an additive identity and a multiplicative identity?

Additive identity: $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

Multiplicative identity: $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

(e) Are there additive inverses?

Yes: $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

(f) Is S with $+$ and $\star$ a commutative ring?

Yes!

9. **BONUS:** Find the units digit of 42^{4017}.

$$42^{4017} \equiv 2^{4017} \equiv (2^4)^{1004} \cdot 2 \equiv 6^{1004} \cdot 2 \equiv 6 \cdot 2 \equiv 2 \pmod{10}$$