Discrete Structures

Number Theory/ Direct proofs
9/20/2022

Topics

- Set operator review
- Closure
- Parity
- Divisibility
- Primes
- Mod
- *Direct* Proofs

Set Review: Identify the operator

$\{1,2,3\}\ ?_0\ \{1,3,4\} = \{2\}$

$\{a,b,c\}\ ?_0\ \{1,4\} = \{a,b,c\}$

$\{1,2,3\}\ ?_1\ \{1,3,4\} = \{1,2,3,4\}$

$\{a,b,c\}\ ?_1\ \{1,4\} = \{1,a,b,c,4\}$

$\{1,2,3\}\ ?_2\ \{1,3,4\} = \{1,3\}$

$\{a,b,c\}\ ?_2\ \{1,4\} = \{\}$

Set Review: Identify the operator

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

$\{a,b,c\} - \{1,4\} = \{a,b,c\}$

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

$\{a,b,c\} \cup \{1,4\} = \{1,a,b,c,4\}$

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

$\{a,b,c\} \cap \{1,4\} = \{\}$

Closure property

Z is closed under addition.

Z is closed under negation.

Z is closed under subtraction.

N is closed under addition.

N is *not* closed under subtraction.

N is *not* closed under negation.

R is not closed under square root$^+$.

R$^+$ is closed under square root$^+$.

Closure property

Z is closed under addition.

Z is closed under negation.

Z is closed under subtraction.

N is closed under addition.

N is *not* closed under subtraction.

N is *not* closed under negation.

R is not closed under square root$^+$.

R$^+$ is closed under square root$^+$.

Does the result of applying the operator *ever* result in a value *outside* the domain?

Yes $\Leftrightarrow$ not closed.

No $\Leftrightarrow$ closed.

Closure property

Closure property

Z is closed under addition. $\forall x,y \in Z, (x + y) \in Z$

Z is closed under negation. $\forall x \in Z, -x \in Z$

Z is closed under subtraction. $\forall x,y \in Z, (x - y) \in Z$

N is closed under addition. $\forall x,y \in N, (x + y) \in N$

N is *not* closed under subtraction. $1, 5 \in N, (1 - 5) \notin N$

N is *not* closed under negation. $5 \in N, (-5) \notin N$

R is not closed under square root$^+$. $-2 \in R, \mathrm{sqrt}(-2) \notin R$

R^+ is closed under square root$^+$.

Closure Property

In this class we may assume

- Laws of algebra
- Equality:
  - $A = B \Leftrightarrow B = A$
  - $A = B \wedge B = C \Rightarrow A = C$
- Substitution:
  - If $A =$ B, you may substitute B wherever there is A.
- that there is no integer between 0 and 1
- that the set of all integers is closed under
  - addition,
  - subtraction,
  - multiplication

Parity

Property of an integer being even or odd.

Parity

Property of an integer being even or odd.

Examples:

127:

354:

999:

-192:

Parity

Property of an integer being even or odd.

Examples:

127: odd

354: even

999: odd

-192: even

Parity

x is even ***iff*** there is some integer k such that $x=2k$

x is odd ***iff*** there is some integer k such that $x=2k+1$

$\forall\ x \in Z, \mathrm{EVEN}(x) \Leftrightarrow \exists\ k \in \mathrm{Z}, x = 2k$

$\forall\ x \in Z, \mathrm{ODD}(x) \Leftrightarrow \exists\ k \in Z, x = 2k + 1$

$$\forall\, x \in Z, \mathrm{EVEN}(x) \Leftrightarrow \exists\, k \in \mathrm{Z}, x = 2k$$

$$\forall\, x \in Z, \mathrm{ODD}(x) \Leftrightarrow \exists\, k \in Z, x = 2k + 1$$

Parity

Property of an integer being even or odd.

Examples:

127 =

354 =

999 =

-192 =

Parity

$$\forall\, x \in Z, \mathrm{EVEN}(x) \Leftrightarrow \exists\, k \in \mathrm{Z}, x = 2k$$

$$\forall\, x \in Z, \mathrm{ODD}(x) \Leftrightarrow \exists\, k \in Z, x = 2k + 1$$

Property of an integer being even or odd.

Examples:

$127 = 2(63) + 1$

$354 = 2(177)$

$999 = 2(499) + 1$

$-192 = 2(-96)$

$8 = 2(4)$

$9 = 2(4) + 1$

$-7 = 2(-4) + 1$

Parity

$\forall\, x \in Z, \mathrm{EVEN}(x) \Leftrightarrow \exists\, k \in \mathrm{Z}, x = 2k$

$\forall\, x \in Z, \mathrm{ODD}(x) \Leftrightarrow \exists\, k \in Z, x = 2k + 1$

0, odd or even?

$$0 = 2(0)$$

$\forall$ a,b $\in$ Z, $\mathrm{EVEN}(6a^2b)$?

$$6a^2b = 2(3a^2b)$$

$\forall$ a,b $\in$ Z, $\mathrm{ODD}(10a + 8b + 1)$?

$$2(5a + 4b) + 1$$

Parity

Is every integer either odd or even?

Divisibility

$5|15$ because $5(3)=15$

$3|10$ is false, because there is no integer z such that $3z=10$

Divisibility

If $n,d \in Z$ then n **is divisible by** d iff $n = d$ times some integer and $d \neq 0$.

$d \mid n$

$\forall\, n,d \in Z$

$$(d \mid n) \Leftrightarrow (\exists\, k \in Z, n = dk \wedge d \neq 0)$$

Divisibility

Equivalent statements:

n is divisible by d

$d \mid n$

n is a multiple of d

d is a factor of n

d is a divisor of n

d divides n

Divisibility

$d \nmid n$ is read "d does not divide n"

Divisibility

a. Is 21 divisible by 3?
    a. Yes, $21 = 3(7)$
b. Does 5 divide 40?
    b. Yes, $40 = 5(8)$
c. Does $7 \mid 42$?
    c. Yes, $42 = 7(6)$
d. Is 32 a multiple of -16?
    d. Yes, $32 = (-16)(-2)$
e. Is 6 a factor of 54?
    e. Yes, $54 = 6(9)$
f. Is 7 a factor of -7?
    f. Yes, $-7 = 7(-1)$

Divisibility

If $k \in Z^{+}$, $k \mid 0$?

Yes, $0 = k(0)$

Prime

An integer n is **prime** if, and only if, $n > 1$ and $\forall$ positive integers r and s, if $n = rs$, then either r or s equals n.

An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

$\forall\, n \in Z, n > 1$

$$\text{PRIME}(n) \Leftrightarrow \forall\, r,s \in Z^+,\ (n{=}rs) \Rightarrow (r = 1 \wedge s = n) \vee (r = n \wedge s = 1)$$

$$\text{COMPOSITE}(n) \Leftrightarrow \exists\, r,s \in Z^+, (n = rs) \wedge (1 < r < n) \wedge (1 < s < n)$$

Primes (informal)

An integer > 1 is **prime** iff its only positive factors are 1 and itself.

An integer > 1 not prime is **composite**.

NOTE:

$\forall\ x \in \mathbb{Z}, x \leq 1 \Rightarrow \neg PRIME(x) \wedge \neg \mathrm{COMPOSITE}(x)$

Prime Examples

13 is prime. Only factors are 1, 13.

51 is composite. $17(3) = 51$

Modular Arithmetic

$5\ mod\ 3 = \ \ 2$

$4\ mod\ 4 = \ \ 0$

$12\ mod\ 5 = 2$

$7\ mod\ 5 = \ \ 2$

$-17\ mod\ 5 = \ 3$ because $-17 = -4(5) + 3$

x mod $m = r$

$x = km + r$, where k is an integer $\wedge\ 0 \leq r < m$

Modular Arithmetic

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
n mod 5	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2

Modular Arithmetic

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
n mod 5	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2

Modular Arithmetic

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
n mod 5	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2

"7 is congruent (equivalent) to 2 modulo 5"

$7 \equiv 2 \pmod{5} \Leftrightarrow 5 \mid (7 - 2)$

$2 \equiv 7 \pmod{5} \Leftrightarrow 5 \mid (2 - 7)$

$m \equiv n \pmod{d} \Leftrightarrow d \mid (m - n)$

Modular Arithmetic

$-8 \equiv 7 \pmod{3}$?

Yes, because $3 \mid (-8 - 7)$

$-8 = -5(3) + 7$

Recall

(1)	$p \Rightarrow \neg z$	assumption
(2)	$z \wedge (p \vee r)$	assumption
(3)	$\neg q$	assumption
$\therefore$	$p \Rightarrow q$	

Recall

(1)	$p \Rightarrow \neg z$	assumption
(2)	$z \land (p \lor r)$	assumption
(3)	$\neg q$	assumption
(4)	z	Specialization (2)
(5)	$\neg p$	Modus Tollens (1,4)
(6)	$\neg p \lor q$	Generalization (5)
$\therefore$	$p \Rightarrow q$	Definition of Implication Equivalence

Direct Proof

$a,b,c \in Z$
a | b
b | c

Prove: for all integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

We must show: $a \mid c$

In other words, we must prove $\exists\ k \in Z$, $c = ak$ by definition of divisibility.

Since $a \mid b$, we know $\exists\ r \in \mathrm{Z}$, $b = ar$

Since $b \mid \mathrm{c}$, we know $\exists\ s \in Z$, $c = bs$

Recall we must show $c = ak$ for some k.

Let us substitute the value for $b = ar$ in $c = bs$: $c = (ar)s$.

By associativity, we can state: $c = a(rs)$.

Since r & s are integers, rs is an integer by the closure property of addition over Z.

Therefore, we have shown that $c = ak$ where $k = rs$ and c is therefore divisible by a.

Direct Proof

Prove: for all integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

integer k (7,8)

Direct Proof

Prove: for all integers *a*, *b*, and *c*, if $a \mid b$ and $b \mid c$, then $a \mid c$.

(1)	$a,b,c \in Z$	Assumption
(2)	$a \mid b$	Assumption
(3)	$b \mid c$	Assumption

integer k (7,8)

Direct Proof

Prove: for all integers *a*, *b*, and *c*, if $a \mid b$ and $b \mid c$, then $a \mid c$.

(1)	$a,b,c \in Z$	Assumption
(2)	$a \mid b$	Assumption
(3)	$b \mid c$	Assumption
(4)	$\exists\ r \in Z, b = ar$	Definition of (2)

integer k (7,8)

Direct Proof

Prove: for all integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

(1)	$a,b,c \in Z$	Assumption
(2)	$a \mid b$	Assumption
(3)	$b \mid c$	Assumption
(4)	$\exists\ r \in Z, b = ar$	Definition of (2)
(5)	$\exists\ s \in Z, c = bs$	Definition of (3)

integer k (7,8)

Direct Proof

Prove: for all integers *a*, *b*, and *c*, if $a \mid b$ and $b \mid c$, then $a \mid c$.

(1)	$a,b,c \in Z$	Assumption
(2)	$a \mid b$	Assumption
(3)	$b \mid c$	Assumption
(4)	$\exists\ r \in Z, b = ar$	Definition of (2)
(5)	$\exists\ s \in Z, c = bs$	Definition of (3)
(6)	$\exists\ s \in Z, c = (ar)s$	Substitution (4,5)

integer k (7,8)

Direct Proof

Prove: for all integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

(1)	$a, b, c \in Z$	Assumption
(2)	$a \mid b$	Assumption
(3)	$b \mid c$	Assumption
(4)	$\exists\ r \in Z, b = ar$	Definition of (2)
(5)	$\exists\ s \in Z, c = bs$	Definition of (3)
(6)	$\exists\ s \in Z, c = (ar)s$	Substitution (4,5)
(7)	$s \in Z, c = a(rs)$	Associativity (6)
		integer k (7,8)

Direct Proof

Prove: for all integers *a*, *b*, and *c*, if $a \mid b$ and $b \mid c$, then $a \mid c$.

(1)	$a,b,c \in Z$	Assumption
(2)	$a \mid b$	Assumption
(3)	$b \mid c$	Assumption
(4)	$\exists\ r \in Z, b = ar$	Definition of (2)
(5)	$\exists\ s \in Z, c = bs$	Definition of (3)
(6)	$\exists\ s \in Z, c = (ar)s$	Substitution (4,5)
(7)	$s \in Z, c = a(rs)$	Associativity (6)
(8)	$(rs) \in Z$	Since $r, s \in Z$ & closure of *
		integer k (7,8)

Direct Proof

Prove: for all integers *a*, *b*, and *c*, if $a \mid b$ and $b \mid c$, then $a \mid c$.

(1)	$a,b,c \in Z$	Assumption
(2)	$a \mid b$	Assumption
(3)	$b \mid c$	Assumption
(4)	$\exists\ r \in Z, b = ar$	Definition of (2)
(5)	$\exists\ s \in Z, c = bs$	Definition of (3)
(6)	$\exists\ s \in Z, c = (ar)s$	Substitution (4,5)
(7)	$s \in Z, c = a(rs)$	Associativity (6)
~~(8)~~	~~$(rs) \in Z$~~	~~Since r, s ∈ Z & closure of *~~
(9)	a | c	By definition of divisibility, since c can be written in terms of a * some integer k (7,8)

Direct Proof

Prove: $(\forall\, x \in Z)$[if x is even, then $3x+7$ is odd]

Assuming $x \in Z \land x$ is even, we must show $3x + 7$ is odd.

In other words, we must show $(\exists\, k \in Z)[3x+7 = 2k + 1]$.

If x is even, $(\exists\, s \in Z)[x = 2s]$.

Let us rewrite: $3x+7 = 3(2s) + 7 = 6s + 7$

$6s + 7 = 6s + 6 + 1 = (6s + 6) + 1 = 2(3s + 3) + 1$.

Therefore, if $(3s + 3)$ is an integer, then $3x + 7 = 2k + 1$ where $k = (3s + 3)$.

We know $3s + 3$ is an integer because s is an integer and +, * are closed on Z.

Therefore, $3x + 7$ is odd because it can be written as $2(3s+3) + 1$.