速成教育
SPEED UP EDUCATION

MACM101 Andrei

DISCRETE MATHEMATICS I

导师: **Stacy Cao**

SFU Week 14 Class | 2021/4/14

Logic

Truth Table

p	q	$p \vee q$	$p \wedge q$	$\neg p$	$p \to q$	$p \leftrightarrow q$	$p \oplus q$
0	0						
0	1						
1	0						
1	1						

看 equivalence，看 tautology，看 contradiction

(a) The implication $(\neg q \vee p) \to q$ is:

i. a tautology
ii. true for exactly one truth assignment to the variables p and q.
iii. false for exactly one truth assignment to the variables p and q.
iv. true whenever p is true, but false otherwise.
v. true whenever q is true, false otherwise.

(c) The propositional expression $[p \vee (q \wedge r)] \vee \neg[p \vee (q \wedge r)]$ is a tautology.

Laws of Logics

For any primitive statements p, q, r, any tautology T_0, and any contradiction F_0,

1)	$\neg\neg p \iff p$	Law of *Double Negation*
2)	$\neg(p \vee q) \iff \neg p \wedge \neg q$ $\neg(p \wedge q) \iff \neg p \vee \neg q$	*DeMorgan's* Laws
3)	$p \vee q \iff q \vee p$ $p \wedge q \iff q \wedge p$	*Commutative* Laws
4)	$p \vee (q \vee r) \iff (p \vee q) \vee r^{\dagger}$ $p \wedge (q \wedge r) \iff (p \wedge q) \wedge r$	*Associative* Laws
5)	$p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$	*Distributive* Laws
6)	$p \vee p \iff p$ $p \wedge p \iff p$	*Idempotent* Laws
7)	$p \vee F_0 \iff p$ $p \wedge T_0 \iff p$	*Identity* Laws
8)	$p \vee \neg p \iff T_0$ $p \wedge \neg p \iff F_0$	*Inverse* Laws
9)	$p \vee T_0 \iff T_0$ $p \wedge F_0 \iff F_0$	*Domination* Laws
10)	$p \vee (p \wedge q) \iff p$ $p \wedge (p \vee q) \iff p$	*Absorption* Laws

逻辑化简步骤：

1. Implication reduction: $p \to q \equiv \neg p \vee q$
2. DeMogan and Double Negation
3. 原则：一样或相反的凑一块

3. (4 points) Give reasons for each step in the proof of the following. A proof based on the truth table is not acceptable.

$$[(p \vee q) \wedge (p \vee \neg q)] \vee q \Leftrightarrow p \vee q$$

4. (4 points) Determine with justification whether $p \to (q \vee r)$ and $(p \wedge \neg q) \to r$ are logically equivalent.

Translation

1. $p \to q$

If p then q.
If p, q.
p implies q.
p only if q.
p is sufficient for q.
A sufficient condition for q is p.
q is necessary for p.
A necessary condition for p is q.
q if p.
q when (whenever) p.
q follows from p.
q unless $\neg p$

2. Converse: $q \to p$

3. Inverse: $\neg p \to \neg q$

4. Contrapositive: $\neg q \to \neg p \equiv p \to q$

5. $p \leftrightarrow q$: if and only if

1. (6 points) Consider the statement "If x is a perfect square and x is even, then x is divisible by 4".

   (a) Designate propositional variables to stand for the three conditions about x mentioned in the statement.

   (b) Write the statement formally in terms of these propositions.

   (c) State the contrapositive of your answer in part (b), both in terms of your propositional variables and in colloquial terms.

Rules of Inference

Rule of Inference	Related Logical Implication	Name of Rule
1) p $p \to q$ $\therefore q$	$[p \wedge (p \to q)] \to q$	Rule of Detachment (Modus Ponens)
2) $p \to q$ $q \to r$ $\therefore p \to r$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Law of the Syllogism
3) $p \to q$ $\neg q$ $\therefore \neg p$	$[(p \to q) \wedge \neg q] \to \neg p$	Modus Tollens
4) p q $\therefore p \wedge q$		Rule of Conjunction
5) $p \vee q$ $\neg p$ $\therefore q$	$[(p \vee q) \wedge \neg p] \to q$	Rule of Disjunctive Syllogism
6) $\neg p \to F_0$ $\therefore p$	$(\neg p \to F_0) \to p$	Rule of Contradiction
7) $p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Rule of Conjunctive Simplification
8) p $\therefore p \vee q$	$p \to p \vee q$	Rule of Disjunctive Amplification
9) $p \wedge q$ $p \to (q \to r)$ $\therefore r$	$[(p \wedge q) \wedge [p \to (q \to r)]] \to r$	Rule of Conditional Proof
10) $p \to r$ $q \to r$ $\therefore (p \vee q) \to r$	$[(p \to r) \wedge (q \to r)] \to [(p \vee q) \to r]$	Rule for Proof by Cases
11) $p \to q$ $r \to s$ $p \vee r$ $\therefore q \vee s$	$[(p \to q) \wedge (r \to s) \wedge (p \vee r)] \to (q \vee s)$	Rule of the Constructive Dilemma
12) $p \to q$ $r \to s$ $\neg q \vee \neg s$ $\therefore \neg p \vee \neg r$	$[(p \to q) \wedge (r \to s) \wedge (\neg q \vee \neg s)] \to (\neg p \vee \neg r)$	Rule of the Destructive Dilemma

(a)

$p \to q$
$q \to r$
$\neg r$
$\therefore \neg p$

(a)

If I drive on the freeway, I will see the fire.
I will drive on the freeway or take surface streets (or both).
I am not going to take surface streets.
$\therefore$ I will see the fire.

Quantifier

Predicate: Statements with variables 带有不确定变量的 statement
Universal quantifier: ∀ for all
Existential quantifier: ∃ exist, some

判断带有 quantifier 的 predicate 的 True or False

Negate of Quantifier

Translation of Quantifiers

(b) Let $F(x, y)$: "x can fool y". What would be the appropriate equivalent of the statement "John can fool Mary, but Mary cannot fool John "?

i. $\neg F(John, Mary)$
ii. $\neg F(Mary, Fred)$
iii. $\neg F(John, Mary) \wedge \neg F(Mary, John)$
iv. $\neg F(John, Mary) \wedge F(Mary, John)$
v. $\neg(F(John, Mary) \wedge F(Mary, John))$

5. (5 points) Consider the propositions $\forall x \exists y P(x, y)$ and $\exists y \forall x P(x, y)$.

(a) Write out the first of these completely in English.

(b) Write out the second of these completely in English.

(c) Give an example to show that the two propositions are not logically equivalent.

2. (5 points) For the following formulas, let the universe be $\mathbb{R}$. Translate each of the following sentences into a formula using quantifiers.

(a) There is no largest number.

(b) There is no smallest positive number.

(c) Between any two distinct numbers, there is a third number not equal to either of them.

带有 quantifier 的 inference

Rule of Universal Specification:
If $\forall x P(x)$ is true, then for arbitrary *c*, *P(c)* is true.
用来去掉∀

Rule of Universal Generalization:
If for any *c*, *P(c)* is true, then $\forall x P(x)$ is true.
用来加上∀

Rule of Existential Specification:
If $\exists x P(x)$ is true, then for some *c*, *P(c)* is true.
用来去掉∃

Rule of Existential Generalization:
If for some *c*, *P(c)* is true, then $\exists x P(x)$ is true.
用来加上∃

(d) The domain is the set of students at an elementary school.

Every student who has a permission slip can go on the field trip.
Every student has a permission slip.

∴ Every student can go on the field trip.

Proof

1. Direct proof
2. Proof by contrapositive (Indirect proof)
3. Proof by contradiction
4. Proof by cases

6. (8 points) Answer any two of the following three.

   (a) Suppose $a, b, c, d \in \mathbb{Z}$. Prove, using a direct proof approach, that if $a|b$ and $c|d$, then $ac|bd$.

   (b) Use the contrapositive proof method to show "if the average of n numbers (all of them are not the same) is 100, then one of the numbers is greater than 100".

3. (5 points) Prove or disprove each of the following propositions:

   (a) If n is a multiple of 4 and k is a multiple of 3, the nk is a multiple of 12.

   (b) If n is a multiple of 4 and k is a multiple of 3, the $n + k$ is a multiple of 7.

Sets

Sets: unordered, no repetition collection of objects

表达 Sets:

Roster Format：列举

Set Builder：公式

Some Concepts:

1. Elements: $x \in A$
2. Subsets: $A \subseteq B: \forall x(x \in A \to x \in B)$
   1) Improper Subsets: $A \subset B: \forall x(x \in A \to x \in B) \wedge \exists x(x \in B \wedge x \notin A)$
3. Empty Set $\emptyset$ $\forall x(x \in U_0 \to x \notin \emptyset)$
4. Power Set: $P(A)$: sets of subsets of A
5. Number of subsets of A
   1) Number of subsets of A contain/not contain element X
   2) Number of subsets of A contain n elements

(a) $|A \cup B| + |A \cap B| = |A| + |B|$ True or False

Operation of sets

1. $A \cap B$ intersection $\{x|x \in A \wedge x \in B\}$

2. $A \cup B$ union $\{x|x \in A \vee x \in B\}$

3. $\bar{A}$ complement $\{x|x \in U_0 \wedge x \notin A\}$

4. $A - B$ difference $\{x|x \in A \wedge x \notin B\}$

5. $A \triangle B$ symmetric difference $\{x|x \in (A \cup B) \wedge x \notin (A \cap B)\}$

6. $A \times B$ product of sets $\{(x, y)|x \in A \wedge y \in B\}$

Membership Table

A	B	$A \cap B$	$A \cup B$	$\bar{A}$	$A - B$	$A \triangle B$
0	0					
0	1					
1	0					
1	1					

Venn Diagram

Define the sets A, B, C, and D as follows:

A = {-3, 0, 1, 4, 17}
B = {-12, -5, 1, 4, 6}
C = {x ∈ **Z**: x is odd}
D = {x ∈ **Z**: x is positive}

Law of Sets

For any sets A, B, and C taken from a universe $\mathcal{U}$

1) $\overline{\overline{A}} = A$	Law of *Double Complement*
2) $\overline{A \cup B} = \overline{A} \cap \overline{B}$	*DeMorgan's* Laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$	
3) $A \cup B = B \cup A$	*Commutative* Laws
$A \cap B = B \cap A$	
4) $A \cup (B \cup C) = (A \cup B) \cup C$	*Associative* Laws
$A \cap (B \cap C) = (A \cap B) \cap C$	
5) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	*Distributive* Laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	
6) $A \cup A = A$	*Idempotent* Laws
$A \cap A = A$	
7) $A \cup \emptyset = A$	*Identity* Laws
$A \cap \mathcal{U} = A$	
8) $A \cup \overline{A} = \mathcal{U}$	*Inverse* Laws
$A \cap \overline{A} = \emptyset$	
9) $A \cup \mathcal{U} = \mathcal{U}$	*Domination* Laws
$A \cap \emptyset = \emptyset$	
10) $A \cup (A \cap B) = A$	*Absorption* Laws
$A \cap (A \cup B) = A$	

(a) $(\overline{A} \cap C) \cup (A \cap C) = C$

(b) $(B \cup A) \cap (\overline{B} \cup A) = A$

(c) $\overline{A \cap \overline{B}} = \overline{A} \cup B$

Cardinality

Finite Sets

If set A has finite elements, then cardinality of A (also called size of A) is $|A| =$ number of elements in A.

Infinite Sets

Countable Sets

Cardinality of the set of natural number is $|\mathbb{N}| = \aleph_0$.
Any sets with the cardinality less than or equal to $\mathbb{N}$ is a countable set.

Example of countably infinite sets

All integers
Positive odd/even integers
Positive rational numbers
Decimals consist of only 1's

Uncountable Sets

Any sets with the cardinality greater than $\mathbb{N}$ is uncountable.

Example of uncountably infinite sets

Irrational numbers
Irrational numbers within any interval
Decimals consist of 2 or more kinds of numbers

Relation

Binary Relation

If R is a binary relation from A to B, then $R \subseteq A \times B$

Operation on Relations

$$R_1 \cap R_2, R_1 \cup R_2, \overline{R_1}, R_1 - R_2, R_1 \circ R_2$$

$$R^{-1} = \{(b, a) | (a, b) \in R\}$$

Properties of Binary Relation on A

Reflexive

$$\forall a((a,a) \in R)$$

Anti-Reflexive

$$\forall a((a,a) \notin R)$$

Symmetric

$$\forall a \forall b((a,b) \in R \rightarrow (b,a) \in R)$$

Anti-Symmetric

$$\forall a \forall b((a,b) \in R \wedge (b,a) \in R \rightarrow a = b)$$

Transitive

$$\forall a \forall b \forall c((a,b) \in R \wedge (b,c) \in R \rightarrow (a,c) \in R)$$

11. (8 points) Let R be a relation on the power-set of a finite set A. Fill in the blanks in the following table on the properties of R when $R \in \{\subset, \subseteq, =, \not\subset\}$

Relation on $\mathcal{P}(A)$	$\subset$	$\subseteq$	$=$	$\not\subset$
reflexive				
symmetric				
antisymmetric				
transitive				

Counting of Relations

Let $|A| = a$ and $|B| = b$

1. Number of relations from A to B: 2^{ab}
2. Number of relations on A: 2^{a^2}
3. Number of reflexive / anti-reflexive relations on A: 2^{a^2-a}
4. Number of symmetric relations on A: $2^{(a^2+a)/2}$
5. Number of anti-symmetric relations on A: $2^a \cdot 3^{(a^2-a)/2}$

Representation of Binary Relation

Matrix

Relation from A to B, 行代表 A 的元素，列代表 B 的元素。

1 代表在 relation 里，0 代表不在。

Direct Graph

11. (4 points) Explain how to tell whether a relation is symmetric under each of the following representations: (a) matrix, (b) digraph.

Equivalence Relation

An equivalence relation is a binary relation on A that is reflexive, symmetric, and transitive.

Equivalence Class and Partition

10. (5 points) Let the relation R be reflexive and transitive on A. Show that $R \cap R^{-1}$ is an equivalence relation on A.

12. (6 points)

    (a) Write down the definition of what it means for a collection C to be a partition of A.

    (b) Explain how a partition C on a set A determines the equivalence relation R on A (give an explicit definition of R).

    (c) The set $C = \{\{1, 3, 5\}, \{2, 4\}, \{6\}\}$ is a partition of $\{1, 2, 3, 4, 5, 6\}$. Write down the equivalence relation determined by the partition and find the partition determined by this relation.

Partial Order

Partial Order 又叫 Poset.

A partial order is a binary relation on A that is reflexive, anti-symmetric, and transitive.

Hesse Diagram

Total Order

$$\forall x \forall y((x, y) \in R)$$

Hesse Diagram 是一条直线

Maximal / Minimal Element

Greatest / Least

9. (10 points)

(a) Let R be a relation defined on $A \times B$ such that $((a, b), (x, y)) \epsilon R$ if and only if $a \leq x$ and $b \leq y$. Show that R is a partial order relation.

(b) Draw the Hasse diagram for the poset $(A \times B, R)$ where $A = \{1, 2, 3\}$ and $B = \{2, 3\}$ and R is defined as in part (a).

Function

Definition:

1. Every input can only have one output.
2. Every element in the set of input must have an output.

Domain:

Codomain:

Range:

Special functions:

Absolute function:

Floor and ceiling functions:

Identity function:

Factorial:

Bijection and Inverse

One-to-one (injective):

$$\forall a \forall b (f(a) = f(b) \rightarrow a = b)$$

一个 output 只对应一个 input。从$f(a) = f(b)$开始证，推出$a = b$.

Onto (surjective):

$$\forall y \exists x (f(x) = y)$$

Range = codomain. 从$y = f(x)$开始变形成$x = g(y)$，得到 y 的取值范围(range)和 codomain 比较。

Bijective function (one-to-one corresponds)

f is bijective if f is one-to-one and onto.

Inverse function:

f has an inverse f^{-1} if and only if f is bijective.

$$f^{-1}(x) = g(x)$$

Counting of Function

For $f: A \to B$, if $|A| = a$ and $|B| = b$, then

Number of functions:

$$b^a$$

Number of one-to-one:

$P(b, a)$ for $b \geq a$

Number of onto: for $a \geq b$

$$b! \cdot S(a, b) = \sum_{k=0}^{b} (-1)^k \binom{b}{k} (b-k)^a$$

S(m,n)

m \ n	1	2	3	4	5	6	7	8
1	1							
2	1	1						
3	1	3	1					
4	1	7	6	1				
5	1	15	25	10	1			
6	1	31	90	65	15	1		
7	1	63	301	350	140	21	1	
8	1	127	966	1701	1050	266	28	1

Number of bijective functions: $a!$ for $a = b$

(c) The function $f : A \to B$ maps every element of A to an element of B. Suppose $|A| > |B| > 0$. From this information, we can conclude that:

i. f is injective but not surjective
ii. f is surjective but not injective
iii. f is injective but not necessarily surjective
iv. f is surjective but not necessarily injective
v. none of the above

(i) Consider the function $f : \{1, 2, 3, 4, 5, 6, 7\} \to \{0, 1, 2, 3, 4\}$. How many such functions have the property that $|f^{-1}(\{3\})| = 3$?

(i) $\binom{7}{3}$ (ii) $\binom{4}{3} \times \binom{7}{3}$ (iii) $4^4 \times \binom{7}{3}$ (iv) none of the above

11. (8 points) Determine whether each of the following statements is true or false. For each false statement give a counterexample.

    (a) If $f : A \to B$ and $(a, b), (a, c) \epsilon f$, then $b = c$.

    (b) If $f : A \to B$ is a one-to-one correspondence and A and B are finite, then $A = B$.

    (c) If $f : A \to B$ is one-to-one, then f is invertible.

4. (5 points) Suppose A and B are two sets containing n and 2 elements respectively. In this question we will consider the functions:

    (a) Describe the functions from $A \to B$ that are not onto.

    (b) How many different one-to-one functions g are there from B to A?

Composition functions

$$(f \circ g)(x) = f(g(x))$$
$$f \circ f^{-1} = f^{-1} \circ f = x$$

If $f \circ g$ is one-to-one, then g must be one-to-one.
If $f \circ g$ is onto, then f must be onto.

7. (4 points) Suppose that $h : X \to Y$ is any one-to-one function, and $g : Y \to Z$ is any onto function. Prove or disprove

   (a) $g \circ h$ must be onto.

   (b) $g \circ h$ must be one-to-one.

Recurrence

普通 recurrence

特殊 recurrence

1. Fibonacci

$$F_1 = 1, F_2 = 1, F_{n+1} = F_n + F_{n-1}$$

2. Lucas

$$L_1 = 2, L_1 = 1, L_{n+1} = L_n + L_{n-1}$$

3. Others

7. (4 points) Define the infinite sequence of values a_n for $n \geq 1$ as follows:

   - $a_1 = 2$
   - $a_n = a_{\lfloor n/2 \rfloor} * a_{\lceil n/2 \rceil}$ for $n \geq 2$.

   Give the values of a_2, of a_3 and of a_4.

Mathematical Induction

Simple MI

1. Basic Step: prove that for smallest n_0, $P(n_0)$ is true
2. Inductive step:
   1) Assume for $n = k$, $P(k)$ is true
   2) Use basic step and assumption to prove that for $n = k + 1$, $P(k + 1)$ is true.

Strong MI

1. Basic Step: prove that for smallest n_0, $P(n_0)$ is true
2. Inductive step:
   1) Assume for all $n_0 \leq n \leq k$, $P(n)$ is true
   2) Use basic step and assumption to prove that for $n = k + 1$, $P(k + 1)$ is true.

(d) Which of the following statements would be least likely to appear in an inductive proof as the induction hypothesis?

i. "Assume that $S(k)$ is true for some fixed but arbitrary $k \in \mathbb{N}$".
ii. "Assume that $S(k)$ is true for all $0 \leq k < n$".
iii. "Assume that $S(k)$ is true for all $0 \leq k \leq n$."
iv. "Assume that $S(k)$ is true for all for all natural numbers k."

9. (8 points) Using the Mathematical Induction Principle solve any two of the following. Identify the parts very clearly. Marks are alloted for the correct structure of the proof.

   (a) Prove the validity of the following Rule of Inference for all integers $n \geq 1$:

$$\begin{array}{lll} p_1 & \rightarrow & p_2 \\ p_2 & \rightarrow & p_3 \\ \ldots & \ldots & \ldots \\ p_n & \rightarrow & p_{n+1} \\ \neg p_{n+1} & & \\ \hline \neg p_1 & & \end{array}$$

   (b) A sequence $a_1, a_2, \ldots$ is defined recursively by $a_1 = 3$ and $a_n = 7a_{n-1}$ for $n \geq 2$. Show that $a_n = 3.7^{n-1}$ for all $n \geq 1$.

   (c) Show that 23 is the largest integer which cannot be written as a sum of $5's$ and/or $7's$.

Counting

Rule of Sum and Rule of Product

Counting Equations

		Formula
Permutation	With repetition	n^r
	No repetition	$\frac{n!}{(n-r)!}$
	No repetition, repeated objects	$\frac{n!}{n_1!n_2!...n_r!}$
Combination	No repetition	$\binom{n}{r}=\frac{n!}{r!(n-r)!}$
	With repetition	$\binom{n+r-1}{r}=\frac{(n+r-1)!}{r!(n-1)!}$

单词排列

捆绑，插空

坐标系问题

旋转问题

(e) Suppose that a committee of 5 people from a group of 7 women and 9 men is to be formed such that at least one woman serves on a committee. How many such committees can be formed?

i. $\binom{7}{5}$
ii. $\binom{7}{1} \times \binom{15}{4}$
iii. $\binom{16}{5} - \binom{9}{5}$
iv. $\binom{16}{5} - \binom{7}{5}$
v. none of the above

(f) Two labeled fair dice are rolled. What is the probability that the product of the two spots is odd?

$(i)\ \frac{1}{2}$ $(ii)\ \frac{1}{4}$ $(iii)\ \frac{2}{3}$ $(iv)\ \frac{3}{4}$ $(v)\ \frac{1}{8}$

(g) A person is positioned at the origin of 2-dimensional coordinate system, and need to reach the point (4,5). The movement is restricted by one-unit steps in only the directions of positive x and y. Under these conditions, in how many ways can it make the trip to the destination point $(4, 5)$?

$(i)\ 9$ $(ii)\ 20$ $(iii)\ 9!$ $(iv)\ \frac{9!}{4!5!}$ $(v)\ \frac{20!}{4!5!}$

(h) How many ordered 4-tuples (w, x, y, z) are solutions to the equation $w+x+y+z = 50$ if each of w, x, y and z is to be positive multiple of 5?

$(i)\ \binom{33}{3}$ $(ii)\ \binom{50}{3}$ $(iii)\ \binom{10}{3}$ $(iv)\ \binom{13}{3}$ (v) none of the above

(i) Consider the function $f : \{1, 2, 3, 4, 5, 6, 7\} \to \{0, 1, 2, 3, 4\}$. How many such functions have the property that $|f^{-1}(\{3\})| = 3$?

$(i)\ \binom{7}{3}$ $(ii)\ \binom{4}{3} \times \binom{7}{3}$ $(iii)\ 4^4 \times \binom{7}{3}$ (iv) none of the above

(b) There are exactly 130 integers between 1 and 1000 (inclusive) which are divisible 7 but not by 11.

1. (15 points) This problem is on "placing balls in bins".

(a) We are interested in placing m balls in n bins. Placement is either unrestricted (some bins may be left empty), one-to-one (each bin has at most one ball), or onto (each bin must have at least one ball). Determine the number of ways of placing balls in bins for each of the following cases:

Constraints	unrestricted	one-to-one	onto
balls labeled bins labeled			
balls unlabeled bins labeled			
balls labeled bins unlabeled			

Binomial

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

4. (6 points) For any positive integer n show by using the binomial theorem that

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k 2^{n-k} = 1.$$

1. (3 points) Find the coefficient of x^{10} in $(3x+2)^{10}$.

Probability

$$\Pr(A) = \frac{|A|}{|S|}$$

8. (4 points) Find the probability that a family of 4 children there will be (a) at least 1 boy and (b) at least 1 boy and 1 girl. Assume that the probability of a male or a girl birth is the same. What is the sample space?

2. (10 points) Six different numbers were chosen at random from the numbers 1 through 49. The winning combinations do not depend on the order in which these numbers are drawn.

   (a) How many different lottery outcomes are possible?

   (b) A jackpot prize occurs if all numbers are chosen correctly. What is the probability of winning the jackpot?

   (c) If you choose five out of six correctly, you share the second prize. What is the probability of winning the second prize?

Pigeonhole

If there are N pigeons (objects) and k pigeonholes (categories), then there is at least one pigeonhole contains at least $m = \left\lceil \frac{N}{k} \right\rceil$ pigeons.

$$N \geq k(m-1)+1$$

(j) Among any 800 distinct integers chosen from the set $\{n : (n \in \mathbb{N}) \wedge (1 \leq n \leq 1600)\}$ at least two must be consecutive.

(b) Consider the points $(x_i, y_i, z_i), x_i, y_i, z_i \in \mathbb{N}, i = 1, 2, \ldots, n$ in 3-dimension. What is the smallest value for n such that for any given n points, there exist at least two pair of points whose midpoints also have integer coordinates. The midpoint of (a, b, c) and (α, β, γ) is $(\frac{a+\alpha}{2}, \frac{b+\beta}{2}, \frac{c+\gamma}{2})$.

8. (8 points) There are 51 houses on a street. Each house has an address between 1 and 100 inclusive.

   (a) Show that at least two houses have addresses that are consecutive.

Number Theory

Divisibility

整除符号

$$a|b \Leftrightarrow b = an\ (n \in \mathbb{Z})$$

Indicate whether each expression is true or false.

(a) 8 | 40

Solution

(b) 7 | 50

Solution

(c) $6 \nmid 36$

Solution

(d) $8 \nmid 79$

Solution

$$a = dq + r$$

a: dividend; b: divisor; q: quotient; r: remainder

$$q = a \text{ div } d, \qquad r = a \bmod d$$

Determine the value of n based on the given information.

(a)

n div 7 = 11, n mod 7 = 5

(b)

n div 5 = -10, n mod 5 = 4

(c)

n div 11 = -3, n mod 11 = 7

(d)

n div 10 = 2, n mod 10 = 8

Congruence

$$a \equiv b (\mathrm{mod}\, m)$$

a 和 b 对 m 求余相等, $m|(a-b)$

Operation on mod

If $a \equiv b (\mathrm{mod}\, m)$ and $c \equiv d (\mathrm{mod}\, m)$,
Then $a + c \equiv b + c (\mathrm{mod}\, m)$, $a - c \equiv b - d (\mathrm{mod}\, m)$, $a \cdot c \equiv b \cdot d (\mathrm{mod}\, m)$

Residue: 余数

Set of residues: 余数的集合 $\mathbb{Z}_m$
Operation tables for $\mathbb{Z}_m$

Proper divisor of 0

a is a proper divisor of 0 if there is a b such that $b \not\equiv (\mathrm{mod}\, a)$ and $a \cdot b \equiv 0 (\mathrm{mod}\, m)$.

Equivalent statements

1. a has an inverse
2. a is not a proper divisor of 0
3. a is relatively prime with m

Inverse of x mod m

Definition 10.6.1: Multiplicative inverse mod n.

A ***multiplicative inverse mod n*** (or just ***inverse mod n***) of an integer x, is an integer s ∈ {1, 2, ..., n-1} such that sx mod n = 1.

(c)
x = 53, n = 71

(d)
x = 71, n = 53

Prime

Prime: integer ≥ 2, that is only divisible by 1 and itself
Composite: integer ≥ 2 that has divisors other than 1 and itself

进制转换

Represent integers using product of primes

Every integer ≥ 2 can be represented as product of primes.
If $N = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then it has $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$ divisors.

Suppose that the prime factorizations of two positive integers x and y are expressed using a common set of primes as follows:

- $x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$
- $y = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n}$

(a) What is the prime factorization for x · y?

(b) Suppose y | x. What is the prime factorization for x / y? (It is fine to have some prime factors raised to the zero power in your answer.)

Find lcm and gcd of *a, b*

Relative Prime (Coprime)

a and b are relative primes to each other if $\gcd(a, b) = 1$.

Euclidean algorithm

(d)
259 and 77

(e)
72 and 42

Exercise 10.6.5: GCD and linear combination of integers.

(a)
Prove that for any positive integers a and b, if ax + by = z where x, y and z are integers, then gcd(a, b) | z

Cryptography

Convert each text message to a number. Use the scheme that associates each capital letter to a 2-digit number in the range 01 through 26 ("A"=01, "B"=02, ..., "Z"=26) and the blank character to 27.

(a)

CRYPTO

(b)

MESSAGE

Chinese Remainder Theorem

If $n \bmod 3 = a,\ n \bmod 5 = b,\ n \bmod 7 = c$
Then $n = 70a + 21b + 15c - 105m$