

# 1 Math

**Defn.** Even and Odd Integers

$n$  is even  $\Leftrightarrow \exists$  an integer  $k$  s.t.  $n = 2k$

$n$  is odd  $\Leftrightarrow \exists$  an integer  $k$  s.t.  $n = 2k + 1$

**Defn.** Divisibility

$n$  and  $d$  are integers and  $d \neq 0$

$d|n \Leftrightarrow \exists k \in \mathbb{Z}$  s.t.  $n = dk$

**Theorem 4.2.1.** Every Integer is a rational number

**Theorem 4.2.2.** The sum of any two rational numbers is rational

**Theorem 4.3.1.** For all  $a, b \in \mathbb{Z}^+$ , if  $a|b$ , then  $a \leq b$

**Theorem 4.3.2.** Only divisors of 1 are 1 and  $-1$

**Theorem 4.3.3.**  $\forall a, b, c \in \mathbb{Z}$  if  $a|b$ ,  $b|c$ ,  $a|c$

**Theorem 4.6.1.** There is no greatest integer

**Proposition.** 4.6.4 For all integers  $n$ , if  $n^2$  is even, then  $n$  is even.

**Defn.** Rational  $r$  is rational  $\Leftrightarrow \exists a, b \in \mathbb{Z}$  s.t.  $r = \frac{a}{b}$  and  $b \neq 0$

**Defn.** Fraction in lowest term: fraction  $\frac{a}{b}$  is lowest term if largest  $\mathbb{Z}$  that divides both  $a$  and  $b$  is 1

**Theorem 4.7.1.**  $\sqrt{2}$  is irrational

## 2 Logic of Compound Statements

**Theorem 3.2.1.** Negation of universal stmt  $\sim (\forall x \in D, P(x)) \equiv \exists x \in D$  s.t.  $\sim P(x)$

**Theorem 3.2.1.** Negation of existential stmt  $\sim (\exists x \in D$  s.t.  $P(x)) \equiv \forall x \in D, \sim P(x)$

**Defn.** Contrapositive of  $p \Rightarrow q \equiv \sim q \Rightarrow \sim p$

**Defn.** Converse of  $p \Rightarrow q$  is  $q \Rightarrow p$

**Defn.** Inverse of  $p \Rightarrow q$  is  $\sim p \Rightarrow \sim q$

**Defn.** Only if:  $p$  only if  $q$  means  $\sim q \Rightarrow \sim p \equiv p \Rightarrow q$

**Defn.** Biconditional:  $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$

**Defn.**  $r$  is sufficient condition for  $s$  means if  $r$  then  $s$ ,  $r \Rightarrow s$

**Defn.**  $r$  is necessary condition for  $s$  means if  $\sim r$  then  $\sim s$ ,  $s \Rightarrow r$

**Defn.** Proof by Contradiction

If you can show that the supposition that statement  $p$  is false leads to a contradiction, then you can conclude that  $p$  is true

### 3 Methods of Proof

|                                     |  |
|-------------------------------------|--|
| Statement<br>$\forall x \in D P(X)$ | Proof Approach<br>Direct: Pick arbitrary $x$ , prove $P$ is true for that $x$ .<br>Contradiction: Suppose not, i.e. $\exists x(\sim p)$ ... Hence supposition $\sim p$ is false (P3) |
| $\exists x \in D P(X)$              | Direct: Find $x$ where $P$ is true.<br>Contradiction: Suppose not, i.e. $\forall x(\sim p)$ ... Hence supposition $\sim p$ is false (P3)   |
| $P \Rightarrow Q$                   | Direct: Assume $P$ is true, prove $Q$<br>Contradiction: Assume $P$ is true and $Q$ is false, then derive contradiction<br>Contrapositive: Assume $\sim Q$ , then prove $\sim P$      |
| $P \Leftrightarrow Q$               | Prove both $P \Rightarrow Q$ and $Q \Rightarrow P$   |
| $xRy$ . Prove $R$ is equivalence    | Prove Reflexive, Symmetric and Transitive  |
| Reflexive                           |  |
| Symmetric                           |  |
| Antisymmetric                       |  |
| Transitive                          |  |

**Defn.** Proof by Contraposition

1. Statement to be proved  $\forall x \in D (P(x) \Rightarrow Q(x))$
2. Contrapositive Form:  $\forall x \in D (\sim Q(x) \Rightarrow \sim P(x))$
3. Prove by direct proof
  - 3.1 Suppose  $x$  is an element of  $D$  s.t.  $Q(x)$  is false
  - 3.2 Show that  $P(x)$  is false.
4. Therefore, original statement is true

### 4 Set Theory

**Defn.** Set: Unordered collection of objects

Order and duplicates don't matter

**Defn.** Membership of Set  $\in$ : If  $S$  is set,  $x \in S$  means  $x$  is an element of  $S$

**Defn.** Cardinality of Set  $|S|$ : The number of elements in  $S$

Common Sets:

$\mathbb{N}$  - Natural Numbers,  $\{0, 1, 2\}$

$\mathbb{Z}$  - Integers

$\mathbb{Q}$  - Rational

$\mathbb{R}$  - Real

$\mathbb{C}$  - Complex

$\mathbb{Z}^{\pm}$  - Positive/Negative Integers

**Defn.** Subset  $A \subseteq B \Leftrightarrow$  Every element of  $A$  is also an element of  $B$

$A \subseteq B \Leftrightarrow \forall x(x \in A \Rightarrow x \in B)$

**Defn.** Proper Subset  $A \subsetneq B \Leftrightarrow (A \subseteq B \wedge A \neq B)$

**Theorem 6.2.4.** An empty set is a subset of every set, i.e.  $\emptyset \subseteq A$  for all sets  $A$

**Defn.** Cartesian Product  $A \times B = \{(a, b) : a \in A \wedge b \in B\}$

**Defn.** Set Equality  $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

$A = B \Leftrightarrow \forall x(x \in A \Leftrightarrow x \in B)$

**Defn.** Union:  $A \cup B = \{x \in U : x \in A \vee x \in B\}$

**Defn.** Intersection:  $A \cap B = \{x \in U : x \in A \wedge x \in B\}$

**Defn.** Difference:  $B \setminus A = \{x \in U : x \in B \wedge x \notin A\}$

**Defn.** Disjoint:  $A \cap B = \emptyset$

**Theorem 4.4.1.** Quotient-Remainder  $n \in \mathbb{Z}, d \in \mathbb{Z}^+$   
there exists unique integers  $q$  and  $r$  such that  $n = dq + r$  and  $0 \leq r < d$

**Defn.** Power Set: The set of all subsets of  $A$ , has  $2^n$  elements.

**Theorem 6.3.1.** Suppose  $A$  is a finite set with  $n$  elements, then  $P(A)$  has  $2^n$  elements.  $|P(A)| = 2^{|n|}$

**Defn.** Cartesian Product of  $A_n = A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) : a_1 \in A_1 \wedge a_2 \in A_2 \dots\}$

**Theorem 6.2.1.** Subset Relations

1. Inclusion of Intersection:  $A \cup B \subseteq A, A \cup B \subseteq B$
2. Inclusion in Union  $A \subseteq A \cup B, B \subseteq A \cup B$
3. Transitive Property of Substs:  $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$

## 5 Relations

**Defn.** Relation from  $A$  to  $B$  is a subset of  $A \times B$

Given an ordered pair  $(x, y) \in A \times B$ ,  $x$  is related to  $y$  by  $R$  is written  $xRy \Leftrightarrow (x, y) \in R$

**Defn.** Domain, Co-domain, Range

Let  $A$  and  $B$  be sets and  $R$  be a relation from  $A$  to  $B$

1. Domain of  $R$ : is set  $\{a \in A : aRb \text{ for some } b \in B\}$
2. Codomain of  $R$ : Set  $B$
3. Range of  $R$ : is set  $\{b \in B : aRb \text{ for some } a \in A\}$

**Defn.** Inverse Relation

Let  $R$  be a relation from  $A$  to  $B$ ,  $R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}$

$\forall x \in A, \forall y \in B ((y, x) \in R^{-1} \Leftrightarrow (x, y) \in R)$

**Defn.** Relation on a Set  $A$  is a relation from  $A$  to  $A$ .

**Defn.** Composition of Relations

$A, B$  and  $C$  be sets.  $R \subseteq A \times B$  be a relation.  $S \subseteq B \times C$  be relation. Composition of  $R$  with  $S$ , denoted  $S \circ R$  is relation from  $A$  to  $C$  such that:

$\forall x \in A, \forall z \in C (xS \circ Rz \Leftrightarrow (\exists y \in B (xRy \wedge ySz)))$

**Proposition.** Composition is Associative  $A, B, C, D$  be sets.  $R \subseteq A \times B, S \subseteq B \times C, T \subseteq C \times D$   
 $T \circ (S \circ R) = T \circ S \circ R$

**Proposition.** Inverse of Composition  $A, B, C$  be sets.  $R \subseteq A \times B, S \subseteq B \times C$   
 $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

**Defn. Reflexivity, Symmetry, Transitivity**

1. Reflexivity:  $\forall x \in A (xRx)$
2. Symmetry:  $\forall x, y \in A (xRy \Rightarrow yRx)$
3. Transitivity:  $\forall x, y, z \in A (xRy \wedge yRz \Rightarrow xRz)$

Refer to proof 6

**Defn.** Transitive Closure

Transitive closure of  $R$  is relation  $R^t$  on  $A$  that satisfies

1.  $R^t$  is transitive
2.  $R \subseteq R^t$
3. If  $S$  is any other transitive relation that contains  $R$ , then  $R^t \subseteq S$

**Defn.** Partition

$P$  is partition of set  $A$  if

1.  $P$  is a set of which all elements are non empty subsets of  $A$ ,  $\emptyset \neq S \subseteq A$  for all  $S \in P$
2. Every element of  $A$  is in exactly on element of  $P$ ,  
 $\forall x \in A \exists S \in P (x \in S)$  and  
 $\forall x \in A \exists S_1, S_2 \in P (x \in S_1 \wedge x \in S_2 \Rightarrow S_1 = S_2)$

OR  $\forall x \in A \exists! S \in P(x \in S)$

Elements of a partition are called components

**Defn.** Relation Induced by a partition

Given partition  $P$  of  $A$ , the relation  $R$  induced by partition:

$\forall x, y \in A, xRy \Rightarrow \exists$  a component of  $S$  of  $P$  s.t.  $x, y \in S$

**Theorem 8.3.1** (Relation Induced by a Partition). Let  $A$  be a set with a partition and let  $R$  be a relation induced by the partition. Then  $R$  is reflexive, symmetric and transitive

**Defn** (Equivalence Relation).  $A$  be set and  $R$  be relation.  $R$  is equivalence relation iff  $R$  is reflexive, symmetric and transitive

**Defn.** Equivalence Class

Suppose  $A$  is set and  $\sim$  is equivalence relation on  $A$ . For each  $A \in A$ , equivalence class of  $a$ , denoted  $[a]$  and called class of  $a$  is set of all elements  $x \in A$  s.t.  $a \sim x$

$[a]_{\sim} = \{x \in A : a \sim x\}$

**Theorem 8.3.4.** The partition induced by an Equivalence Relation

If  $A$  is a set and  $R$  is an equivalence relation on  $A$ , then distinct equivalence classes of  $R$  form a partition of  $A$ ; that is, the union of the equivalence classes is all of  $A$ , and the intersection of any 2 distinct classes is empty.

**Defn.** Congruence

Let  $a, b \in \mathbb{Z}$  and  $n \in \mathbb{Z}^+$ . Then  $a$  is congruent to  $b$  modulo  $n$  iff  $a - b = nk$ , for some  $k \in \mathbb{Z}$ . In other words,  $n|(a - b)$ . We write  $a \equiv b(\text{mod } n)$

**Defn.** Set of equivalence classes

Let  $A$  be set and  $\sim$  be an equivalence relation on  $A$ . Denote by  $A/\sim$ , the set of all equivalence classes with respect to  $\sim$ , i.e.

$A/\sim = \{[x]_{\sim} : x \in A\}$

**Theorem Equivalence Classes.** form a partition Let  $\sim$  be an equiv. relation on  $A$ . Then  $A/\sim$  is a partition of  $A$ .

**Defn** (Antisymmetry).  $R$  is antisymmetric iff  $\forall x, y \in A(xRy \wedge yRx \Rightarrow x = y)$  (DOES NOT IMPLY NOT SYMMETRIC)

**Defn** (Partial Order Relation).  $R$  is Partial Order iff  $R$  is *reflexive*, *antisymmetric* and *transitive*.

**Defn.** Partially Ordered Set Set  $A$  is called poset with respect to partial order relation  $R$  on  $A$ , denoted by  $(A, R)$  (Proof 7)

**Defn.**  $x \preceq y$  is used as a general partial order relation notation

**Defn** (Hasse Diagram). Let  $\preceq$  be a partial order on set  $A$ . Hasse diagram satisfies the following condition for all distinct  $x, y, m \in A$

If  $x \preceq y$  and no  $m \in A$  is s.t.  $x \preceq m \preceq y$ , then  $x$  is placed below  $y$  with a line joining them, else no line joins  $x$  and  $y$ .

**Defn** (Comparability).  $a, b \in A$  are comparable iff  $a \preceq b$  or  $b \preceq a$ . Otherwise, they are **noncomparable**

**Defn** (Maximal, Minimal, Largest Smallest). Set  $A$  be partially ordered w.r.t. a relation  $\preceq$  and  $c \in A$

1.  $c$  is maximal element of  $A$  iff  $\forall x \in A$ , either  $x \preceq c$  or  $x$  and  $c$  are non-comparable. OR  $\forall x \in A(c \preceq x \Rightarrow c = x)$
2.  $c$  is minimal element of  $A$  iff  $\forall x \in A$ , either  $c \preceq x$  or  $x$  and  $c$  are non-comparable. OR  $\forall x \in A(x \preceq c \Rightarrow c = x)$
3.  $c$  is largest element of  $A$  iff  $\forall x \in A(x \preceq c)$
4.  $c$  is smallest element of  $A$  iff  $\forall x \in A(c \preceq x)$

**Proposition.** A smallest element is minimal

Consider a partial order  $\preceq$  on set  $A$ . Any smallest element is minimal.

1. Let  $c$  be smallest element
2. Take any  $x \in A$  s.t.  $x \preceq c$
3. By smallestness, we know  $c \preceq x$  too.
4. So  $c = x$  by antisymmetry

**Defn** (Total Order Relations). All elements of the set are comparable

$R$  is total order iff  $R$  is a partial order and  $\forall x, y \in A(xRy \vee yRx)$

**Defn** (Linearization of a partial order). Let  $\preceq$  be a partial order on set  $A$ . A linearization of  $\preceq$  is a total order  $\preceq^*$  on

$A$  s.t.  $\forall x, y \in A (x \preceq y \Rightarrow x \preceq * y)$

**Defn** (Kahn's Algorithm). Input: A finite set  $A$  and partial order  $\preceq$  on  $A$

1. Set  $A_0 := A$  and  $i := 0$
2. Repeat until  $A_i = \emptyset$ 
  - 2.1. Find minimal element  $c_i$  of  $A_i$  wrt  $\preceq$
  - 2.2. Set  $A_{i+1} = A_i \setminus c_i$
  - 2.3. Set  $i = i + 1$

Output: A linearization  $\preceq *$  of  $\preceq$  defined by setting, for all indices  $i, j$   
 $c_i \preceq * c_j \Leftrightarrow i \leq j$

**Defn** (Well ordered set). Let  $\preceq$  be a total order on set  $A$ .  $A$  is well ordered iff every nonempty subset of  $A$  contains a smallest element. OR

$\forall S \in P(A), S \neq \emptyset \Rightarrow (\exists x \in S \forall y \in S (x \preceq y))$  E.g.  $(\mathbb{N}, \leq)$  is well ordered but  $(\mathbb{Z}, \leq)$  is not as there is no smallest integer (Theorem 4.6.1)

## 6 Proofs

*Proof L1S28.* Prove that the product of two consecutive odd numbers is always odd.

1. Let  $a$  and  $b$  be two consecutive odd numbers
  - 1.1. Without loss of generality, assume that  $a < b$ , hence  $b = a + 2$
  - 1.2. Now,  $a = 2k + 1$  (by defn of odd numbers)
  - 1.3. Similarly,  $b = a + 2 = 2k + 3$
  - 1.4. Therefore,  $ab = (2k + 1)(2k + 3) = (4k^2 + 6k) + (2k + 3) = 4k^2 + 8k + 3 = 2(2k^2 + 4k + 1) + 1$  (by Basic Algebra)
  - 1.5. Let  $m = (2k^2 + 4k + 1)$  which is an integer (by closure of integers under  $\times$  and  $+$ )
  - 1.6. Then  $ab = 2m + 1$  which is odd (by defn of odd numbers)
2. Therefore, the product of two consecutive odd numbers is always odd.

*Proof L4S16.* Sum of 2 even  $\mathbb{Z}$  is even

1. Let  $m$  and  $n$  be two particular but arbitrarily chosen even integers
  - 1.1. Then  $m = 2r$  and  $n = 2s$  for some  $\mathbb{Z} r$  and  $s$  (by defn of even number)
  - 1.2.  $m + n = 2r + 2s = 2(r + s)$  (by basic algebra)
  - 1.3.  $2(r+s)$  is an integer (closure of int under  $\times$  and  $+$ ) and an even number (by defn of even number)
  - 1.4. Hence  $m + n$  is an even number
2. Therefore sum of any two even integers is even

*Proof T 4.6.1.* There is no greatest integer (Contradiction)

1. Suppose not, i.e. there is a greatest intger
  - 1.1. Lets call this greatest integer  $g$ , and  $g \geq n$  for all integers  $n$
  - 1.2. Let  $G = g + 1$
  - 1.3. Now,  $G$  is an integer (closure of integers under  $+$ ) and  $G > g$
  - 1.4. Hence,  $g$  is not the greatest integer, contradicting 1.1
2. Hence, the supposition that there is a greatest integer is false.
3. Therefore there is no greatest integer

*Proof L5S19.* L5S19 Two sets are equal

1. Let sets  $X$  and  $Y$  be given. To prove  $X = Y$
2.  $(\subseteq)$  Prove  $X \subseteq Y$
3.  $(\supseteq)$  Prove  $X \supseteq Y$
4. From (2) and (3), we can conclude that  $X = Y$

*Proof L5S22.* L5S22  $\{x \in \mathbb{Z} : x^2 = 1\} = \{1, -1\}$

1.  $\rightarrow$ 
  - 1.1. Take any  $z \in \{x \in \mathbb{Z} : x^2 = 1\}$
  - 1.2. Then  $z \in \mathbb{Z}$  and  $z^2 = 1$
  - 1.3. So,  $z^2 - 1 = (z - 1)(z + 1) = 0$  (by basic algebra)
  - 1.4.  $\therefore z - 1 = 0$  or  $z + 1 = 0$
  - 1.5.  $\therefore z = 1$  or  $z = -1$
  - 1.6. So,  $z \in \{1, -1\}$
2.  $\leftarrow$ 
  - 2.1. Take any  $z \in \{1, -1\}$
  - 2.2. Then  $z = 1$  or  $z = -1$
  - 2.3. In either case, we have  $z \in \mathbb{Z}$  and  $z^2 = 1$
  - 2.4. So,  $z \in \{x \in \mathbb{Z} : x^2 = 1\}$
3. Therefore,  $\{x \in \mathbb{Z} : x^2 = 1\} = \{1, -1\}$  (from (1) and (2))

*Proof L6S27.*  $\forall x, y \in \mathbb{Z}(xRy \Leftrightarrow 3|(x - y))$  is reflexive, symmetric, transitive

1. Proof of Reflexivity
  - 1.1. Let  $a$  be an arbitrarily chosen integer.
  - 1.2. Now  $a - a = 0$
  - 1.3.  $3|0$  (since  $0 = 3 \cdot 0$ ), hence  $3|(a - a)$
  - 1.4. Therefore  $aRa$  (by defn of R)
2. Proof of Symmetry
  - 2.1. Let  $a, b$  be arbitrarily chosen integers
  - 2.2. Then  $3|(a - b)$  (by defn of R), hence  $a - b = 3k$  for some integer  $k$  (by defn of divisibility)
  - 2.3. Multiplying both sides by  $-1$  gives  $b - a = 3(-k)$
  - 2.4. Since  $-k$  is an integer,  $3|(b - a)$  (by defn of divisibility)
  - 2.5. Therefore,  $aRb \Rightarrow bRa$  (by defn of R)
3. Proof of Transitivity
  - 3.1. Let  $a, b, c$  be arbitrarily chosen integers
  - 3.2. Then,  $3|(a - b)$  and  $3|(b - c)$  (by defn of R), hence  $a - b = 3r$  and  $b - c = 3s$  (by defn of divisibility)
  - 3.3. Adding both equations gives  $a - c = 3r + 3s$
  - 3.4. Since  $r + s$  is an integer,  $3|(a - c)$  (by defn of divisibility)
  - 3.5. Therefore  $aRb \wedge bRc \Rightarrow aRc$  (by defn of R)

*Lemma Equivalence Class L6S47.* Let  $\sim$  be an equivalence relation on  $A$ . The following are equivalent for all  $x, y \in A$   
(i)  $x \sim y$ , (ii)  $[x] = [y]$ , (iii)  $[x] \cap [y] \neq \emptyset$

1.  $x \sim y \Rightarrow [x] = [y]$ 
  - 1.1. Suppose  $x \sim y$
  - 1.2. Then  $y \sim x$  (by symmetry)
  - 1.3. For every  $z \in [x]$ 
    - 1.3.1.  $x \sim z$  (by defn of  $\sim$ )
    - 1.3.2.  $\therefore y \sim z$  (by transitivity of  $y \sim x$ )
    - 1.3.3.  $\therefore z \in [y]$  (by defn of  $[y]$ )
  - 1.4. This shows  $[x] \subseteq [y]$
  - 1.5. Switching roles of  $x$  and  $y$ , we can also see that  $[y] \subseteq [x]$
  - 1.6. Therefore,  $[x] = [y]$
2.  $[x] = [y] \Rightarrow [x] \cap [y] \neq \emptyset$ 
  - 2.1. Suppose  $[x] = [y]$
  - 2.2. Then  $[x] \cap [y] = [x]$  (by idempotent law for  $\cap$ )
  - 2.3. However, we know  $x \sim x$  (by reflexivity of  $\sim$ )
  - 2.4. This shows  $x \in [x] = [x] \cap [y]$  (by defn of  $[x]$  and (2.2))
  - 2.5. Therefore  $[x] \cap [y] \neq \emptyset$
3.  $[x] \cap [y] \neq \emptyset \Rightarrow x \sim y$ 
  - 3.1. Suppose  $[x] \cap [y] \neq \emptyset$
  - 3.2. Take  $z \in [x] \cap [y]$
  - 3.3. Then  $z \in [x]$  and  $z \in [y]$  (by defn of  $\cap$ )
  - 3.4. Then  $x \sim z$  and  $y \sim z$  (by defn of  $[x]$  and  $[y]$ )

- 3.5.  $y \sim z$  implies  $z \sim y$  (by defn of symmetry)
- 3.6. Therefore,  $x \sim y$  (by transitivity)

*Proposition L6S54.* Congruence-mod  $n$  is an equivalence relation on  $\mathbb{Z}$  for every  $n \in \mathbb{Z}^+$

1. (Reflexivity) For all  $a \in \mathbb{Z}$ 
  - 1.1.  $a - a = 0 = n \times 0$
  - 1.2. So  $a \equiv a \pmod{n}$  (by defn of congruence)
2. (Symmetry)
  - 2.1. Let  $a, b \in \mathbb{Z}$  s.t.  $a \equiv a \pmod{n}$
  - 2.2. Then there is a  $k \in \mathbb{Z}$  s.t.  $a - b = nk$
  - 2.3. Then  $b - a = -(a - b) = -nk = n(-k)$
  - 2.4.  $-k \in \mathbb{Z}$  (by closure of integers under  $\times$ ), so  $b \equiv a \pmod{n}$  (by defn of congruence)
3. (Transitivity)
  - 3.1. Let  $a, b, c \in \mathbb{Z}$  s.t.  $a \equiv a \pmod{n}$  and  $b \equiv c \pmod{n}$
  - 3.2. Then there is a  $k, l \in \mathbb{Z}$  s.t.  $a - b = nk$  and  $b - c = nl$
  - 3.3. Then  $a - c = (a - b) + (b - c) = nk + nl = n(k + l)$
  - 3.4.  $k + l \in \mathbb{Z}$  (by closure of integers under  $+$ ), so  $a \equiv c \pmod{n}$  (by defn of congruence)

*Proof L6S69.*  $\forall a, b \in \mathbb{Z}^+, \forall a|b \Leftrightarrow b = ka$  for some integer  $k$ . Prove  $|$  is a partial order relation on  $A$

1.  $|$  is reflexive: Suppose  $a \in A$ . Then  $a = 1a$ , so  $a|a$  (by defn of divisibility)
2.  $|$  is antisymmetric
  - 2.1. Suppose  $a, b \in \mathbb{Z}^+$  such that  $aRb$  and  $bRa$
  - 2.2. Then  $b = ra$  and  $a = sb$  for some integers  $r$  and  $s$  (by defn of divides). It follows that  $b = ra = r(sb)$
  - 2.3. Dividing both sides by  $b$  gives  $1 = rs$
  - 2.4. Only product of two positive integers that equals 1 is 11.
  - 2.5. Thus  $r = s = 1$ , and so  $a = sb = 1b = b$
  - 2.6. Therefore,  $|$  is antisymmetric
- OR
- 2.1. Suppose  $a, b \in \mathbb{Z}^+$  such that  $a|b$  and  $b|a$
- 2.2. then  $a \leq b$  and  $b \leq a$  (by theorem 4.3.1)
- 2.3. So  $a = b$
3.  $|$  is transitive: Show that  $\forall a, b, c \in A, a|b \wedge b|c \Rightarrow a|c$  (theorem 4.3.3)

*Proof T01Q9.* The product of any two odd integers is an odd integer

1. Take any 2 odd numbers  $a$  and  $b$
2. Then  $a = 2k + 1$  and  $b = 2p + 1$  for  $k, p \in \mathbb{Z}$  (by defn of odd number)
3. Then  $a \cdot b = (2k + 1)(2p + 1) = (4kp + 2k) + (2p + 1) = 2(2kp + p + k) + 1$  (by defn of odd number)
4. Let  $q = 2kp + p + k$  which is an integer (by closure of int under  $+$  and  $\times$ )
5. Then  $nm = 2q + 1$  which is odd (by defn of odd numbers)

*Proof T01Q10.* Let  $n$  be an integer. Then  $n^2$  is odd iff  $n$  is odd

1. Proof By Contraposition, that is "if  $n$  is even,  $n^2$  is even ( $\Rightarrow$ )"
  - 1.1. Suppose  $n$  is even.
  - 1.2. Then  $\exists k \in \mathbb{Z}$  s.t.  $n = 2k$  (by defn of even integers)
  - 1.3.  $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
  - 1.4. Hence,  $n^2 = 2p$ , where  $p = 2k^2 \in \mathbb{Z}$  (by closure of integers under  $\times$ )
  - 1.5. Therefore,  $n^2$  is even and this proves that if  $n^2$  is odd,  $n$  is odd.
2. If  $n$  is odd, then  $n \times n = n^2$  is odd (T01Q9)
3. Therefore  $n^2$  is odd if and only if  $n$  is odd.

*Proof T02Q3.* Rational numbers are closed under addition

1. Let  $r$  and  $s$  be rational numbers
2.  $\exists a, b, c, d \in \mathbb{Z}$  s.t.  $r = \frac{a}{b}, s = \frac{c}{d}$  and  $b \neq 0, d \neq 0$  (by defn of rational numbers)
3. Hence  $r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$  (by basic algebra)
4.  $ad + bc \in \mathbb{Z}$  and  $bd \in \mathbb{Z}$  (closure of integers under  $+$  and  $\times$ )
5.  $bd \neq 0$  since  $b \neq 0, d \neq 0$
6. Hence  $r + s$  is rational, therefore rational numbers are closed under addition

*Proof T02Q10.* if  $n$  is a product of 2 positive integers  $a$  and  $b$ , then  $a \leq n^{1/2}$  or  $b \leq n^{1/2}$

1. Proof by contraposition, that is if  $a > n^{1/2}$  and  $b > n^{1/2}$ , then  $n$  is not a product of  $a$  and  $b$
2. Suppose  $a > n^{1/2}$  and  $b > n^{1/2}$ , then  $ab > n^{1/2} \cdot n^{1/2} = n$  (by Appendix A T27)
3. Since  $ab \neq n$ , the contrapositive statement is true

or by contradiction

1. Proof by contradiction, that is  $n = ab$  and  $a > n^{1/2}$  and  $b > n^{1/2}$
2. Since  $a > n^{1/2}$  and  $b > n^{1/2}$ , then  $ab > n^{1/2} \cdot n^{1/2} = n$  (by Appendix A T27)
3. This contradicts  $n = ab$ . Therefore original statement is true

*Proof T03Q04.* Let  $A = \{2n + 1 : n \in \mathbb{Z}\}$  and  $B = \{2n - 5 : n \in \mathbb{Z}\}$ . Is  $A = B$ ?

1.  $\subseteq$ 
  - 1.1. Let  $a \in A$ , and  $a = 2n + 1, n \in \mathbb{Z}$
  - 1.2. Then  $a = 2n + 1 = 2(n + 3) - 5$
  - 1.3.  $n + 3 \in \mathbb{Z}$  (by closure of int under  $+$ )
  - 1.4. Therefore,  $a \in B$  (by defn of B)
2.  $\supseteq$ 
  - 2.1. Let  $b \in A$ , and  $b = 2n - 5, n \in \mathbb{Z}$
  - 2.2. Then  $b = 2n - 5 = 2(n - 3) + 1$
  - 2.3.  $n - 3 \in \mathbb{Z}$  (by closure of int under  $-$ )
  - 2.4. Therefore,  $b \in A$  (by defn of B)
3. Therefore,  $A = B$

*Proof T03Q05.* Prove  $\forall A, B, C, A \cap (B \setminus C) = (A \cap B) \setminus C$

1.  $A \cap (B \setminus C) = \{x : x \in A \wedge x \in (B \setminus C)\}$  (by defn of  $\cap$ )
2.  $= \{x : x \in A \wedge (x \in B \wedge x \notin C)\}$  (by defn of  $\setminus$ )
3.  $= \{x : x \in (A \wedge x \in B) \wedge x \notin C\}$  (by associativity of  $\wedge$ )
4.  $= \{x : x \in (A \cap B) \wedge x \notin C\}$  (by defn of  $\cap$ )
5.  $= \{x : x \in (A \cap B) \setminus C\}$  (by defn of  $\setminus$ )

*Proof T03Q05.* Prove  $\forall A, B, C, A \cap (B \setminus C) = (A \cap B) \setminus C$

1.  $A \cap (B \setminus C) = \{x : x \in A \wedge x \in (B \setminus C)\}$  (by defn of  $\cap$ )
2.  $= \{x : x \in A \wedge (x \in B \wedge x \notin C)\}$  (by defn of  $\setminus$ )
3.  $= \{x : x \in (A \wedge x \in B) \wedge x \notin C\}$  (by associativity of  $\wedge$ )
4.  $= \{x : x \in (A \cap B) \wedge x \notin C\}$  (by defn of  $\cap$ )
5.  $= \{x : x \in (A \cap B) \setminus C\}$  (by defn of  $\setminus$ )

*Proof T03Q8.* Let  $A$  and  $B$  be set. Show that  $A \subseteq B$  if and only if  $A \cup B = B$   
To show  $A \cup B = B$ , we need to show  $A \cup B \subseteq B$  and  $B \subseteq A \cup B$

1.  $\implies$ 
  - 1.1. Suppose  $A \subseteq B$
  - 1.2. (Show  $A \cup B \subseteq B$ )
    - 1.2.1. Let  $z \in A \cup B$
    - 1.2.2. Then  $z \in A$  or  $z \in B$  (by defn of  $\cup$ )
    - 1.2.3. Case 1: Suppose  $z \in A$ , then  $z \in B$  as  $A \subseteq B$  line (1.1)
    - 1.2.4. Case 2: Suppose  $z \in B$ , then  $z \in B$ . We have  $z \in B$  in either case
  - 1.3. (Show  $A \cup B \supseteq B$ )
    - 1.3.1. Let  $z \in B$
    - 1.3.2. Then  $z \in A$  or  $z \in B$  (by generalization)
    - 1.3.3. So  $z \in A \cup B$  (by defn of  $\cup$ )
  - 1.4. Therefore  $A \cup B = B$
2.  $\impliedby$ 
  - 2.1. Suppose  $A \cup B = B$
  - 2.2. Let  $z \in A$ 
    - 2.2.1. Then  $z \in A$  or  $z \in B$  (by generalization)
    - 2.2.2. So  $z \in A \cup B$  (by defn of  $\cup$ )
    - 2.2.3. So  $z \in B$  since  $A \cup B = B$  (2.1)
  - 2.3. Therefore  $A \subseteq B$
3. Therefore,  $A \subseteq B$  if and only iff  $A \cup B = B$

*Proof T04Q05.* Relation  $S = \{(m, n) \in \mathbb{Z}^2 : m^3 + n^3 \text{ is even}\}$ , Proof  $S \circ S = S$

1.  $(\subseteq)$  Suppose  $(x, z) \in S \circ S$ 
  - 1.1. Then  $(x, y) \in S$  and  $(y, z) \in S$  for some  $y \in \mathbb{Z}$  (defn of composition of relations)
  - 1.2. So  $x^3 + y^3$  is even and  $y^3 + z^3$  is even
  - 1.3. This implies that  $x^3 + 2y^3 + z^3$  is even
  - 1.4. This implies that  $x^3 + z^3$  is even as  $2y^3$  is even
  - 1.5. Therefore,  $(x, z) \in S$  (by defn of  $S$ )
2.  $(\supseteq)$  Suppose  $(x, z) \in S$ 
  - 2.1. Then  $x^3 + z^3$  is even (by defn of  $S$ )
  - 2.2. Case 1:  $x^3$  is odd.
    - 2.2.1. Then  $z^3$  is also odd.
    - 2.2.2. This implies that  $x^3 + 1^3$  is even and  $1^3 + z^3$  is even
    - 2.2.3. Thus,  $(x, 1) \in S$  and  $(1, z) \in S$  (by defn of  $S$ )
    - 2.2.4. So,  $(x, z) \in S \circ S$
  - 2.3. Case 2:  $x^3$  is even.
    - 2.3.1. Then  $z^3$  is also even.
    - 2.3.2. This implies that  $x^3 + 0^3$  is even and  $0^3 + z^3$  is even
    - 2.3.3. Thus,  $(x, 0) \in S$  and  $(0, z) \in S$  (by defn of  $S$ )
    - 2.3.4. So,  $(x, z) \in S \circ S$
  - 2.4. In all cases,  $(x, z) \in S \circ S$
- OR
3.  $(\supseteq)$  Suppose  $(x, z) \in S$ 
  - 3.1. Note that  $(x, x) \in S$  as  $x^3 + x^3$  is even
  - 3.2. Since  $(x, x) \in S$  and  $(x, z) \in S$ , we have  $(x, z) \in S \circ S$  (by defn of composition of relations)

*Proof.*  $R$  is asymmetric if and only if  $R$  is antisymmetric and irreflexive.

1.  $\implies$ 
  - 1.1.  $R$  is irreflexive ( $R$  is irreflexive  $\implies R$  is antisymmetric and irreflexive)
    - 1.1.1. Let  $x \in A$  s.t.  $xRx \implies x \not R x$  ( $R$  is Asymmetric)
    - 1.1.2. Since  $x \not R x$ ,  $R$  is irreflexive (by defn of irreflexive)
  - 1.1.  $R$  is antisymmetric (Tutorial Qn 6c)
2.  $\impliedby$  ( $R$  is antisymmetric and irreflexive  $\implies$  asymmetry)
  - 2.1. Let  $x, y \in A$ , s.t.  $xRy$  is antisymmetric and irreflexive
  - 2.2. There is 2 cases to consider,  $x = y$  and  $x \neq y$
  - 2.3.  $x = y$ 
    - 2.3.1.  $xRx$  is not valid as it contradicts irreflexive,  $\forall x \in A (x \not R x)$
    - 2.3.2. Therefore,  $xRx \implies x \not R x$

2.4.  $x \neq y$

2.4.1.  $xRy \wedge yRx \implies x = y$

## 7 Tables

|   |  |   |
|---|--|---|
| Commutative<br>Associative<br>Distributive<br>Identity<br>Negation<br>Double Negative<br>Idempotent<br>Universal bound<br>de Morgan's<br>Absorption<br>Implication<br>$\sim$ (Implication)  | $p \wedge q \equiv q \wedge p$ $p \wedge q \wedge r \equiv (p \wedge q) \wedge r$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \wedge \text{true} \equiv p$ $p \vee \sim p \equiv \text{true}$ $\sim(\sim p) \equiv p$ $p \vee p \equiv p$ $p \vee \text{true} \equiv \text{true}$ $\sim(p \wedge q) \equiv \sim p \vee \sim q$ $p \vee (p \wedge q) \equiv p$ $p \Rightarrow q \equiv \sim p \vee q$ $\sim(p \Rightarrow q) \equiv p \wedge \sim q$                         | $p \vee q \equiv q \vee p$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \vee \text{false} \equiv p$ $p \wedge \sim p \equiv \text{false}$ $p \wedge p \equiv p$ $p \wedge \text{false} \equiv \text{false}$ $\sim(p \vee q) \equiv \sim p \wedge \sim q$ $p \wedge (p \vee q) \equiv p$ |
| Modus Ponens<br>Modus Tollens<br>Generalization<br>Specialization<br>Conjunction<br>Elimination<br>Transitivity<br>Division into cases<br>Contradiction   | $p \Rightarrow q, p$ $p \Rightarrow q, \sim q$ $p$ $p \wedge q$ $p, q$ $p \vee q, \sim q$ $p \Rightarrow q, q \Rightarrow r$ $p \wedge q, p \Rightarrow r, q \Rightarrow r$ $\sim p \Rightarrow \text{false}$  | $q$ $\sim p$ $p \vee q$ $p$ $p \wedge q$ $p$ $p \Rightarrow r$ $r$ $p$  |
| Commutative<br>Associative<br>Distributive<br>Identity<br>Complement<br>Double Complement<br>Idempotent<br>Universal Bound<br>De Morgan's<br>Absorption<br>Complements of U and $\emptyset$<br>Set Difference                               | $A \cup B = B \cup A$ $(A \cup B) \cup C = A \cup (B \cup C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cup \emptyset = A$ $A \cup \bar{A} = U$ $\bar{\bar{A}} = A$ $A \cup A = A$ $A \cup U = U$ $\overline{A \cup B} = \bar{A} \cap \bar{B}$ $A \cup (A \cap B) = A$ $\bar{U} = \emptyset$ $A \setminus B = A \cap \bar{B}$   | $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cap U = A$ $A \cap \bar{A} = \emptyset$ $A \cap A = A$ $A \cap \emptyset = \emptyset$ $\overline{A \cap B} = \bar{A} \cup \bar{B}$ $A \cap (A \cup B) = A$ $\bar{\emptyset} = U$   |
| F1 Commutative<br>F2 Associative<br>F3 Distributive<br>F4 Identity<br>F5 Additive inverses<br>F6 Reciprocals  | $a + b = b + a$ $(a + b) + c = a + (b + c)$ $a(b + c) = ab + ac$ $0 + a = a + 0 = a$ $a + (-a) = (-a) + a = 0$ $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$   | $ab = ba$ $(ab)c = a(bc)$ $(b + c)a = ba + ca$ $1 \cdot a = a \cdot 1 = a$ $a \neq 0$   |
| T1 Cancellation Add<br>T2 Possibility of Sub<br>T3<br>T4<br>T5<br>T6<br>T7 Cancellation Mul<br>T8 Possibility of Div<br>T9<br>T10<br>T11 Zero Product<br>T12 Mul with -ve<br>T13 Equiv Frac<br>T14 Add Frac<br>T15 Mul Frac<br>T16 Div Frac | $a + b = a + c$ <p>There is one <math>x, a + x = b</math></p> $b - a = b + (-a)$ $-(-a) = a$ $a(b - c) = ab - ac$ $0 \cdot a = a \cdot 0 = 0$ $ab = ac$ $a \neq 0, ax = b$ $a \neq 0, \frac{b}{a} = b \cdot a^{-1}$ $a \neq 0, (a^{-1})^{-1} = a$ $ab = 0 \Rightarrow a = 0 \vee b = 0$ $(-a)b = a(-b) - -(ab)$ $\frac{a}{b} = \frac{ac}{bc}$ $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ac}{bd}$ | $b = c$ $x = b - a$ $b = c, a \neq 0$ $x = \frac{b}{a}$ $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$ $b \neq 0, c \neq 0$ $b \neq 0, d \neq 0$ $b \neq 0, d \neq 0$ $b \neq 0, d \neq 0$  |

|                    |  |   |
|--------------------|--|---|
| Ord1               | $\forall a, b \in \mathbb{R}^+$        | $a + b > 0, ab > 0$                       |
| Ord2               | $\forall a, b \in \mathbb{R}_{\neq 0}$ | $a$ is positive or negative and not both  |
| Ord3               | 0 is not positive                      |   |
| $a < b$            | means $b + (-a)$ is positive           |   |
| $a \leq b$         | means $a < b$ or $a = b$               |   |
| $a < 0$            | means $a$ is negative                  |   |
| T17 Trichotomy Law | $a < b \vee b > a \vee a = b$          |   |
| T18 Transitive Law | $a < b$ and $b < c$                    | $a < c$                                   |
| T19                | $a < b$                                | $a + c < b + c$                           |
| T20                | $a < b$ and $c > 0$                    | $ac < bc$                                 |
| T21                | $a \neq 0$                             | $a^2 > 0$                                 |
| T22                | $1 > 0$                                |   |
| T23                | $a < b$ and $c < 0$                    | $ac > bc$                                 |
| T24                | $a < b$                                | $-a > -b$                                 |
| T25                | $ab > 0$                               | $a$ and $b$ are both positive or negative |
| T26                | $a < c$ and $b < d$                    | $a + b < c + d$                           |
| T30                | $0 < a < c$ and $0 < b < d$            | $0 < ab < cd$                             |