The Foundations: Logic and Proofs

Proofs

- A proof is a valid argument that establishes the truth of a mathematical statement.

- Ingredients:
  - hypotheses of the theorem
  - axioms assumed to be true
  - previously proven theorems
  - rules of inference

You get:
truth of the statement being proved

Usefulness

- Computer Science
  - Verifying that computer programs are correct.
  - Establishing that operating systems are secure.
  - Making inferences in artificial intelligence.
  - Showing that system specifications are consistent.

- Mathematics
  - Defining Formalism.
  - Providing specification in a common language.
  - Justification for the results.

Definitions

1. An integer n is even if, and only if, $n = 2k$ for some integer k.
2. An integer n is odd if, and only if, $n = 2k + 1$ for some integer k.
3. An integer n is prime if, and only if, $n > 1$ and for all positive integers r and s, if $n = r \cdot s$, then $r = 1$ or $s = 1$.
4. An integer $n > 1$ is composite if, and only if, $n = r \cdot s$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.
5. A real number r is rational if, and only if, $r = \frac{a}{b}$ for some integers a and b with $b \neq 0$.
6. If n and d are integers and $d \neq 0$, then d divides n, written $d|n$ if, and only if, $n = d.k$ for some integers k.
7. An integer n is called a perfect square if, and only if, $n = k^2$ for some integer k.

Types of Proofs

- **Proving conditional Statements**
  - Direct Proofs
  - Indirect Proofs
    - **Proof by Contraposition**
    - **Proofs by Contradiction**
- **Proving Non-conditional Statements**
  - Indirect Proofs
  - If-And-Only-If Proof
  - Constructive Versus Non-constructive Proofs
  - Existence Proofs; Existence and Uniqueness Proofs
  - Disproofs (Counterexample, Contradiction, Existence Statement)
  - Proofs Involving Sets
- **Mathematical Induction**

Direct Proofs

- p □q
  - first step is the assumption that *p is true*
  - subsequent steps constructed using rules of inference.
  - final step showing that *q must also be true*

showing that if *p is true,*
then q must also be true,
so that the combination
p true and q false never occurs

Outline for Direct Proof

Proposition If P, then Q.

Proof. Suppose P.

⋮

Therefore Q. ■

Activity Time

Prove that the sum of two odd integers is even.

Prove that the sum of two odd integers is even.

Let **m** and **n** be two odd integers. Then by definition of odd numbers

$m = 2k + 1$ for some $k \in Z$

$n = 2l + 1$ for some $l \in Z$

Now $m + n = (2k + 1) + (2l + 1)$

$= 2k + 2l + 2$

$= 2(k + l + 1)$

$= 2r$ where $r = (k + l + 1) \in Z$

Hence $m + n$ is even.

EXERCISE:

Prove that if n is any even integer, then $(-1)^n = 1$

SOLUTION:

Suppose n is an even integer. Then $n = 2k$ for some integer k.

Now

$$(-1)^n = (-1)^{2k}$$
$$= [(-1)^2]^k$$
$$= (1)^k$$
$$= 1 \qquad \text{(proved)}$$

EXERCISE:

Prove that the product of an even integer and an odd integer is even.

SOLUTION:

Suppose m is an even integer and n is an odd integer. Then

$m = 2k$ for some integer k

and $n = 2l + 1$ for some integer l

Now

$$m \cdot n = 2k \cdot (2l + 1)$$
$$= 2 \cdot k\,(2l + 1)$$
$$= 2 \cdot r \quad \text{where } r = k(2l + 1) \text{ is an integer}$$

Hence $m \cdot n$ is even. (Proved)

EXERCISE:

Prove that the square of an even integer is even.

SOLUTION:

Suppose n is an even integer. Then $n = 2k$

Now

$$\text{square of } n = n^2 = (2 \cdot k)^2$$
$$= 4k^2$$
$$= 2 \cdot (2k^2)$$
$$= 2 \cdot p \text{ where } p = 2k^2 \in Z$$

Hence, n^2 is even. (proved)

proved that if *n is an odd integer, then* n^2 *is an odd integer*

- We assume that the hypothesis of this conditional statement is true, namely, we assume that *n is odd.*
- By the definition of an odd integer, it follows that $n = 2k + 1$, *where k is some integer.*
- *Square both sides* $n^2 = (2k + 1)^2$
  - $4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$
- Consequently, we have proved that if *n is an odd integer, then* n^2 *is an odd integer*

EXERCISE:

Prove that if n is an odd integer, then $n^3 + n$ is even.

SOLUTION:

Let n be an odd integer, then $n = 2k + 1$ for some $k \in Z$

Now $n^3 + n = n(n^2 + 1)$

$= (2k + 1)((2k+1)^2 + 1)$

$= (2k + 1)(4k^2 + 4k + 1 + 1)$

$= (2k + 1)(4k^2 + 4k + 2)$

$= (2k + 1)\,2.\,(2k^2 + 2k + 1)$

$= 2 \cdot (2k + 1)(2k^2 + 2k + 1)$ $\quad k \in Z$

= an even integer

Proposition If x is an even integer, then $x^2 - 6x + 5$ is odd.

Proof. Suppose x is an even integer.

Then $x = 2a$ for some $a \in \mathbb{Z}$, by definition of an even integer.

So $x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5 = 4a^2 - 12a + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1$.

Therefore we have $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2 \in \mathbb{Z}$.

Consequently $x^2 - 6x + 5$ is odd, by definition of an odd number.

EXERCISE:

Prove that, if the sum of any two integers is even, then so is their difference.

SOLUTION:

Suppose m and n are integers so that m + n is even. Then by definition of even numbers

$$m + n = 2k \qquad \text{for some integer } k$$

$$\Rightarrow \quad m = 2k - n \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Now $m - n = (2k - n) - n$ using (1)

$$= 2k - 2n$$

$$= 2(k - n) = 2r \qquad \text{where } r = k - n \text{ is an integer}$$

Hence m - n is even.

EXERCISE:

Prove that the sum of any two rational numbers is rational.

SOLUTION:

Suppose r and s are rational numbers.

Then by definition of rational

$$r = \frac{a}{b} \quad \text{and} \quad s = \frac{c}{d}$$

for some integers a, b, c, d with $b \neq 0$ and $d \neq 0$

Now

$$r + s = \frac{a}{b} + \frac{c}{d}$$

$$= \frac{ad + bc}{bd}$$

$$= \frac{p}{q}$$

where $p = ad + bc \in Z$ and $q = bd \in Z$ and $q \neq 0$

Hence r + s is rational.

EXERCISE:

Given any two distinct rational numbers r and s with $r < s$. Prove that there is a rational number x such that $r < x < s$.

SOLUTION:

Given two distinct rational numbers r and s such that

$r < s$ .....(1)

Adding r to both sides of (1), we get

$$r + r < r + s$$

$$2r < r + s$$

$$\Rightarrow \quad r < \frac{r+s}{2} \qquad \text{.....(2)}$$

Next adding s to both sides of (1), we get

$$r + s < s + s$$

$$\Rightarrow \quad r + s < 2s$$

$$\Rightarrow \quad \frac{r+s}{2} < s \qquad \text{.....(3)}$$

Combining (2) and (3), we may write

$$r < \frac{r+s}{2} < s \quad \text{.....(4)}$$

Since the sum of two rationals is rational, therefore $r + s$ is rational. Also the quotient of a rational by a non-zero rational, is rational, therefore $\frac{r+s}{2}$ is rational and by (4) it lies between r & s. Hence, we have found a rational number such that $r < x < s$. (proved)

EXERCISE:

Prove that the sum of any three consecutive integers is divisible by 3.

PROOF:

Let n, $n + 1$ and $n + 2$ be three consecutive integers.

Now

$$n + (n + 1) + (n + 2) = 3n + 3$$
$$= 3(n + 1)$$
$$= 3 \cdot k \quad \text{where } k = (n+1) \in Z$$

Hence, the sum of three consecutive integers is divisible by 3.

Activity Time

Give a direct proof that if *m and n are both perfect squares, then nm is also a perfect square.*

Proof

- We assume that the hypothesis of this conditional statement is true, namely, we assume that m and n are both perfect squares.
- By the definition of a perfect square, It follows that there are integers s and t such that $m = s^2$ and $n = t^2$.
- Multiplying both m and n to get s^2t^2.
- Hence, $mn = s^2t^2 = (ss)(tt) = (st)(st) = (st)^2$, using commutativity and associativity of multiplication.
- By the definition of perfect square, it follows that mn is also a perfect square, because it is the square of st, which is an integer.
- We have proved that if m and n are both perfect squares, then mn is also a perfect square.

Activity Time

Give a direct proof that if *n is an integer and n is odd, then 3n + 2 is odd.*

Indirect Proofs

- Direct proof begin with the premises, continue with a sequence of deductions, and end with the conclusion.
- Attempts at direct proofs often reach dead ends
- Proofs that **do not** start with the premises and end with the conclusion, are called **indirect proofs**

PROOF BY CONTRAPOSITION:

A proof by contraposition is based on the logical equivalence between a statement and its contrapositive. Therefore, the implication $p \rightarrow q$ can be proved by showing that its contrapositive $\sim q \rightarrow \sim p$ is true. The contrapositive is usually proved directly.

The method of proof by contrapositive may be summarized as:

1. Express the statement in the form if p then q.
2. Rewrite this statement in the contrapositive form
   if not q then not p.
3. Prove the contrapositive by a direct proof.

Outline for Contrapositive Proof

Proposition If P, then Q.

Proof. Suppose $\sim Q$.

⋮

Therefore $\sim P$. ■

Prove that if *n is an integer and 3n + 2 is odd, then n is odd.*

PROOF:

The contrapositive of the given conditional statement is

" if n is even then 3n + 2 is even"

Suppose n is even, then

$n = 2k$ for some $k \in Z$

Now $3n + 2 = 3(2k) + 2$

$= 2.(3k + 1)$

$= 2.r$ where $r = (3k + 1) \in Z$

Hence 3n + 2 is even. We conclude that the given statement is true since its contrapositive is true.

EXERCISE:

Prove that for all integers n, if n^2 is even then n is even.

PROOF:

The contrapositive of the given statement is:

"if n is not even (odd) then n^2 is not even (odd)"

We prove this contrapositive statement directly.

Suppose n is odd. Then $n = 2k + 1$ for some $k \in Z$

Now $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

$= 2 \cdot (2k^2 + 2k) + 1$

$= 2 \cdot r + 1$ where $r = 2k^2 + 2k \in Z$

Hence n^2 is odd. Thus the contrapositive statement is true and so the given statement is true.

EXERCISE:

Prove that if n is an integer and $n^3 + 5$ is odd, then n is even.

PROOF:

Suppose n is an odd integer. Since, a product of two odd integers is odd, therefore $n^2 = n.n$ is odd; and $n^3 = n^2.n$ is odd.

Since a sum of two odd integers is even therefore $n^2 + 5$ is even.

Thus we have prove that if n is odd then $n^3 + 5$ is even.

Since this is the contrapositive of the given conditional statement, so the given statement is true.

EXERCISE:

Prove that if n^2 is not divisible by 25, then n is not divisible by 5.

SOLUTION:

The contra positive statement is:

"if n is divisible by 5, then n^2 is divisible by 25"

Suppose n is divisible by 5. Then by definition of divisibility

$$n = 5 \cdot k \qquad \text{for some integer } k$$

Squaring both sides

$$n^2 = 25 \cdot k^2 \qquad \text{where } k^2 \in Z$$

n^2 is divisible by 25

Proofs by Contradiction

A proof by contradiction is based on the fact that either a statement is true or it is false but not both. Hence the supposition, that the statement to be proved is false, leads logically to a contradiction, impossibility or absurdity, then the supposition must be false. Accordingly, the given statement must be true.

The method of proof by contradiction may be summarized as follows:

1. Suppose the statement to be proved is false.

2. Show that this supposition leads logically to a contradiction.

3. Conclude that the statement to be proved is true.

Basic Idea

- Assume that the statement we want to prove is *false, and then show* that this assumption leads to nonsense!

Outline for Proof by Contradiction

Proposition P.

Proof. Suppose $\sim P$.

⋮

Therefore $C \wedge \sim C$. ■

We are then led to conclude that we were wrong to assume the statement was false, so the statement must be true.

THEOREM:

There is no greatest integer.

PROOF:

Suppose there is a greatest integer N. Then $n \leq N$ for every integer n.

Let $M = N + 1$

Now M is an integer since it is a sum of integers.

Also $M > N$ since $M = N + 1$

Thus M is an integer that is greater than the greatest integer, which is a contradiction. Hence our supposition is not true and so there is no greatest integer.

EXERCISE:

Give a proof by contradiction for the statement:

"If n^2 is an even integer then n is an even integer."

PROOF:

Suppose n^2 is an even integer and n is not even, so that n is odd.

Hence $n = 2k + 1$ for some integer k.

Now $n^2 = (2k + 1)^2$

$= 4k^2 + 4k + 1$

$= 2 \cdot (2k^2 + 2k) + 1$

$= 2r + 1$ where $r = (2k^2 + 2k) \in Z$

This shows that n^2 is odd, which is a contradiction to our supposition that n^2 is even. Hence the given statement is true.

EXERCISE:

Prove that if n is an integer and $n^3 + 5$ is odd, then n is even using contradiction method.

SOLUTION:

Suppose that $n^3 + 5$ is odd and n is not even (odd). Since n is odd and the product of two odd numbers is odd, it follows that n^2 is odd and $n^3 = n^2 . n$ is odd. Further, since the difference of two odd numbers is even, it follows that

$$5 = (n^3 + 5) - n^3$$

is even. But this is a contradiction. Therefore, the supposition that $n^3 + 5$ and n are both odd is wrong and so the given statement is true.

THEOREM:

The sum of any rational number and any irrational number is irrational.

PROOF:

We suppose that the negation of the statement is true. That is, we suppose that there is a rational number r and an irrational number s such that r + s is rational. By definition of ration

$$r = \frac{a}{b} \quad \ldots\ldots\ldots\ldots\ldots(1) \quad \text{and} \quad r + s = \frac{c}{d} \quad \ldots\ldots\ldots\ldots\ldots(2)$$

for some integers a, b, c and d with b$\neq$ 0 and d $\neq$ 0.

Using (1) in (2), we get

$$\frac{a}{b} + s = \frac{c}{d}$$

$$\Rightarrow \quad s = \frac{c}{d} - \frac{a}{b}$$

$$s = \frac{bc - ad}{bd} \qquad (bd \neq 0)$$

Now bc - ad and bd are both integers, since products and difference of integers are integers. Hence s is a quotient of two integers bc-ad and bd with bd $\neq$ 0. So by definition of rational, s is rational.

This contradicts the supposition that s is irrational. Hence the supposition is false and the theorem is true.

EXERCISE:

Prove that $\sqrt{2}$ is irrational.

PROOF:

Suppose $\sqrt{2}$ is rational. Then there are integers m and n with no common factors so

$$\sqrt{2} = \frac{m}{n}$$

that

Squaring both sides gives

$$2 = \frac{m^2}{n^2}$$

Or $m^2 = 2n^2$ .....(1)

This implies that m^2 is even (by definition of even). It follows that m is even. Hence

$m = 2k$ for some integer k (2)

Substituting (2) in (1), we get

$$(2k)^2 = 2n^2$$

$$\Rightarrow \quad 4k^2 = 2n^2$$

$$\Rightarrow \quad n^2 = 2k^2$$

This implies that n^2 is even, and so n is even. But we also know that m is even. Hence both m and n have a common factor 2. But this contradicts the supposition that m and n have no common factors. Hence our supposition is false and so the theorem is true.

PROOF BY COUNTER EXAMPLE

Disprove the statement by giving a counter example.
For all real numbers a and b, if $a < b$ then $a^2 < b^2$.

SOLUTION:

Suppose $a = -5$ and $b = -2$
then clearly $-5 < -2$

But $a^2 = (-5)^2 = 25$ and $b^2 = (-2)^2 = 4$

But $25 > 4$

This disproves the given statement.

EXERCISE:

Prove or give counter example to disprove the statement.

For all integers n, $n^2 - n + 11$ is a prime number.

SOLUTION:

The statement is not true

For n = 11

we have , $n^2 - n + 11 = (11)^2 - 11 + 11$

$= (11)^2$

$= (11)(11)$

$= 121$

which is obviously not a prime number.

Mathematical Induction

Shoaib Raza

Conjecture: The sum of the first n odd natural numbers equals n^2.

n	sum of the first n odd natural numbers	n^2
1	$1 =$	1
2	$1+3 =$	4
3	$1+3+5 =$	9
4	$1+3+5+7 =$	16
5	$1+3+5+7+9 =$	25
⋮	⋮	⋮
n	$1+3+5+7+9+11+\cdots+(2n-1) =$	n^2
⋮	⋮	⋮

An infinite ladder

- Suppose that we have an infinite ladder, and we want to know whether we can reach every step on this ladder.

- We know two things:
  1. We can reach the first rung of the ladder.
  2. If we can reach a particular rung of the ladder, then we can reach the next rung.

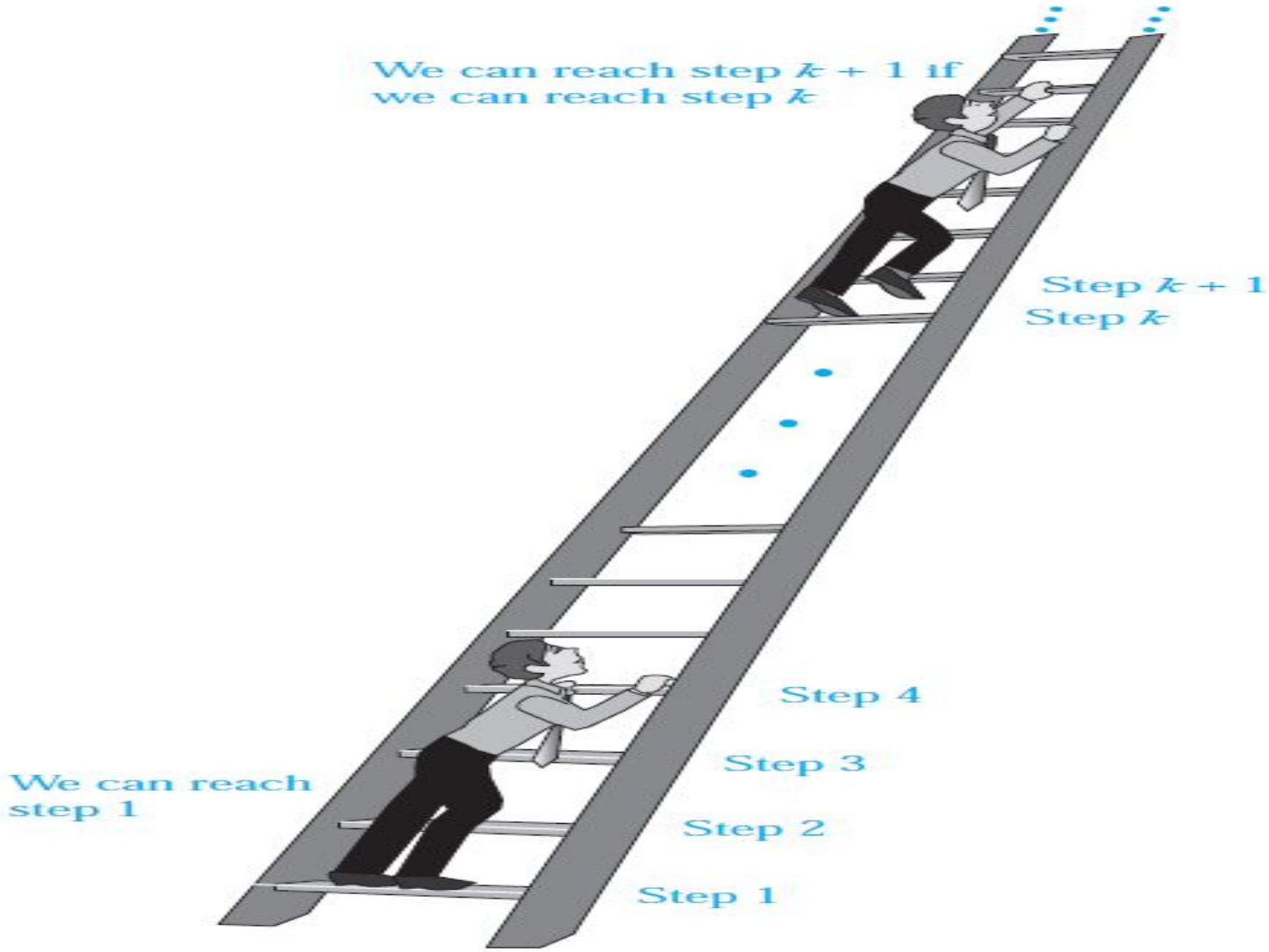


FIGURE 1 **Climbing an Infinite Ladder.**

Mathematical Induction

- Mathematical statements assert that a property is true for all positive integers.

- Proofs using mathematical induction have two parts.
  - First, they show that the statement holds for the positive integer 1 (base case).
  - Second, they show that if the statement holds for a positive integer then it must also hold for the next larger integer. (inductive case)

- The method can be extended to prove statements about more general well-founded structures, such as trees; this generalization, known as structural induction, is used in mathematical logic and computer science.

NOTE

- It is extremely important to note that mathematical induction can be used only to prove results obtained in some other way.
- It is *not a tool for discovering formulae or* theorems.
- Mathematicians sometimes find proofs by mathematical induction unsatisfying because they do not provide insights as to why theorems are true.
- You can prove a theorem by mathematical induction even if you do not have the slightest idea why it is true!

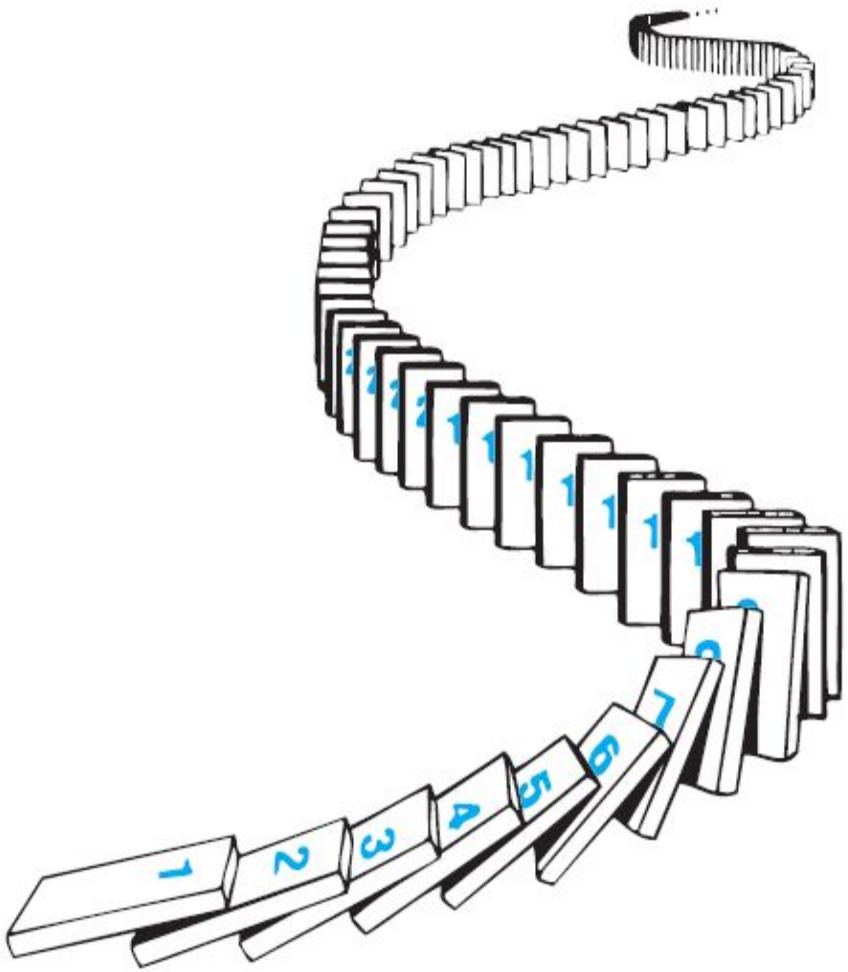
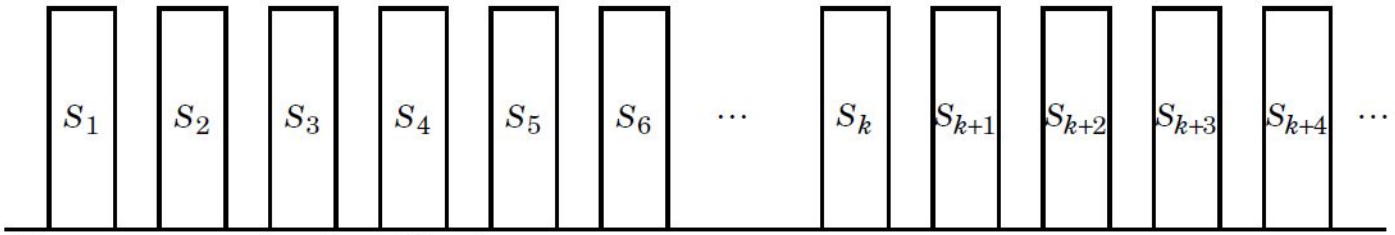
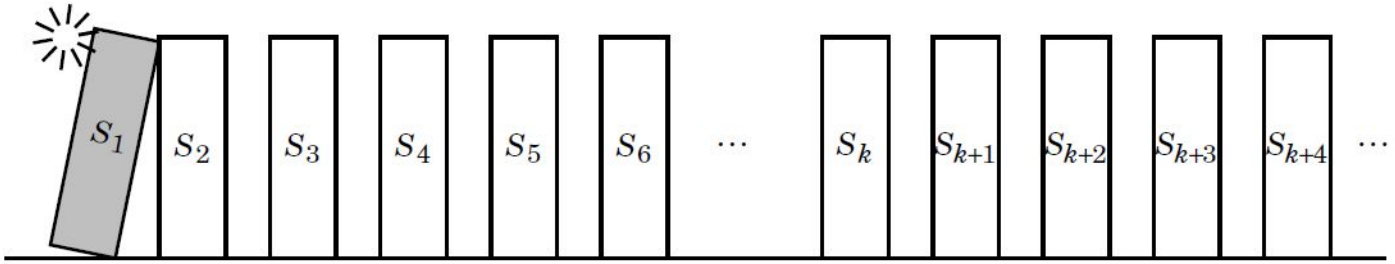


FIGURE 2 Illustrating How Mathematical Induction Works Using Dominoes.

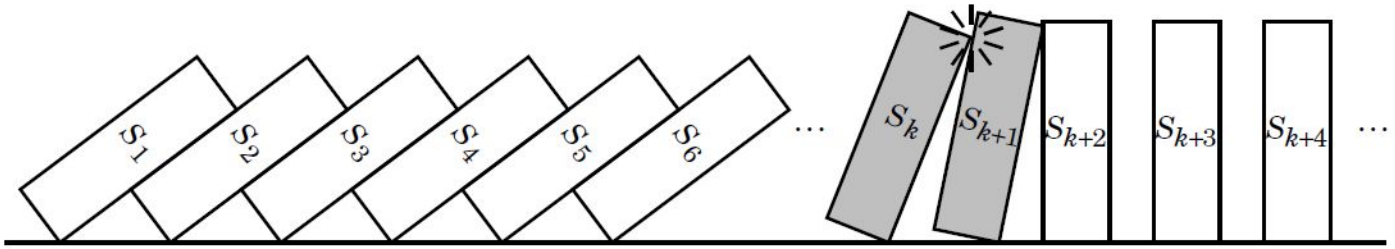
The Simple Idea Behind Mathematical Induction



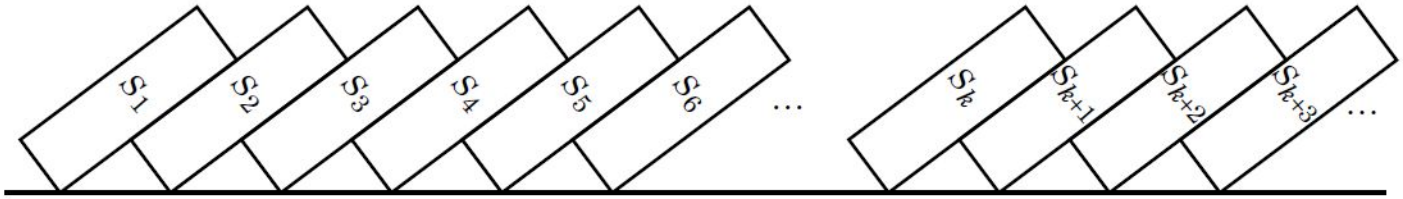
Statements are lined up like dominoes.



(1) Suppose the first statement falls (i.e. is proved true);



(2) Suppose the k^{th} falling always causes the $(k+1)^{th}$ to fall;



Then all must fall (i.e. all statements are proved true).

PRINCIPLE OF MATHEMATICAL INDUCTION:

Let P(n) be a propositional function defined for all positive integers n. P(n) is true for every positive integer n if

1.Basis Step:

The proposition P(1) is true.

2.Inductive Step:

If P(k) is true then P(k + 1) is true for all integers $k \geq 1$.

i.e. $\forall k \quad p(k) \rightarrow P(k+1)$

EXAMPLE:

Use Mathematical Induction to prove that

$$1+2+3+\cdots+n=\frac{n(n+1)}{2} \quad \text{for all integers } n \geq 1$$

SOLUTION:

Let $$P(n):1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

1.Basis Step:

P(1) is true.

For n = 1, left hand side of P(1) is the sum of all the successive integers starting at 1 and ending at 1, so LHS = 1 and RHS is

$$R.H.S=\frac{1(1+1)}{2}=\frac{2}{2}=1$$

so the proposition is true for n = 1.

2. Inductive Step: Suppose P(k) is true for, some integers $k \geq 1$.

(1) $$1+2+3+\cdots+k=\frac{k(k+1)}{2}$$

To prove P(k + 1) is true. That is,

$$(2) \qquad 1+2+3+\cdots+(k+1)=\frac{(k+1)(k+2)}{2}$$

Consider L.H.S. of (2)

$$1+2+3+\cdots+(k+1) = 1+2+3+\cdots+k+(k+1)$$

$$= \frac{k(k+1)}{2}+(k+1) \qquad \text{using (1)}$$

$$= (k+1)\left[\frac{k}{2}+1\right]$$

$$= (k+1)\left[\frac{k+2}{2}\right]$$

$$= \frac{(k+1)(k+2)}{2} = \text{RHS of (2)}$$

Hence by principle of Mathematical Induction the given result true for all integers greater or equal to 1.

EXERCISE:

Use mathematical induction to prove that
$1+3+5+\ldots+(2n-1) = n^2$ for all integers $n \geq 1$.

SOLUTION:

Let P(n) be the equation $1+3+5+\ldots+(2n-1) = n^2$

1. **Basis Step:**

   P(1) is true
   For n = 1, L.H.S of P(1) = 1and
   R.H.S = $1^2 = 1$
   Hence the equation is true for n = 1

2. **Inductive Step:**

   Suppose P(k) is true for some integer $k \geq 1$. That is,
   $1 + 3 + 5 + \ldots + (2k - 1) = k^2$ .....(1)

To prove P(k+1) is true; i.e.,
$1 + 3 + 5 + \ldots + [2(k+1)-1] = (k+1)^2$ .....(2)

Consider L.H.S. of (2)

$$1+3+5+\cdots+[2(k+1)-1] = 1+3+5+\cdots+(2k+1)$$
$$= 1+3+5+\cdots+(2k-1)+(2k+1)$$
$$= k^2+(2k+1) \quad \text{using (1)}$$
$$= (k+1)^2$$
$$= \text{R.H.S. of (2)}$$

Thus P(k+1) is also true. Hence by mathematical induction, the given equation is true for all integers $n \geq 1$.

Exercise (cont.)

Proof.

1. $P(n)$: $2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$
2. Basis step $P(0)$: $2^0 = 1 = 2^{0+1} - 1$.
3. Inductive step:
   Inductive hypothesis $P(k)$: $2^0 + 2^1 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$
   Let's prove $P(k+1)$:

$$\begin{aligned} 2^0 + 2^1 + 2^2 + \cdots + 2^k + 2^{k+1} &= 2^{k+1} - 1 + 2^{k+1} && \text{(by IH)} \\ &= 2(2^{k+1}) - 1 && \text{(by arithmetic)} \\ &= 2^{k+2} - 1 && \text{(by arithmetic)} \end{aligned}$$

Number Theory and Cryptography

Chapter 4

Chapter Motivation

- *Number theory* is the part of mathematics devoted to the study of the integers and their properties.
- Key ideas in number theory include divisibility and the primality of integers.
- Number theory has long been studied because of the beauty of its ideas, its accessibility, and its wealth of open questions.
- We'll use many ideas developed in Chapter 1 about proof methods and proof strategy in our exploration of number theory.
- Mathematicians have long considered number theory to be pure mathematics, but it has important applications to computer science and cryptography studied in Sections 4.5 and 4.6.

Chapter Summary

- Divisibility and Modular Arithmetic
- Primes and Greatest Common Divisors
- Solving Congruencies
- Applications of Congruencies
- Cryptography

Divisibility and Modular Arithmetic

Section 4.1

Section Summary

- Division
- Division Algorithm
- Modular Arithmetic

Division

Definition: If a and b are integers with $a \neq 0$, then a *divides* b if there exists an integer c such that $b = ac$.

- When a divides b we say that a is a *factor* or *divisor* of b and that b is a multiple of a.
- The notation $a \mid b$ denotes that a divides b.
- If $a \mid b$, then b/a is an integer.
- If a does not divide b, we write $a \nmid b$.

Example: Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Properties of Divisibility

Theorem 1: Let a, b, and c be integers, where $a \neq 0$.

i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

ii. If $a \mid b$, then $a \mid bc$ for all integers c;

iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: (i) Suppose $a \mid b$ and $a \mid c$, then it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

$b + c = as + at = a(s + t)$. Hence, $a \mid (b + c)$

(Exercises 3 and 4 ask for proofs of parts (ii) and (iii).) ◀

Corollary: If a, b, and c be integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Can you show how it follows easily from from (ii) and (i) of Theorem 1?

Division Algorithm

- When an integer is divided by a positive integer, there is a quotient and a remainder. This is traditionally called the "Division Algorithm," but is really a theorem.

Division Algorithm: If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$ (*proved in Section* 5.2).

- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.

Definitions of Functions **div** and **mod**

$q = a$ **div** d

$r = a$ **mod** d

Examples:

- What are the quotient and remainder when 101 is divided by 11?

  Solution: The quotient when 101 is divided by 11 is 9 = 101 **div** 11, and the remainder is 2 = 101 **mod** 11.

- What are the quotient and remainder when −11 is divided by 3?

  Solution: The quotient when −11 is divided by 3 is −4 = −11 **div** 3, and the remainder is 1 = −11 **mod** 3.

Congruence Relation

Definition: If a and b are integers and m is a positive integer, then a is *congruent* to b *modulo* m if m divides $a - b$.

- The notation $a \equiv b \pmod{m}$ says that a is congruent to b modulo m.
- We say that $a \equiv b \pmod{m}$ is a *congruence* and that m is its *modulus*.
- Two integers are congruent mod m if and only if they have the same remainder when divided by m.
- If a is not congruent to b modulo m, we write

$$a \not\equiv b \pmod{m}$$

Example: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution:

- $17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$.
- $24 \not\equiv 14 \pmod{6}$ since 6 divides $24 - 14 = 10$ is not divisible by 6.

More on Congruences

Theorem 4: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof:

- If $a \equiv b \pmod{m}$, then (by the definition of congruence) $m \mid a - b$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$.
- Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m \mid a - b$ and $a \equiv b \pmod{m}$.

◀

The Relationship between (mod m) and **mod** m Notations

- The use of "mod" in $a \equiv b \pmod{m}$ and $a \bmod m = b$ are different.
  - $a \equiv b \pmod{m}$ is a relation on the set of integers.
  - In $a \bmod m = b$, the notation **mod** denotes a function.
- The relationship between these notations is made clear in this theorem.
- **Theorem 3**: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$. (*Proof in the exercises*)

Congruencies of Sums and Products

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \text{ and } ac \equiv bd \pmod{m}$$

Example: Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from Theorem 5 that

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

$$77 = 7 \ 11 \equiv 2 * 1 = 2 \pmod{5}$$

Algebraic Manipulation of Congruencies

- Multiplying both sides of a valid congruence by an integer preserves validity.

  If $a \equiv b \pmod{m}$ holds then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer, holds by Theorem 5 with $d = c$.

- Adding an integer to both sides of a valid congruence preserves validity.

  If $a \equiv b \pmod{m}$ holds then $c + a \equiv c + b \pmod{m}$, where c is any integer, holds by Theorem 5 with $d = c$.

- Dividing a congruence by an integer does not always produce a valid congruence.

  Example: The congruence $14 \equiv 8 \pmod{6}$ holds. But dividing both sides by 2 does not produce a valid congruence since $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod{6}$.

Computing the **mod** *m* Function of Products and Sums

- We use the following corollary to Theorem 5 to compute the remainder of the product or sum of two integers when divided by m from the remainders when each is divided by m.

  Corollary: Let m be a positive integer and let a and b be integers. Then

  $(a + b) \pmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

  and

  $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$.

  (*proof in text*)

Applications of Congruences

Section Summary

- Hashing Functions
- Pseudorandom Numbers
- Check Digits

Hashing Functions

Definition: A *hashing function h* assigns memory location $h(k)$ to the record that has k as its key.

- A common hashing function is $h(k) = k$ **mod** m, where m is the number of memory locations.
- Because this hashing function is onto, all memory locations are possible.

Example: Let $h(k) = k$ **mod** 111. This hashing function assigns the records of customers with social security numbers as keys to memory locations in the following manner:

h(064212848) = 064212848 **mod** 111 = 14

h(037149212) = 037149212 **mod** 111 = 65

h(107405723) = 107405723 **mod** 111 = 14, but since location 14 is already occupied, the record is assigned to the next available position, which is 15.

- The hashing function is not one-to-one as there are many more possible keys than memory locations. When more than one record is assigned to the same location, we say a *collision* occurs. Here a collision has been resolved by assigning the record to the first free location.
- For collision resolution, we can use a *linear probing function*:

  $h(k,i) = (h(k) + i)$ **mod** m, where i runs from 0 to $m - 1$.
- There are many other methods of handling with collisions. You may cover these in a later CS course.

Pseudorandom Numbers

- Randomly chosen numbers are needed for many purposes, including computer simulations.
- *Pseudorandom numbers* are not truly random since they are generated by systematic methods.
- The *linear congruential method* is one commonly used procedure for generating pseudorandom numbers.
- Four integers are needed: the *modulus m*, the *multiplier a*, the *increment c*, and *seed* x_0, with $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$.
- We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \leq x_n < m$ for all n, by successively using the recursively defined function

$$x_{n+1} = (ax_n + c) \bmod m.$$

(*an example of a recursive definition, discussed in Section* 5.3*)*

- If psudorandom numbers between 0 and 1 are needed, then the generated numbers are divided by the modulus, x_n/m.

Pseudorandom Numbers

- **Example**: Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x_0 = 3$.
- **Solution**: Compute the terms of the sequence by successively using the congruence $x_{n+1} = (7x_n + 4) \bmod 9$, with $x_0 = 3$.

$x_1 = 7x_0 + 4 \bmod 9 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7,$
$x_2 = 7x_1 + 4 \bmod 9 = 7 \cdot 7 + 4 \bmod 9 = 53 \bmod 9 = 8,$
$x_3 = 7x_2 + 4 \bmod 9 = 7 \cdot 8 + 4 \bmod 9 = 60 \bmod 9 = 6,$
$x_4 = 7x_3 + 4 \bmod 9 = 7 \cdot 6 + 4 \bmod 9 = 46 \bmod 9 = 1,$
$x_5 = 7x_4 + 4 \bmod 9 = 7 \cdot 1 + 4 \bmod 9 = 11 \bmod 9 = 2,$
$x_6 = 7x_5 + 4 \bmod 9 = 7 \cdot 2 + 4 \bmod 9 = 18 \bmod 9 = 0,$
$x_7 = 7x_6 + 4 \bmod 9 = 7 \cdot 0 + 4 \bmod 9 = 4 \bmod 9 = 4,$
$x_8 = 7x_7 + 4 \bmod 9 = 7 \cdot 4 + 4 \bmod 9 = 32 \bmod 9 = 5,$
$x_9 = 7x_8 + 4 \bmod 9 = 7 \cdot 5 + 4 \bmod 9 = 39 \bmod 9 = 3.$

The sequence generated is 3,7,8,6,1,2,0,4,5,3,7,8,6,1,2,0,4,5,3,…

It repeats after generating 9 terms.

- Commonly, computers use a linear congruential generator with increment $c = 0$. This is called a *pure multiplicative generator*. Such a generator with modulus $2^{31} - 1$ and multiplier $7^5 = 16{,}807$ generates $2^{31} - 2$ numbers before repeating.

Check Digits: UPCs

- A common method of detecting errors in strings of digits is to add an extra digit at the end, which is evaluated using a function. If the final digit is not correct, then the string is assumed not to be correct.

Example: Retail products are identified by their *Universal Product Codes* (*UPC*s). Usually these have 12 decimal digits, the last one being the check digit. The check digit is determined by the congruence:

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}.$$

a. Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

b. Is 041331021641 a valid UPC?

Solution:

c. $3\cdot 7 + 9 + 3\cdot 3 + 5 + 3\cdot 7 + 3 + 3\cdot 4 + 3 + 3\cdot 1 + 0 + 3\cdot 4 + x_{12} \equiv 0 \pmod{10}$

$21 + 9 + 9 + 5 + 21 + 3 + 12 + 3 + 3 + 0 + 12 + x_{12} \equiv 0 \pmod{10}$

$98 + x_{12} \equiv 0 \pmod{10}$

$x_{12} \equiv 0 \pmod{10}$ So, the check digit is 2.

b. $3\cdot 0 + 4 + 3\cdot 1 + 3 + 3\cdot 3 + 1 + 3\cdot 0 + 2 + 3\cdot 1 + 6 + 3\cdot 4 + 1 \equiv 0 \pmod{10}$

$0 + 4 + 3 + 3 + 9 + 1 + 0 + 2 + 3 + 6 + 12 + 1 = 44 \equiv 4 \not\equiv \pmod{10}$

Hence, 041331021641 is not a valid UPC.

Check Digits:ISBNs

Books are identified by an *International Standard Book Number* (ISBN-10), a 10 digit code. The first 9 digits identify the language, the publisher, and the book. The tenth digit is a check digit, which is determined by the following congruence

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}.$$

The validity of an ISBN-10 number can be evaluated with the equivalent $\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}$.

a. Suppose that the first 9 digits of the ISBN-10 are 007288008. What is the check digit?

b. Is 084930149X a valid ISBN10?

Solution:

a. $X_{10} \equiv 1\cdot 0 + 2\cdot 0 + 3\cdot 7 + 4\cdot 2 + 5\cdot 8 + 6\cdot 8 + 7\cdot 0 + 8\cdot 0 + 9\cdot 8 \pmod{11}$.
$X_{10} \equiv 0 + 0 + 21 + 8 + 40 + 48 + 0 + 0 + 72 \pmod{11}$.
$X_{10} \equiv 189 \equiv 2 \pmod{11}$. Hence, $X_{10} = 2$.

X is used for the digit 10.

b. $1\cdot 0 + 2\cdot 8 + 3\cdot 4 + 4\cdot 9 + 5\cdot 3 + 6\cdot 0 + 7\cdot 1 + 8\cdot 4 + 9\cdot 9 + 10\cdot 10 =$
$0 + 16 + 12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 = 299 \equiv 2 \not\equiv 0 \pmod{11}$
Hence, 084930149X is not a valid ISBN-10.

- A *single error* is an error in one digit of an identification number and a *transposition error* is the accidental interchanging of two digits. Both of these kinds of errors can be detected by the check digit for ISBN-10. (*see text for more details*)

Arithmetic Modulo *m*

Definitions: Let $\mathbf{Z}_m$ be the set of nonnegative integers less than m: $\{0,1, \ldots., m-1\}$

- The operation $+_m$ is defined as $a +_m b = (a + b)$ **mod** m. This is *addition modulo m*.
- The operation $\cdot_m$ is defined as $a \cdot_m b = (a \,.\, b)$ **mod** m. This is *multiplication modulo m*.
- Using these operations is said to be doing *arithmetic modulo m*.

Example: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution: Using the definitions above:

- $7 +_{11} 9 = (7 + 9)$ **mod** $11 = 16$ **mod** $11 = 5$
- $7 \cdot_{11} 9 = (7 \cdot 9)$ **mod** $11 = 63$ **mod** $11 = 8$

Arithmetic Modulo *m*

- The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication.
  - *Closure*: If a and b belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.
  - *Associativity*: If a, b, and c belong to $\mathbf{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
  - *Commutativity*: If a and b belong to $\mathbf{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
  - *Identity elements*: The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively.
    - If a belongs to $\mathbf{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

continued →

Arithmetic Modulo *m*

- *Additive inverses*: If $a \neq 0$ belongs to $\mathbf{Z}_m$, then $m - a$ is the additive inverse of a modulo m and 0 is its own additive inverse.
  - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$
- *Distributivity*: If a, b, and c belong to $\mathbf{Z}_m$, then
  - $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.
- Exercises 42-44 ask for proofs of these properties.
- Multiplicatative inverses have not been included since they do not always exist. For example, there is no multiplicative inverse of 2 modulo 6.
- (*optional*) Using the terminology of abstract algebra, $\mathbf{Z}_m$ with $+_m$ is a commutative group and $\mathbf{Z}_m$ with $+_m$ and $\cdot_m$ is a commutative ring.

Primes and Greatest Common Divisors

Section 4.3

Section Summary

- Prime Numbers and their Properties
- Greatest Common Divisors and Least Common Multiples
- The Euclidian Algorithm
- gcds as Linear Combinations

Primes

Definition: A positive integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

Example: The integer 7 is prime because its only positive factors are 1 and 7, but 9 is composite because it is divisible by 3.

The Fundamental Theorem of Arithmetic

Theorem: Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non decreasing size.

Examples:

- $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
- $641 = 641$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
- $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

The Sieve of Erastosthenes

TABLE 1 The Sieve of Eratosthenes.

Integers divisible by 2 other than 2 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 3 other than 3 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 5 other than 5 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

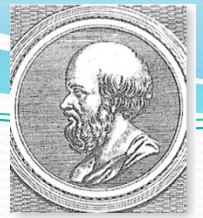
Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

If an integer n is a composite integer, then it has a prime divisor less than or equal to $\sqrt{n}$.

To see this, note that if $n = ab$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Trial division, a very inefficient method of determining if a number n is prime, is to try every integer $i \leq \sqrt{n}$ and see if n is divisible by i.



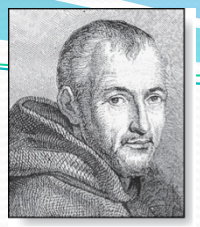
Erastothenes
(276-194 B.C.)

The Sieve of Erastosthenes

- The *Sieve of Erastosthenes* can be used to find all primes not exceeding a specified positive integer. For example, begin with the list of integers between 1 and 100.
  a. Delete all the integers, other than 2, divisible by 2.
  b. Delete all the integers, other than 3, divisible by 3.
  c. Next, delete all the integers, other than 5, divisible by 5.
  d. Next, delete all the integers, other than 7, divisible by 7.
  e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are:

{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89, 97}

continued →



Marin Mersenne
(1588-1648)

Mersenne Primes

Definition: Prime numbers of the form $2^p - 1$, where p is prime, are called *Mersenne primes*.

- $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$, and $2^7 - 1 = 127$ are Mersenne primes.
- $2^{11} - 1 = 2047$ is not a Mersenne prime since $2047 = 23 \cdot 89$.
- There is an efficient test for determining if $2^p - 1$ is prime.
- The largest known prime numbers are Mersenne primes.
- As of mid 2011, 47 Mersenne primes were known, the largest is $2^{43,112,609} - 1$, which has nearly 13 million decimal digits.
- The *Great Internet Mersenne Prime Search* (*GIMPS*) is a distributed computing project to search for new Mersenne Primes.

http://www.mersenne.org/

Greatest Common Divisor

Definition: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and also $d \mid b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by $\gcd(a,b)$.

One can find greatest common divisors of small numbers by inspection.

Example: What is the greatest common divisor of 24 and 36?

Solution: $\gcd(24,36) = 12$

Example: What is the greatest common divisor of 17 and 22?

Solution: $\gcd(17,22) = 1$

Greatest Common Divisor

Definition: The integers a and b are *relatively prime* if their greatest common divisor is 1.

Example: 17 and 22

Definition: The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Example: Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

Solution: Because gcd(10,17) = 1, gcd(10,21) = 1, and gcd(17,21) = 1, 10, 17, and 21 are pairwise relatively prime.

Example: Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution: Because gcd(10,24) = 2, 10, 19, and 24 are not pairwise relatively prime.

Finding the Greatest Common Divisor Using Prime Factorizations

- Suppose the prime factorizations of a and b are:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} , \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n} ,$$

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)} .$$

- This formula is valid since the integer on the right (of the equals sign) divides both a and b. No larger integer can divide both a and b.

Example: $120 = 2^3 \cdot 3 \cdot 5 \qquad 500 = 2^2 \cdot 5^3$

$\gcd(120,500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$

- Finding the gcd of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Least Common Multiple

Definition: The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by $\text{lcm}(a,b)$.

- The least common multiple can also be computed from the prime factorizations.

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

This number is divided by both a and b and no smaller number is divided by a and b.

Example: $\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)}\ 3^{\max(5,3)}\ 7^{\max(2,0)} = 2^4\ 3^5\ 7^2$

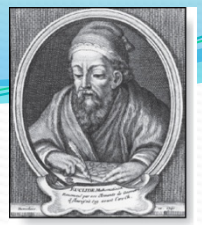
- The greatest common divisor and the least common multiple of two integers are related by:

Theorem 5: Let a and b be positive integers. Then

$$ab = \gcd(a,b) \cdot \text{lcm}(a,b)$$

(*proof is Exercise* 31)

Euclidean Algorithm



Euclid
(325 B.C.E. – 265 B.C.E.)

- The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that gcd(a,b) is equal to gcd(a,c) when $a > b$ and c is the remainder when a is divided by b.

Example: Find gcd(91, 287):

- $287 = 91 \cdot 3 + 14$
- $91 = 14 \cdot 6 + 7$
- $14 = 7 \cdot 2 + 0$

Divide 287 by 91

Divide 91 by 14

Divide 14 by 7

Stopping condition

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$$

continued →

Euclidean Algorithm

- The Euclidean algorithm expressed in pseudocode is:

```
procedure gcd(a, b: positive integers)
x := a
x := b
while   y ≠ 0
      r := x mod y
      x := y
      y := r
return x {gcd(a,b) is x}
```

- In Section 5.3, we'll see that the time complexity of the algorithm is $O(\log b)$, where $a > b$.

Étienne Bézout
(1730-1783)

gcds as Linear Combinations

Bézout's Theorem: If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$.

Definition: If a and b are positive integers, then integers s and t such that $\gcd(a,b) = sa + tb$ are called *Bézout coefficients* of a and b. The equation $\gcd(a,b) = sa + tb$ is called *Bézout's identity*.

- By Bézout's Theorem, the gcd of integers a and b can be expressed in the form $sa + tb$ where s and t are integers. This is a *linear combination* with integer coefficients of a and b.
  - $\gcd(6,14) = (-2)\cdot 6 + 1\cdot 14$

Finding gcds as Linear Combinations

Example: Express gcd(252,198) = 18 as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show gcd(252,198) = 18

i. $252 = 1 \cdot 198 + 54$
ii. $198 = 3 \cdot 54 + 36$
iii. $54 = 1 \cdot 36 + 18$
iv. $36 = 2 \cdot 18$

- Now working backwards, from iii and i above
  - $18 = 54 - 1 \cdot 36$
  - $36 = 198 - 3 \cdot 54$
- Substituting the 2nd equation into the 1st yields:
  - $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$
- Substituting $54 = 252 - 1 \cdot 198$ (from i)) yields:
  - $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

- This method illustrated above is a two pass method. It first uses the Euclidian algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers. A one pass method, called the *extended Euclidean algorithm*, is developed in the exercises.

Dividing Congruencies by an Integer

- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence (see Section 4.1).
- But dividing by an integer relatively prime to the modulus does produce a valid congruence:

  Theorem 7: Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c,m) = 1$, then $a \equiv b \pmod{m}$.

  Proof: Since $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$ by Lemma 2 and the fact that $\gcd(c,m) = 1$, it follows that $m \mid a - b$. Hence, $a \equiv b \pmod{m}$. ◀

Solving Congruencies

Section 4.4

Section Summary

- Linear Congruencies
- The Chinese Remainder Theorem
- Fermat's Little Theorem
- Pseudo primes

Linear Congruencies

Definition: A congruence of the form

$$ax \equiv b \pmod{m},$$

where m is a positive integer, a and b are integers, and x is a variable, is called a *linear congruence*.

- The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

Definition: An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an *inverse* of a modulo m.

Example: 5 is an inverse of 3 modulo 7 since $5 \cdot 3 = 15 \equiv 1 \pmod{7}$

- One method of solving linear congruencies makes use of an inverse $\bar{a}$, if it exists. Although we can not divide both sides of the congruence by a, we can multiply by $\bar{a}$ to solve for x.

Inverse of a modulo m

- The following theorem guarantees that an inverse of a modulo m exists whenever a and m are relatively prime. Two integers a and b are relatively prime when $\gcd(a,b) = 1$.

Theorem 1: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (This means that there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.)

Proof: Since $\gcd(a,m) = 1$, by Theorem 6 of Section 4.3, there are integers s and t such that $sa + tm = 1$.

- Hence, $sa + tm \equiv 1 \pmod{m}$.
- Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$
- Consequently, s is an inverse of a modulo m.
- The uniqueness of the inverse is Exercise 7. ◀

Finding Inverses

- The Euclidean algorithm and Bézout coefficients gives us a systematic approaches to finding inverses.

  Example: Find an inverse of 3 modulo 7.

  Solution: Because gcd(3,7) = 1, by Theorem 1, an inverse of 3 modulo 7 exists.

  - Using the Euclidian algorithm: $7 = 2 \cdot 3 + 1$.
  - From this equation, we get $-2 \cdot 3 + 1 \cdot 7 = 1$, and see that -2 and 1 are Bézout coefficients of 3 and 7.
  - Hence, -2 is an inverse of 3 modulo 7.
  - Also every integer congruent to -2 modulo 7 is an inverse of 3 modulo 7, i.e., 5, -9, 12, etc.

Finding Inverses

Example: Find an inverse of 101 modulo 4620.

Solution: First use the Euclidian algorithm to show that gcd(101,4620) = 1.

$4620 = 45 \cdot 101 + 75$
$101 = 1 \cdot 75 + 26$
$75 = 2 \cdot 26 + 23$
$26 = 1 \cdot 23 + 3$
$23 = 7 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1$

Since the last nonzero remainder is 1, gcd(101,4260) = 1

Working Backwards:

$1 = 3 - 1 \cdot 2$
$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$
$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$
$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$
$1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75$
$= 26 \cdot 101 - 35 \cdot 75$
$1 = 26 \cdot 101 - 35 \cdot (42620 - 45 \cdot 101)$
$= -35 \cdot 42620 + 1601 \cdot 101$

Bézout coefficients : − 35 and 1601

1601 is an inverse of 101 modulo 42620

Using Inverses to Solve Congruences

- We can solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

Example: What are the solutions of the congruence $3x \equiv 4 \pmod{7}$.

Solution: We found that -2 is an inverse of 3 modulo 7 (two slides back). We multiply both sides of the congruence by -2 giving

$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}.$$

Because $-6 \equiv 1 \pmod{7}$ and $-8 \equiv 6 \pmod{7}$, it follows that if x is a solution, then $x \equiv -8 \equiv 6 \pmod{7}$

We need to determine if every x with $x \equiv 6 \pmod{7}$ is a solution. Assume that $x \equiv 6 \pmod{7}$. By Theorem 5 of Section 4.1, it follows that $3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod{7}$ which shows that all such x satisfy the congruence.

The solutions are the integers x such that $x \equiv 6 \pmod{7}$, namely, $6, 13, 20 \ldots$ and $-1, -8, -15, \ldots$

The Chinese Remainder Theorem

Theorem 2: (*The Chinese Remainder Theorem*) Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$.

(That is, there is a solution x with $0 \leq x < m$ and all other solutions are congruent modulo m to this solution.)

- **Proof**: We'll show that a solution exists by describing a way to construct the solution. Showing that the solution is unique modulo m is Exercise 30.

continued →

The Chinese Remainder Theorem

To construct a solution first let $M_k = m/m_k$ for $k = 1,2,\ldots,n$ and $m = m_1 m_2 \cdots m_n$.

Since $\gcd(m_k, M_k) = 1$, by Theorem 1, there is an integer y_k, an inverse of M_k modulo m_k, such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

Form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \pmod{m}$$

Note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo m_k.

Because $M_k y_k \equiv 1 \pmod{m_k}$, we see that $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, for $k = 1,2,\ldots,n$.

Hence, x is a simultaneous solution to the n congruences.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

The Chinese Remainder Theorem

Example: Consider the 3 congruences from Sun-Tsu's problem:

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

- Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_3 = m/5 = 21$, $M_3 = m/7 = 15$.
- We see that
  - 2 is an inverse of $M_1 = 35$ modulo 3 since $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$
  - 1 is an inverse of $M_2 = 21$ modulo 5 since $21 \equiv 1 \pmod 5$
  - 1 is an inverse of $M_3 = 15$ modulo 7 since $15 \equiv 1 \pmod 7$
- Hence,

$$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \pmod m$$
$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$$

- We have shown that 23 is the smallest positive integer that is a simultaneous solution. Check it!

The Chinese Remainder Theorem

Word Problem:

Jessica breeds rabbits. She's not sure exactly how many she has today, but as she was moving them about this morning, she noticed some things. When she fed them, in groups of 5, she had 4 left over. When she bathed them, in groups of 8, she had a group of 6 left over. She took them outside to romp in groups of 9, but then the last group consisted of only 8. She's positive that there are fewer than 250 rabbits - but how many does she have?

Solution:

We have the following congurences

$x \equiv 4 \pmod 5$,

$x \equiv 6 \pmod 8$,

$x \equiv 8 \pmod 9$.

Cryptography

Section Summary

- Classical Cryptography
- Cryptosystems
- Public Key Cryptography
- RSA Cryptosystem
- Fermat's Little theorem

Caesar Cipher

Julius Caesar created secret messages by shifting each letter three letters forward in the alphabet (sending the last three letters to the first three letters.) For example, the letter B is replaced by E and the letter X is replaced by A. This process of making a message secret is an example of *encryption*.

Here is how the encryption process works:

- Replace each letter by an integer from $\mathbf{Z}_{26}$, that is an integer from 0 to 25 representing one less than its position in the alphabet.
- The encryption function is $f(p) = (p + 3)$ **mod** 26. It replaces each integer p in the set $\{0,1,2,\ldots,25\}$ by $f(p)$ in the set $\{0,1,2,\ldots,25\}$.
- Replace each integer p by the letter with the position $p + 1$ in the alphabet.

Example: Encrypt the message "MEET YOU IN THE PARK" using the Caesar cipher.

Solution: 12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by $f(p) = (p + 3)$ **mod** 26.

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13.

Translating the numbers back to letters produces the encrypted message

"PHHW BRX LQ WKH SDUN."

Caesar Cipher

- To recover the original message, use $f^{-1}(p) = (p-3)$ **mod** 26. So, each letter in the coded message is shifted back three letters in the alphabet, with the first three letters sent to the last three letters. This process of recovering the original message from the encrypted message is called *decryption*.
- The Caesar cipher is one of a family of ciphers called *shift ciphers*. Letters can be shifted by an integer k, with 3 being just one possibility. The encryption function is

  $f(p) = (p + k)$ **mod** 26

  and the decryption function is

  $f^{-1}(p) = (p-k)$ **mod** 26

  The integer k is called a *key*.

Shift Cipher

Example 1: Encrypt the message "STOP GLOBAL WARMING" using the shift cipher with $k = 11$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

18 19 14 15 6 11 14 1 0 11 22 0 17 12 8 13 6.

Apply the shift $f(p) = (p + 11)$ **mod** 26, yielding

3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17.

Translating the numbers back to letters produces the ciphertext

"DEZA RWZMLW HLCXTYR."

Shift Cipher

Example 2: Decrypt the message "LEWLYPLUJL PZ H NYLHA ALHJOLY" that was encrypted using the shift cipher with $k = 7$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

11 4 22 11 24 15 11 20 9 11 15 25 7 13 24 11 7 0 0 11 7 9 14 11 24.

Shift each of the numbers by $-k = -7$ modulo 26, yielding

4 23 15 4 17 8 4 13 2 4 8 18 0 6 17 4 0 19 19 4 0 2 7 4 17.

Translating the numbers back to letters produces the decrypted message

"EXPERIENCE IS A GREAT TEACHER."

Number Theory in Cryptography

Terminology: Two parties **Alice** and **Bob** want to communicate securely s.t. a third party **Eve** who intercepts messages cannot learn the content of the messages.

Symmetric Cryptosystems: Alice and Bob share a secret. Only they know a secret key K that is used to encrypt and decrypt messages. Given a message M, Alice encodes it (possibly with padding) into m, and then sends the ciphertext $encrypt(m, K)$ to Bob. Then Bob uses K to decrypt it and obtains $decrypt(encrypt(m, K), K) = m$.
Example: AES.

Public Key Cryptosystems: Alice and Bob do a-priori **not** share a secret. How can they establish a shared secret when others are listening to their messages?

Idea: Have a two-part key, i.e., a key pair. A public key that is used to encrypt messages, and a secret key to decrypt them. Alice uses Bob's public key to encrypt a message (everyone can do that). Only Bob can decrypt the message with his secret key.

Description of RSA: Key generation

- Choose two distinct prime numbers p and q. Numbers p and q should be chosen at random, and be of similar bit-length. Prime integers can be efficiently found using a primality test.
- Let $n = pq$ and $k = (p-1)(q-1)$. (In particular, $k = |Z_n^*|$).
- Choose an integer e such that $1 < e < k$ and $gcd(e, k) = 1$; i.e., e and k are coprime.
  e (for encryption) is released as the public key exponent.
  (e must not be very small.)
- Let d be the multiplicative inverse of e modulo k, i.e., $de \equiv 1 (\mod k)$. (Computed using the extended Euclidean algorithm.) d (for decryption) is the private key and kept secret.

The public key is (n, e) and the private key is (n, d).

RSA: Encryption and Decryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret.

Encryption: Bob then wishes to send message M to Alice. He first turns M into an integer m, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to

$$c \equiv m^e \mod n$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

Decryption: Alice can recover m from c by using her private key exponent d via computing

$$m \equiv c^d \mod n$$

Given m, she can recover the original message M by reversing the padding scheme.

Using RSA

Given pubKey = <e, n> and privKey = <d, n>

If Message = m

Then:

encryption: $c = m^e \bmod n, m < n$

decryption: $m = c^d \bmod n$

signature: $s = md \bmod n, m < n$

verification: $m = se \bmod n$

Example of RSA (1)

Choose p = 7 and q = 17.

Compute n = p*q= 119.

Compute f(n)=(p-1)(q-1)=96.

Select e = 5, (a relatively prime to f(n).)

Compute d = _77_such that e*d=1 mod f(n).

- Public key: <5,119>
- Private key: <77,119>
- Message = 19
- Encryption: 19^5 mod 119 = 66
- Decryption: 66^{77} mod 119 = 19

Example of RSA (2)

p = 7, q = 11, n = 77

Alice chooses e = 17, making d = 53

Bob wants to send Alice secret message

HELLO (07 04 11 11 14)

– 07^{17} mod 77 = 28; 04^{17} mod 77 = 16

– 11^{17} mod 77 = 44; – 11^{17} mod 77 = 44

– 14^{17} mod 77 = 42

• Bob sends **28 16 44 44 42**

Example of RSA (3)

Alice receives **28 16 44 44 42**

Alice uses private key, d = 53, to decrypt message:

– 28^{53} mod 77 = 07; 16^{53} mod 77 = 04

– 44^{53} mod 77 = 11; 44^{53} mod 77 = 11

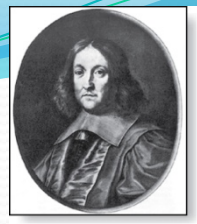
– 42^{53} mod 77 = 14

• Alice translates **07 04 11 11 14** to ***HELLO***

No one else could read it, as only Alice knows her private key (needed for decryption)

Fermat's Little Theorem

Pierre de Fermat
(1601-1665)



Theorem 3: (*Fermat's Little The*orem) If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$

Furthermore, for every integer a we have $a^p \equiv a \pmod{p}$

(*proof outlined in Exercise 19*)

Fermat's little theorem is useful in computing the remainders modulo p of large powers of integers.

Example: Find 7^{222} **mod** 11.

By Fermat's little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, and so $(7^{10})^k \equiv 1 \pmod{11}$, for every positive integer k. Therefore,

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

Hence, 7^{222} **mod** 11 = 5.

Counting

Chapter 6

Mr. Shoaib Raza

Chapter Summary

- The Basics of Counting
- The Pigeonhole Principle
- Permutations and Combinations
- Binomial Coefficients and Identities
- Generalized Permutations and Combinations

The Basics of Counting

Section 6.1

COMBINATORICS

- Combinatorics is the mathematics of counting and arranging objects. Counting of objects with certain properties (enumeration) is required to solve many different types of problem.
- Applications, include topics as diverse as codes, circuit design and algorithm complexity [and gambling]

Counting

- Enumeration, the counting of objects with certain properties, is an important part of combinatorics.
- We must count objects to solve many different types of problems. For example, counting is used to:

1. Determine number of ordered or unordered arrangement of objects.
2. Generate all the arrangements of a specified kind which is important in computer simulations.
3. Compute probabilities of events.
4. Analyze the chance of winning games, lotteries etc.
5. Determine the complexity of algorithms.

Section Summary

- The Sum Rule
- The Product Rule
- The Subtraction Rule
- The Division Rule
- Examples, Examples, and Examples
- Tree Diagrams

Basic Counting Principles: The Sum Rule

The Sum Rule: If a task can be done either in one of n_1 ways or in one of n_2 ways to do the second task, where none of the set of n_1 ways is the same as any of the n_2 ways, then there are $n_1 + n_2$ ways to do the task.

The Sum Rule in terms of sets.

- The sum rule can be phrased in terms of sets.

  $|A \cup B| = |A| + |B|$ as long as A and B are disjoint sets.

- Or more generally,

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = |A_1| + |A_2| + \cdots + |A_m|$$
$$\text{when } A_i \cap A_j = \varnothing \text{ for all } i, j.$$

- The case where the sets have elements in common will be discussed when we consider the subtraction rule and taken up fully in Chapter 8.

Basic Counting Principles: The Sum Rule

Example:

Suppose there are 7 different optional courses in Computer Science and 3 different optional courses in Mathematics. How many ways student can choose a course.

Solution: By the sum rule it follows that there are $7 + 3 = 10$ choices for a student who wants to take one optional course.

Basic Counting Principles: The Sum Rule

Example: The mathematics department must choose either a student or a faculty member as a representative for a university committee. How many choices are there for this representative if there are 37 members of the mathematics faculty and 83 mathematics majors and no one is both a faculty member and a student.

Solution: By the sum rule it follows that there are $37 + 83 = 120$ possible ways to pick a representative.

Basic Counting Principles: The Sum Rule

Example: A student can choose a computer project from one of the three lists. The three lists contain 23, 15 and 19 possible projects, respectively. How many possible projects are there to choose from?

Solution: The student can choose a project from the first list in 23 ways, from the second list in 15 ways, and from the third list in 19 ways. Hence, there are

$23 + 15 + 19 = 57$ projects to choose from.

Basic Counting Principles: The Product Rule

The Product Rule: A procedure can be broken down into a sequence of two tasks. There are n_1 ways to do the first task and n_2 ways to do the second task. Then there are $n_1 \cdot n_2$ ways to do the procedure.

Product Rule in Terms of Sets

- If $A_1, A_2, \ldots, A_m$ are finite sets, then the number of elements in the Cartesian product of these sets is the product of the number of elements of each set.
- The task of choosing an element in the Cartesian product $A_1 \times A_2 \times \cdots \times A_m$ is done by choosing an element in A_1, an element in A_2 , …, and an element in A_m.
- By the product rule, it follows that:

$$|A_1 \times A_2 \times \cdots \times A_m| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_m|.$$

The Product Rule

Example: How many ways a student can choose one optional course each from computer science and mathematics courses if there are 7 different optional courses in Computer Science and 3 different optional courses in Mathematics.

Solution:

A student who wants to take one optional course of each subject, there are $7 \times 3 = 21$ choices.

The Product Rule

Example: The chairs of an auditorium are to be labeled with two characters, a letter followed by a digit. What is the largest number of chairs that can be labeled differently?

Solution:

The procedure of labeling a chair consists of two events, namely,

Assigning one of the 26 letters: A, B, C, …, Z and

Assigning one of the 10 digits: 0, 1, 2, …, 9

By product rule, there are $26 \times 10 = 260$ different ways that a chair can be labeled by both a letter and a digit.

The Product Rule

Example: Find the number n of ways that an organization consisting of 15 members can elect a president, treasurer, and secretary. (assuming no person is elected to more than one position)

Solution:

The president can be elected in 15 different ways; following this, the treasurer can be elected in 14 different ways; and following this, the secretary can be elected in 13 different ways. Thus, by product rule, there are

$$n = 15 \times 14 \times 13 = 2730$$

different ways in which the organization can elect the officers.

The Product Rule

Example: There are four bus lines between A and B; and three bus lines between B and C.

Find the number of ways a person can travel:

a) By bus from A to C by way of B;

b) Round trip by bus from A to C by way of B;

c) Round trip by bus from A to C by way of B, if the person does not want to use a bus line more than once.

The Product Rule

a) By bus from A to C by way of B;

Solution:

$$A \xrightarrow{4} B \xrightarrow{3} C$$

There are 4 ways to go from A to B and 3 ways to go from B to C; hence there are $4 \times 3 = 12$ ways to go from A to C by way of B.

The Product Rule

b) Round trip by bus from A to C by way of B;

Solution:

The person will travel from A to B to C to B to A for the round trip. i.e. (A →B →C →B →A)

$$A \xrightarrow{4} B \xrightarrow{3} C \xrightarrow{3} B \xrightarrow{4} A$$

The person can travel 4 ways from A to B and 3 way from B to C and back.

Thus there are $4 \times 3 \times 3 \times 4 = 144$ ways to travel the round trip.

The Product Rule

c) Round trip by bus from A to C by way of B, if the person does not want to use a bus line more than once.

Solution:

$$A \xrightarrow{4} B \xrightarrow{3} C \xrightarrow{2} B \xrightarrow{3} A$$

The person can travel 4 ways from A to B and 3 ways from B to C, but only 2 ways from C to B and 3 ways from B to A, since bus line cannot be used more than once. Hence there are

$4 \times 3 \times 2 \times 3 = 72$ ways

to travel the round trip without using a bus line more than once.

The Product Rule

Example: A bit string is a sequence of 0's and 1's.How many bit string are there of length 4?

Solution:

Each bit (binary digit) is either 0 or 1.

Hence, there are 2 ways to choose each bit. Since we have to choose four bits therefore,

$$2 \times 2 \times 2 \times 2 = 2^4 = 16$$

the product rule shows, there are a total of different bit strings of length four.

The Product Rule

Example: How many bit strings of length 8:

(i) begin with a 1?

(ii) begin and end with a 1?

Solution:

(i) If the first bit (left most bit) is a 1, then it can be filled in only one way. Each of the remaining seven positions in the bit string can be filled in 2 ways (i.e., either by 0 or 1). Hence, there are

$$1 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^7 = 128$$

different bit strings of length 8 that begin with a 1.

The Product Rule

(ii) begin and end with a 1?

Solution:

If the first and last bit in an 8 bit string is a 1, then only the intermediate six bits can be filled in 2 ways, i.e. by a 0 or 1. Hence there are

$$1 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 1 = 2^6 = 64$$

different bit strings of length 8 that begin and end with a 1.

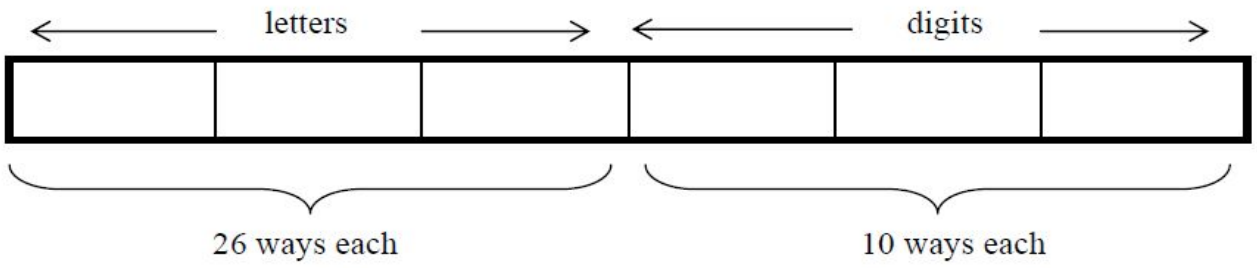
The Product Rule

Example: Suppose that an automobile license plate has three letters followed by three digits.

(a) How many different license plates are possible?

Solution:

Each of the three letters can be written in 26 different ways, and each of the three digits can be written in 10 different ways.



H

$26 \times 26 \times 26 \times 10 \times 10 \times 10 = 17{,}576{,}000$

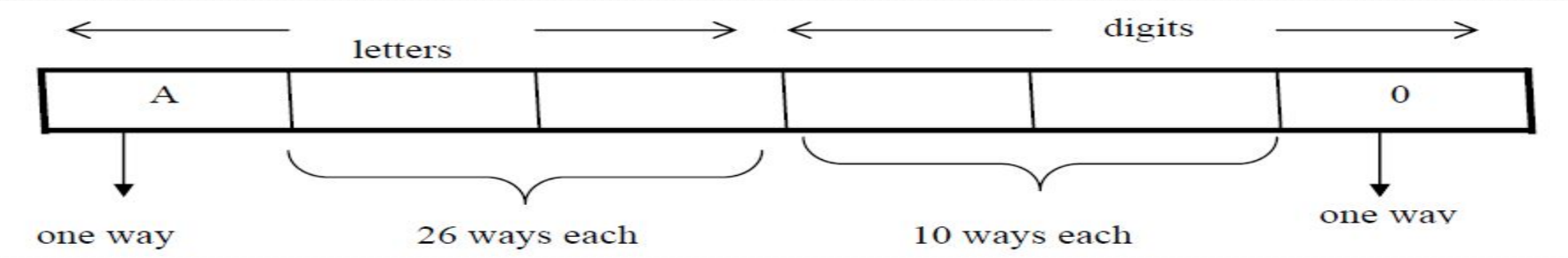
different License plates possible.

The Product Rule

(b) How many license plates could begin with A and end on 0?

Solution:

The first and last place can be filled in one way only, while each of second and third place can be filled in 26 ways and each of fourth and fifth place can be filled in 10 ways.



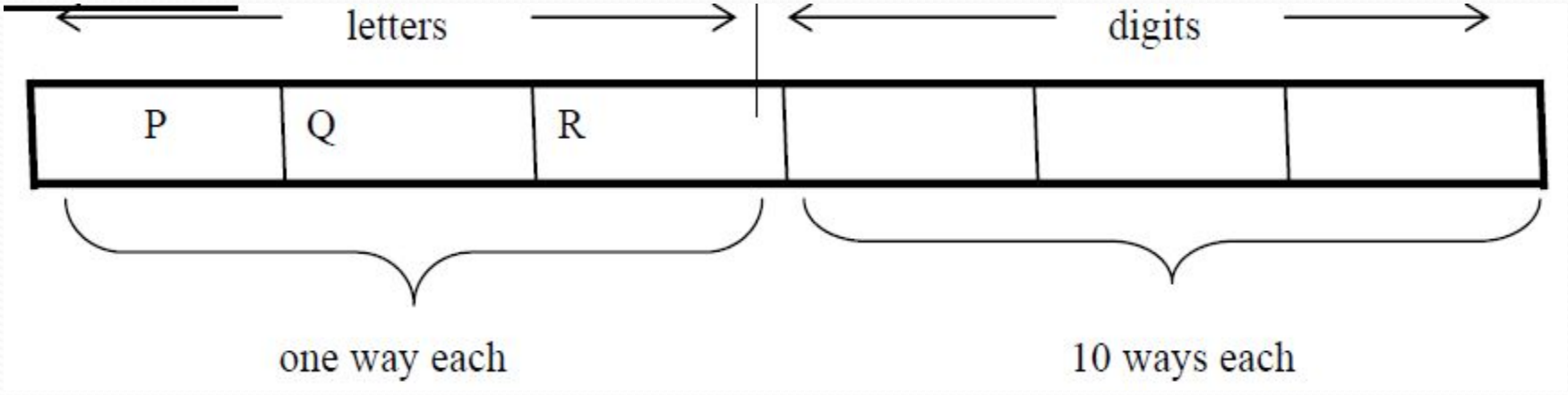
Number of license plates that begin with A and end in 0 are

$$1 \times 26 \times 26 \times 10 \times 10 \times 1 = 67600$$

The Product Rule

(c) How many license plates begin with PQR.

Solution:



Number of license plates that begin with PQR are

$$1 \times 1 \times 1 \times 10 \times 10 \times 10 = 1000 \text{ ways.}$$

The Product Rule

(d) How many license plates are possible in which all the letters and digits are distinct?

Solution:

The first letter place can be filled in 26 ways. Since, the second letter place should contain a different letter than the first, so it can be filled in 25 ways. Similarly, the third letter place can be filled in 24 ways. And the digits can be respectively filled in 10, 9, and 8 ways.

Hence;

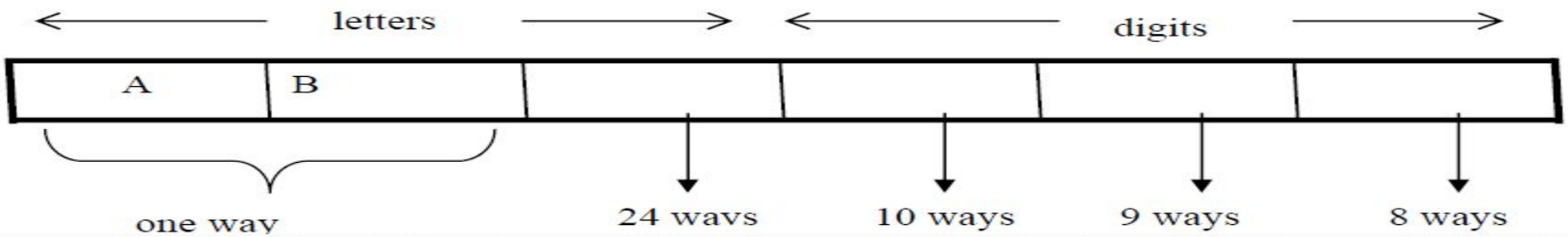
number of license plates in which all the letters and digits are distinct are

$$26 \times 25 \times 24 \times 10 \times 9 \times 8 = 11,232,000$$

The Product Rule

(e) How many license plates could begin with AB and have all three letters and digits distinct.

Solution:



The first two letters places are fixed (to be filled with A and B), so there is only one way to fill them. The third letter place should contain a letter different from A & B, so there

are 24 ways to fill it.

The three digit positions can be filled in 10 and 8 ways to have distinct digits. Hence, desired number of license plates are

$$1 \times 1 \times 24 \times 10 \times 9 \times 8 = 17280$$

Telephone Numbering Plan

Example: The *North American numbering plan* (*NANP*) specifies that a telephone number consists of 10 digits, consisting of a three-digit area code, a three-digit office code, and a four-digit station code. There are some restrictions on the digits.

- Let *X* denote a digit from 0 through 9.
- Let *N* denote a digit from 2 through 9.
- Let *Y* denote a digit that is 0 or 1.
- In the old plan (in use in the 1960s) the format was *NYX-NNX-XXXX*.
- In the new plan, the format is *NXX-NXX-XXXX*.

How many different telephone numbers are possible under the old plan and the new plan?

Solution: Use the Product Rule.

- There are $8 \cdot 2 \cdot 10 = 160$ area codes with the format *NYX*.
- There are $8 \cdot 10 \cdot 10 = 800$ area codes with the format *NXX*.
- There are $8 \cdot 8 \cdot 10 = 640$ office codes with the format *NNX*.
- There are $10 \cdot 10 \cdot 10 \cdot 10 = 10{,}000$ station codes with the format *XXXX*.

Number of old plan telephone numbers: $160 \cdot 640 \cdot 10{,}000 = 1{,}024{,}000{,}000$.

Number of new plan telephone numbers: $800 \cdot 800 \cdot 10{,}000 = 6{,}400{,}000{,}000$.

NUMBER OF ITERATIONS OF A NESTED LOOP

Example: Determine how many times the inner loop will be iterated when the following algorithm is implemented and run

For i: = 1 to 4

For j : = 1 to 3

[Statement in body of inner loop. None contain branching statements that lead out of the inner loop.]

next j

next i

Solution:

The outer loop is iterated four times, and during each iteration of the outer loop, there are three iterations of the inner loop.

Hence, by product rules the total number of iterations of inner loop is $4 \cdot 3 = 12$

Example: Determine how many times the inner loop will be iterated when the following algorithm is implemented and run.

for i = 5 to 50

for j: = 10 to 20

[Statement in body of inner loop. None contain branching statements that lead out of the inner loop.]

next j

next i

Solution:

The outer loop is iterated 50 - 5 + 1 = 46 times and during each iteration of the outer loop there are 20 - 10 + 1 = 11 iterations of the inner loop. Hence by product rule, the total number of iterations of the inner loop is 46×11 = 506.

Example: Determine how many times the inner loop will be iterated when the following algorithm is implemented and run.

```
for i: = 1 to 4
for j: = 1 to i
[Statements in body of inner loop. None contain branching statements that lead outside the loop.]
next j
next i
```

Solution:

The outer loop is iterated 4 times, but during each iteration of the outer loop, the inner loop iterates different number of times.

For first iteration of outer loop, inner loop iterates 1 times.

For second iteration of outer loop, inner loop iterates 2 times.

For third iteration of outer loop, inner loop iterates 3 times.

For fourth iteration of outer loop, inner loop iterates 4 times.

Hence, total number of iterations of inner loop = 1 + 2 + 3 + 4 = 10.

Combining the Sum and Product Rule

Example: Suppose statement labels in a programming language can be either a single letter or a letter followed by a digit. Find the number of possible labels.

Solution:

- First consider variable names one character in length. Since such names consist of a single letter, there are 26 variable names of length 1.
- Next, consider variable names two characters in length. Since the first character is a letter, there are 26 ways to choose it. The second character is a digit, there are 10 ways to choose it. Hence, to construct variable name of two characters in length, there are $26 \times 10 = 260$ ways.
- Finally, by sum rule, there are $26 + 260 = 286$ possible variable names in the programming language.

Combining the Sum and Product Rule

- **Example**: A computer access code word consists of from one to three letters of English alphabets with repetitions allowed. How many different code words are possible.

Solution:

Number of code words of length 1 = 26^1

Number of code words of length 2 = 26^2

Number of code words of length 3 = 26^3

Hence, the total number of code words =

$$26^1 + 26^2 + 26^3 = 18{,}278$$

Counting Passwords

- Combining the sum and product rule allows us to solve more complex problems.

Example: Each user on a computer system has a password, which is six to eight characters long, where each character is an uppercase letter or a digit. Each password must contain at least one digit. How many possible passwords are there?

Solution: Let P be the total number of passwords, and let P_6, P_7, and P_8 be the passwords of length 6, 7, and 8.

- By the sum rule $P = P_6 + P_7 + P_8$.

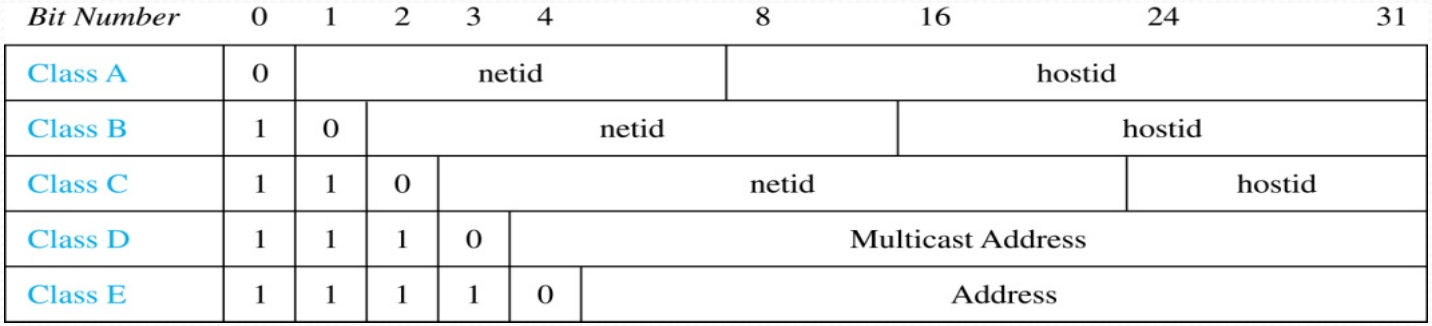
Finding P_6 directly is difficult. To find P_6 it is easier to find the number of strings of uppercase letters and digits that are six characters long, including those with no digits, and subtract from this the number of strings with no digits. By the product rule, the number of strings of six characters is 36^6 ,and the number of strings with no digits is 26^6

Counting Passwords(Continued)

- To find each of P6, P7, and P8 , we find the number of passwords of the specified length composed of letters and digits and subtract the number composed only of letters. We find that:
  - $P_6 = 36^6 - 26^6 = 2{,}176{,}782{,}336 - 308{,}915{,}776 = 1{,}867{,}866{,}560.$
  - $P_7 = 36^7 - 26^7 = 78{,}364{,}164{,}096 - 8{,}031{,}810{,}176 = 70{,}332{,}353{,}920.$
  - $P_8 = 36^8 - 26^8 = 2{,}821{,}109{,}907{,}456 - 208{,}827{,}064{,}576 = 2{,}612{,}282{,}842{,}880.$
  - Consequently, $P = P_6 + P_7 + P_8 = 2{,}684{,}483{,}063{,}360.$

Internet Addresses

- Version 4 of the Internet Protocol (IPv4) uses 32 bits.



Bit Number	0	1	2	3	4	8	16	24	31
Class A	0	netid				hostid			
Class B	1	0	netid				hostid		
Class C	1	1	0	netid				hostid	
Class D	1	1	1	0	Multicast Address				
Class E	1	1	1	1	0	Address			

- **Class A Addresses**: used for the largest networks, a 0,followed by a 7-bit netid and a 24-bit hostid.
- **Class B Addresses**: used for the medium-sized networks, a 10,followed by a 14-bit netid and a 16-bit hostid.
- **Class C Addresses**: used for the smallest networks, a 110,followed by a 21-bit netid and a 8-bit hostid.
  - Neither Class D nor Class E addresses are assigned as the address of a computer on the internet. Only Classes A, B, and C are available.
  - 1111111 is not available as the netid of a Class A network.
  - Hostids consisting of all 0s and all 1s are not available in any network.

Counting Internet Addresses

Example: How many different IPv4 addresses are available for computers on the internet?

Solution: Use both the sum and the product rule. Let x be the number of available addresses, and let x_A, x_B, and x_C denote the number of addresses for the respective classes.

- To find, x_A: $2^7 - 1 = 127$ netids. $2^{24} - 2 = 16{,}777{,}214$ hostids.
  $x_A = 127 \cdot 16{,}777{,}214 = 2{,}130{,}706{,}178.$
- To find, x_B: $2^{14} = 16{,}384$ netids. $2^{16} - 2 = 16{,}534$ hostids.
  $x_B = 16{,}384 \cdot 16{,}534 = 1{,}073{,}709{,}056.$
- To find, x_C: $2^{21} = 2{,}097{,}152$ netids. $2^8 - 2 = 254$ hostids.
  $x_C = 2{,}097{,}152 \cdot 254 = 532{,}676{,}608.$
- Hence, the total number of available IPv4 addresses is

$$\begin{aligned} x &= x_A + x_B + x_C \\ &= 2{,}130{,}706{,}178 + 1{,}073{,}709{,}056 + 532{,}676{,}608 \\ &= 3{,}737{,}091{,}842. \end{aligned}$$

Not Enough Today !!
The newer IPv6 protocol solves the problem of too few addresses.

Basic Counting Principles: Subtraction Rule

Subtraction Rule: If a task can be done either in one of n_1 ways or in one of n_2 ways, then the total number of ways to do the task is $n_1 + n_2$ minus the number of ways to do the task that are common to the two different ways.

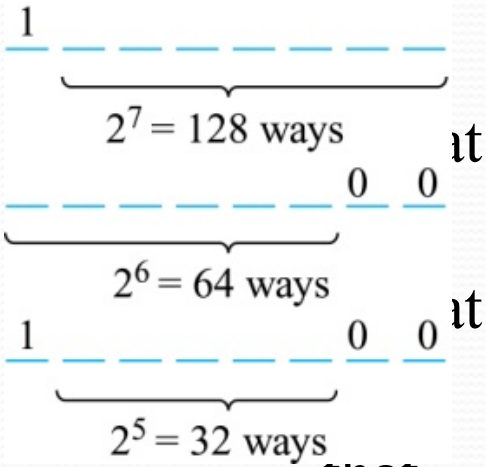
- Also known as, the *principle of inclusion-exclusion*:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Counting Bit Strings

Example: How many bit strings of length eight start either with a 1 bit or end with the two bits 00?

Solution: Use the subtraction rule.



- Number of bit strings of length eight start with a 1 bit: $2^7 = 128$
- Number of bit strings of length eight end with bits 00: $2^6 = 64$
- Number of bit strings of length eight start with a 1 bit and end with bits 00 : $2^5 = 32$

Hence, the number is $128 + 64 - 32 = 160$.

Counting Functions

Counting Functions: How many functions are there from a set with m elements to a set with n elements?

Solution: Since a function represents a choice of one of the n elements of the codomain for each of the m elements in the domain, the product rule tells us that there are $n \cdot n \cdot \cdots \ n = n^m$ such functions.

Counting One-to-One Functions: How many one-to-one functions are there from a set with m elements to one with n elements?

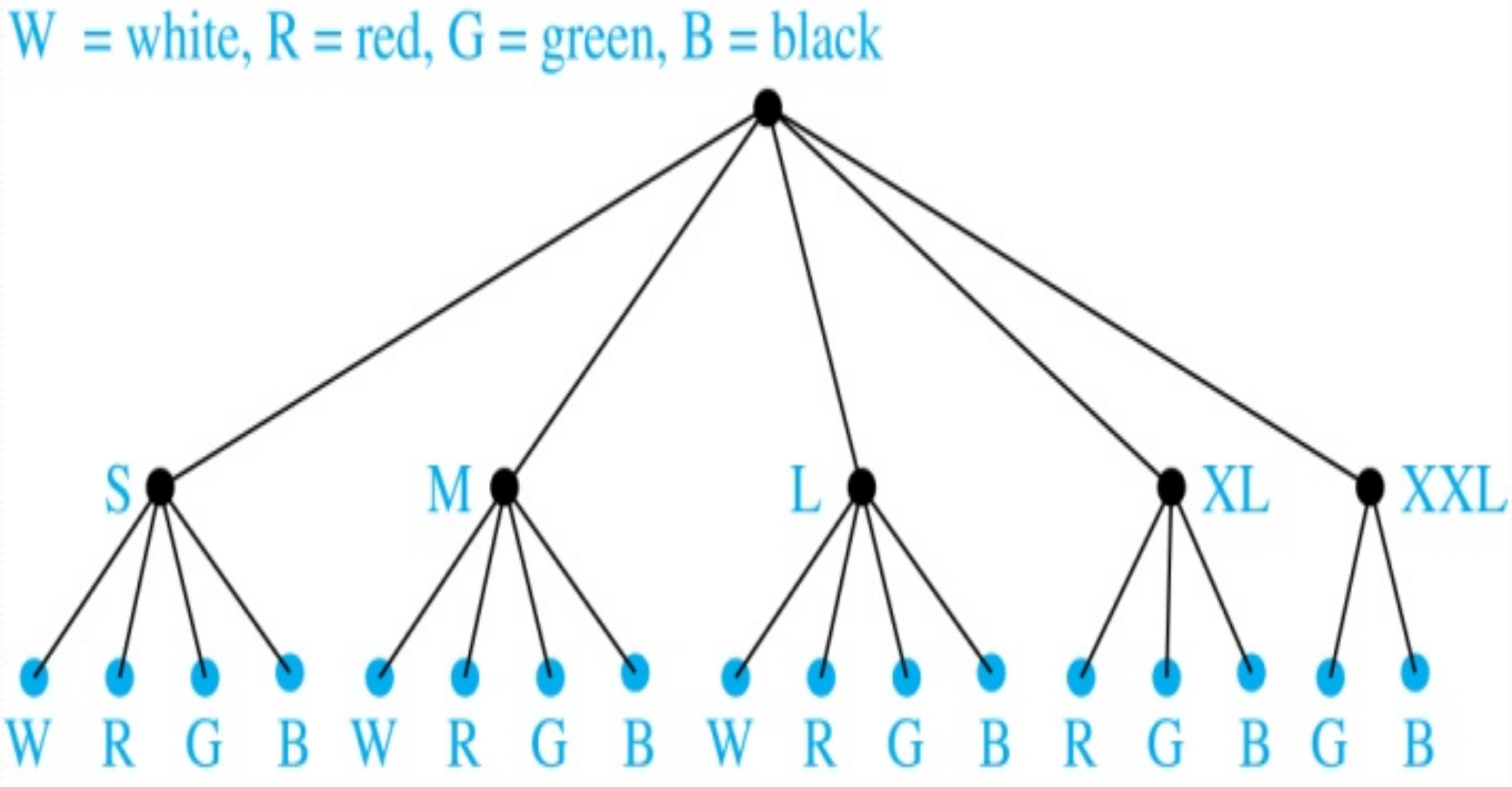
Solution: Suppose the elements in the domain are a_1, $a_2, \ldots, a_m$. There are n ways to choose the value of a_1 and $n-1$ ways to choose a_2, etc. The product rule tells us that there are $n(n-1)\,(n-2)\cdots(n-m+1)$ such functions.

Tree Diagrams

- **Tree Diagrams**: We can solve many counting problems through the use of *tree diagrams*, where a branch represents a possible choice and the leaves represent possible outcomes.
- **Example**: Suppose that "I Love Discrete Math" T-shirts come in five different sizes: S,M,L,XL, and XXL. Each size comes in four colors (white, red, green, and black), except XL, which comes only in red, green, and black, and XXL, which comes only in green and black. What is the minimum number of shirts that the campus book store needs to stock to have one of each size and color available?

Tree Diagrams

- **Solution**: Draw the tree diagram.



- The store must stock 17 T-shirts.

The Pigeonhole Principle

Section 6.2

Section Summary

- The Pigeonhole Principle
- The Generalized Pigeonhole Principle

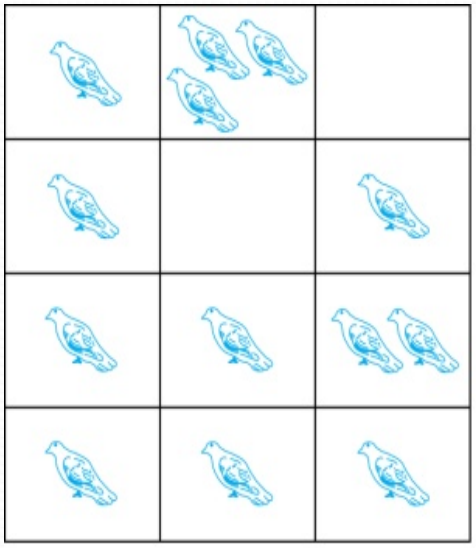
The Pigeonhole Principle

Pigeonhole Principle: If k is a positive integer and $k + 1$ objects are placed into k boxes, then at least one box contains two or more objects.

Proof: We use a proof by contraposition. Suppose none of the k boxes has more than one object. Then the total number of objects would be at most k. This contradicts the statement that we have $k + 1$ objects.

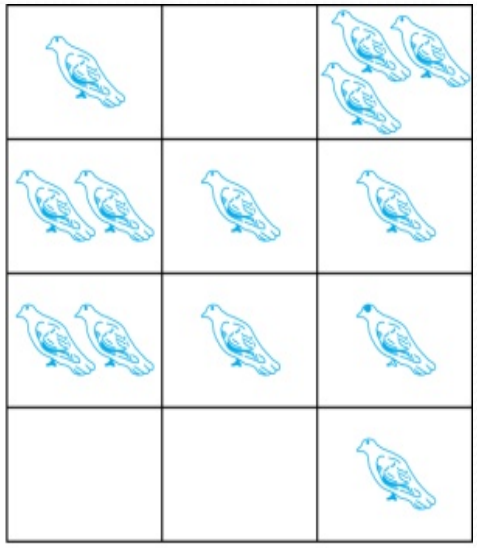
The Pigeonhole Principle

- If a flock of 20 pigeons roosts in a set of 19 pigeonholes, one of the pigeonholes must have more than 1 pigeon.



(a)

(b)



(c)

The Pigeonhole Principle

Corollary 1: A function f from a set with $k + 1$ elements to a set with k elements is not one-to-one.

Proof: Use the pigeonhole principle.

- Create a box for each element y in the codomain of f.
- Put in the box for y all of the elements x from the domain such that $f(x) = y$.
- Because there are $k + 1$ elements and only k boxes, at least one box has two or more elements.

Hence, f can't be one-to-one.

◀

The Generalized Pigeonhole Principle

The Generalized Pigeonhole Principle: If N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ objects.

Proof: We use a proof by contraposition. Suppose that none of the boxes contains more than $\lceil N/k \rceil - 1$ objects. Then the total number of objects is at most

$$k\left(\left\lceil \frac{N}{k} \right\rceil - 1\right) < k\left(\left(\frac{N}{k} + 1\right) - 1\right) = N,$$

where the inequality $\lceil N/k \rceil < \lceil N/k \rceil + 1$ has been used. This is a contradiction because there are a total of n objects. ◀

Pigeonhole Principle

Example: Among any group of 367 people, there must be at least two with the same birthday, because there are only 366 possible birthdays. $\lceil 367/366 \rceil = 2$

Example: Among 100 people there are at least $\lceil 100/12 \rceil = 9$ who were born in the same month.

Example: In any set of 27 English , must be at least two that begin with the same letter, since there are 26 letters in the English alphabet. $\lceil 27/26 \rceil = 2$

The Generalized Pigeonhole Principle

Example: What is the minimum number of students required in a Discrete Mathematics class to be sure that at least six will receive the same grade, if there are five possible grades, A, B, C, D, and F.

Solution:

The minimum number of students needed to guarantee that at least six students receive the same grade is the smallest integer N such that $\lceil N/K \rceil = \lceil N/5 \rceil = 6$. The smallest such integer is

$$N = K(\lceil N/K \rceil - 1) + 1 = 5(6-1)+1 = 5 \cdot 5 + 1 = 26.$$

Thus 26 is the minimum number of students needed to be sure that at least 6 students will receive the same grades.

Permutations and Combinations

Section 6.3

Section Summary

- Permutations
- Combinations
- Combinatorial Proofs

Permutations

Definition: A *permutation* of a set of distinct objects is an ordered arrangement of these objects. An ordered arrangement of r elements of a set is called an *r-permutation*.

Example: Let $S = \{1,2,3\}$.

- The ordered arrangement 3,1,2 is a permutation of S.
- The ordered arrangement 3,2 is a 2-permutation of S.

- The number of r-permutations of a set with n elements is denoted by $P(n,r)$.
- The 2-permutations of $S = \{1,2,3\}$ are 1,2; 1,3; 2,1; 2,3; 3,1; and 3,2. Hence, $P(3,2) = 6$.

A Formula for the Number of Permutations

Theorem 1: If n is a positive integer and r is an integer with $1 \leq r \leq n$, then there are

$$P(n, r) = n(n-1)(n-2)\cdots(n-r+1)$$

r-permutations of a set with n distinct elements.

Proof: Use the product rule. The first element can be chosen in n ways. The second in $n-1$ ways, and so on until there are $(n-(r-1))$ ways to choose the last element.

- Note that $P(n,0) = 1$, since there is only one way to order zero elements.

Corollary 1: If n and r are integers with $1 \leq r \leq n$, then

$$P(n,r) = \frac{n!}{(n-r)!}$$

Solving Counting Problems by Counting Permutations

Example: How many ways are there to select a first-prize winner, a second prize winner, and a third-prize winner from 100 different people who have entered a contest?

Solution:

$$P(100,3) = 100 \cdot 99 \cdot 98 = 970{,}200$$

Solving Counting Problems by Counting Permutations (*continued*)

- **Example**: Suppose that there are eight runners in a race. The winner receives a gold medal, the second place finisher receives a silver medal, and the third-place finisher receives a bronze medal. How many different ways are there to award these medals, if all possible outcomes of the race can occur and there are no ties?
- **Solution**: The number of different ways to award the medals is the number of 3-permutations of a set with eight elements. Hence, there are

$$P(8, 3) = 8 \cdot 7 \cdot 6 = 336$$

possible ways to award the medals.

Solving Counting Problems by Counting Permutations (*continued*)

Example: Suppose that a saleswoman has to visit eight different cities. She must begin her trip in a specified city, but she can visit the other seven cities in any order she wishes. How many possible orders can the saleswoman use when visiting these cities?

Solution: The first city is chosen, and the rest are ordered arbitrarily. Hence the orders are:

$P(7,7) = 7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040$

If she wants to find the tour with the shortest path that visits all the cities, she must consider 5040 paths!

Solving Counting Problems by Counting Permutations (*continued*)

Example: How many permutations of the letters *ABCDEFGH* contain the string *ABC* ?

Solution: We solve this problem by counting the permutations of six objects, *ABC*, *D*, *E*, *F*, *G*, and *H*.

$P(6,6) = 6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$

Combinations

Definition: An *r-combination* of elements of a set is an unordered selection of *r* elements from the set. Thus, an *r*-combination is simply a subset of the set with *r* elements.

- The number of *r*-combinations of a set with n distinct elements is denoted by $C(n, r)$.

- The notation $\binom{n}{r}$ is also used and is called a *binomial coefficient*. (*We will see the notation again in the binomial theorem in Section*. 6.4)

Combinations

Example:

- Let S be the set $\{a, b, c, d\}$. Then $\{a, c, d\}$ is a 3-combination from S. It is the same as $\{d, c, a\}$ since the order listed does not matter.
- $C(4,2) = 6$ because the 2-combinations of $\{a, b, c, d\}$ are the six subsets $\{a, b\}$, $\{a, c\}$, $\{a, d\}$, $\{b, c\}$, $\{b, d\}$, and $\{c, d\}$.

Combinations

Theorem 2: The number of r-combinations of a set with n elements, where $n \geq r \geq 0$, equals

$$C(n, r) = \frac{n!}{(n-r)!r!}.$$

Proof: By the product rule $P(n, r) = C(n,r) \cdot P(r,r)$. Therefore,

$$C(n, r) = \frac{P(n,r)}{P(r,r)} = \frac{n!/(n-r)!}{r!/(r-r)!} = \frac{n!}{(n-r)!r!}.$$

Combinations

Example: How many poker hands of five cards can be dealt from a standard deck of 52 cards? Also, how many ways are there to select 47 cards from a deck of 52 cards?

Solution: Since the order in which the cards are dealt does not matter, the number of five card hands is:

$$C(52,5) = \frac{52!}{5!47!}$$

$$= \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 26 \cdot 17 \cdot 10 \cdot 49 \cdot 12 = 2,598,960$$

- The different ways to select 47 cards from 52 is

$$C(52,47) = \frac{52!}{47!5!} = C(52,5) = 2,598,960.$$

This is a special case of a general result. →

Combinations

Corollary 2: Let n and r be nonnegative integers with $r \leq n$. Then $C(n, r) = C(n, n - r)$.

Proof: From Theorem 2, it follows that

$$C(n, r) = \frac{n!}{(n-r)!r!}$$

and

$$C(n, n - r) = \frac{n!}{(n-r)![n-(n-r)]!} = \frac{n!}{(n-r)!r!} .$$

Hence, $C(n, r) = C(n, n - r)$. ◀

This result can be proved without using algebraic manipulation. →

Combinatorial Proofs

- **Definition 1**: A *combinatorial proof* of an identity is a proof that uses one of the following methods.
  - A *double counting proof* uses counting arguments to prove that both sides of an identity count the same objects, but in different ways.
  - A *bijective proof* shows that there is a bijection between the sets of objects counted by the two sides of the identity.

Combinatorial Proofs

- Here are two combinatorial proofs that

$$C(n, r) = C(n, n - r)$$

when r and n are nonnegative integers with $r < n$:

- *Bijective Proof*: Suppose that S is a set with n elements. The function that maps a subset A of S to $\bar{A}$ is a bijection between the subsets of S with r elements and the subsets with $n - r$ elements. Since there is a bijection between the two sets, they must have the same number of elements.
- *Double Counting Proof*: By definition the number of subsets of S with r elements is $C(n, r)$. Each subset A of S can also be described by specifying which elements are not in A, i.e., those which are in $\bar{A}$. Since the complement of a subset of S with r elements has $n - r$ elements, there are also $C(n, n - r)$ subsets of S with r elements.

Combinations

Example: How many ways are there to select five players from a 10-member tennis team to make a trip to a match at another school.

Solution: By Theorem 2, the number of combinations is

$$C(10,5) = \frac{10!}{5!5!} = 252.$$

Example: A group of 30 people have been trained as astronauts to go on the first mission to Mars. How many ways are there to select a crew of six people to go on this mission?

Solution: By Theorem 2, the number of possible crews is

$$C(30,6) = \frac{30!}{6!24!} = \frac{30\cdot 29\cdot 28\cdot 27\cdot 26\cdot 25}{6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1} = 593,775\ .$$

Binomial Coefficients and Identities

Section 6.4

Section Summary

- The Binomial Theorem
- Pascal's Identity and Triangle

Binomial Theorem

Binomial Theorem: Let x and y be variables, and n a nonnegative integer. Then:

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j}y^j = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n.$$

Proof: We use combinatorial reasoning . The terms in the expansion of $(x + y)^n$ are of the form $x^{n-j}y^j$ for $j = 0,1,2,\ldots,n$. To form the term $x^{n-j}y^j$, it is necessary to choose $n-j$ xs from the n sums. Therefore, the coefficient of $x^{n-j}y^j$ is $\binom{n}{n-j}$ which equals $\binom{n}{j}$.

◀

Powers of Binomial Expressions

Definition: A *binomial* expression is the sum of two terms, such as $x + y$. (More generally, these terms can be products of constants and variables.)

- We can use counting principles to find the coefficients in the expansion of $(x + y)^n$ where n is a positive integer.
- To illustrate this idea, we first look at the process of expanding $(x + y)^3$.
- $(x + y)\ (x + y)\ (x + y)$ expands into a sum of terms that are the product of a term from each of the three sums.
- Terms of the form x^3, x^2y, $x\,y^2$, y^3 arise. The question is what are the coefficients?
  - To obtain x^3 , an x must be chosen from each of the sums. There is only one way to do this. So, the coefficient of x^3 is 1.
  - To obtain x^2y, an x must be chosen from two of the sums and a y from the other. There are $\binom{3}{2}$ ways to do this and so the coefficient of x^2y is 3.
  - To obtain xy^2, an x must be chosen from of the sums and a y from the other two . There are $\binom{3}{1}$ ways to do this and so the coefficient of xy^2 is 3.
  - To obtain y^3, a y must be chosen from each of the sums. There is only one way to do this. So, the coefficient of y^3 is 1.
- We have used a counting argument to show that $(x + y)^3 = x^3 + 3x^2y + 3x\,y^2 + y^3$.
- Next we present the binomial theorem gives the coefficients of the terms in the expansion of $(x + y)^n$.

Using the Binomial Theorem

Example:

What is the expansion of $(x + y)^4$?

Solution: From the binomial theorem it follows that

$$(x+y)^4 = \sum_{j=0}^{4} \binom{4}{j} x^{4-j} y^j$$

$$= \binom{4}{0} x^4 + \binom{4}{1} x^3 y + \binom{4}{2} x^2 y^2 + \binom{4}{3} x y^3 + \binom{4}{4} y^4$$

$$= x^4 + 4x^3 y + 6x^2 y^2 + 4xy^3 + y^4.$$

Using the Binomial Theorem

What is the coefficient of $x^{12}y^{13}$ in the expansion of $(x+y)^{25}$?

Solution: From the binomial theorem it follows that this coefficient is

$$\binom{25}{13} = \frac{25!}{13!\,12!} = 5,200,300.$$

Using the Binomial Theorem

Example: What is the coefficient of $x^{12}y^{13}$ in the expansion of $(2x - 3y)^{25}$?

Solution: We view the expression as $(2x + (-3y))^{25}$.
By the binomial theorem

$$(2x + (-3y))^{25} = \sum_{j=0}^{25} \binom{25}{j} (2x)^{25-j}(-3y)^{j}.$$

Consequently, the coefficient of $x^{12}y^{13}$ in the expansion is obtained when $j = 13$.

$$\binom{25}{13} 2^{12}(-3)^{13} = -\frac{25!}{13!12!} 2^{12}3^{13}.$$

A Useful Identity

Corollary 1: With $n \geq 0$,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Proof (*using binomial theorem*): With $x = 1$ and $y = 1$, from the binomial theorem we see that:

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

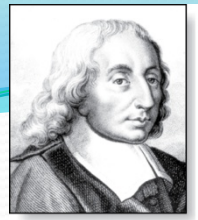
Proof (*combinatorial*): Consider the subsets of a set with n elements. There are $\binom{n}{0}$ subsets with zero elements, $\binom{n}{1}$ with one element, with two elements, $\binom{n}{2}$, …, and with n elements. Therefore the total is $\binom{n}{n}$.

$$\sum_{k=0}^{n} \binom{n}{k}.$$

Since, we know that a set with n elements has 2^n subsets, we conclude:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n. \quad \blacktriangleleft$$

Blaise Pascal
(1623-1662)



Pascal's Identity

Pascal's Identity: If n and k are integers with $n \geq k \geq 0$, then

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

Proof (*combinatorial*): Let T be a set where $|T| = n + 1$, $a \in T$, and $S = T - \{a\}$. There are $\binom{n+1}{k}$ subsets of T containing k elements. Each of these subsets either:

- contains a with $k - 1$ other elements, or
- contains k elements of S and not a.

There are

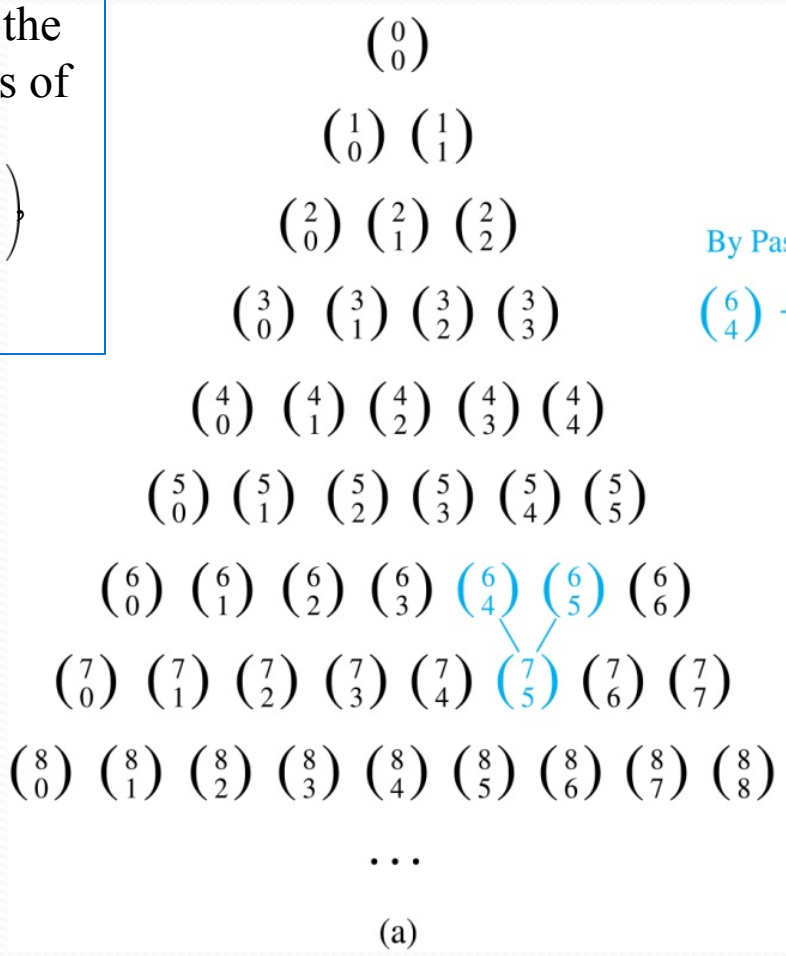
- $\binom{n}{k-1}$ subsets of k elements that contain a, since there are $\binom{n}{k-1}$ subsets of $k - 1$ elements of S,
- $\binom{n}{k}$ subsets of k elements of T that do not contain a, because there are $\binom{n}{k}$ subsets of k elements of S.

Hence, $$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$ ◀

See Exercise 19 *for an algebraic proof.*

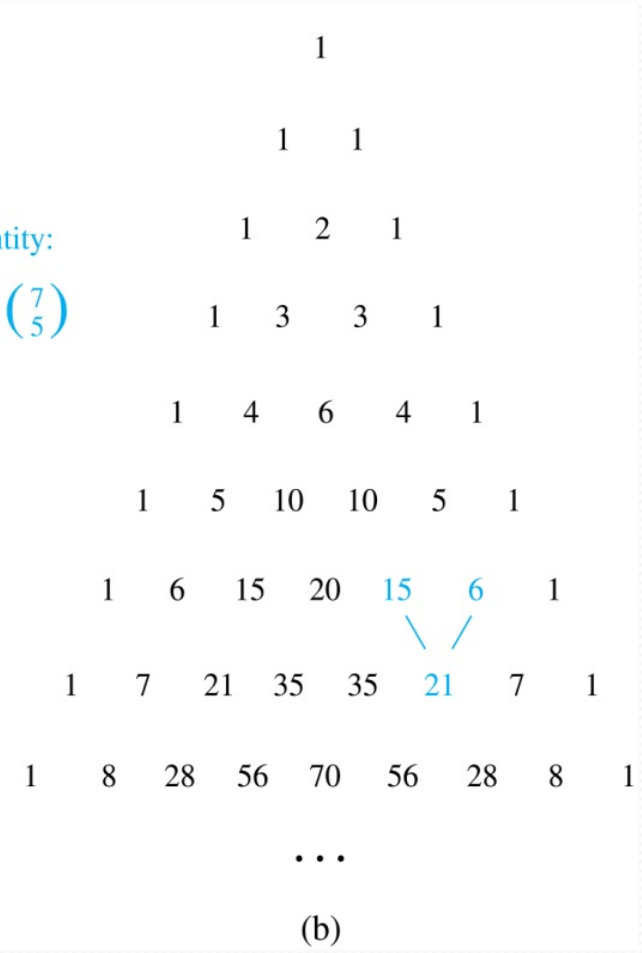
Pascal's Triangle

The nth row in the triangle consists of the binomial coefficients $\binom{n}{k}$, $k = 0,1,\ldots,n$.



By Pascal's identity:

$\binom{6}{4} + \binom{6}{5} = \binom{7}{5}$



By Pascal's identity, adding two adjacent bionomial coefficients results is the binomial coefficient in the next row between these two coefficients.