

- A proof is a valid argument that establishes the truth of a mathematical statement
- Axiom (or postulate): a statement that is assumed to be true
- Theorem
 - A statement that has been proven to be true
- Hypothesis, premise
 - An assumption (often unproven) defining the structures about which we are reasoning



More Proof Terminology

Lemma

A minor theorem used as a stepping-stone to proving a major theorem.

Corollary

A minor theorem proved as an easy consequence of a major theorem.

Conjecture

 A statement whose truth value has not been proven. (A conjecture may be widely believed to be true, regardless.)



Proof Methods

- For proving a statement p alone
 - Proof by Contradiction (indirect proof):

Assume $\neg p$, and prove $\neg p \rightarrow \mathbf{F}$.

Proof Methods

- For proving implications $p \rightarrow q$, we have:
 - **Trivial** proof: Prove q by itself.
 - Direct proof: Assume p is true, and prove q.
 - Indirect proof:
 - **Proof by Contraposition** $(\neg q \rightarrow \neg p)$: Assume $\neg q$, and prove $\neg p$.
 - **Proof by Contradiction**: Assume $p \land \neg q$, and show this leads to a contradiction. (i.e. prove $(p \land \neg q) \rightarrow \mathbf{F}$)
 - **Vacuous** proof: Prove $\neg p$ by itself.

Direct Proof Example

- Definition: An integer n is called odd iff n=2k+1 for some integer k; n is even iff n=2k for some k.
- **Theorem:** Every integer is either odd or even, but not both.
 - This can be proven from even simpler axioms.

Theorem:

(For all integers n) If n is odd, then n^2 is odd.

Proof:

If n is odd, then n = 2k + 1 for some integer k.

Thus, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Therefore n^2 is of the form 2j + 1 (with j the integer $2k^2 + 2k$), thus n^2 is odd. \blacksquare

Indirect Proof Example: Proof by Contraposition

Theorem: (For all integers n) If 3n + 2 is odd, then n is odd.

Proof:

(Contrapositive: If n is even, then 3n + 2 is even) Suppose that the conclusion is false, *i.e.*, that n is even. Then n = 2k for some integer k.

Then 3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1).

Thus 3n + 2 is even, because it equals 2j for an integer j = 3k + 1. So 3n + 2 is not odd.

We have shown that $\neg(n \text{ is odd}) \rightarrow \neg(3n + 2 \text{ is odd})$, thus its contrapositive $(3n + 2 \text{ is odd}) \rightarrow (n \text{ is odd})$ is also true. \blacksquare

Vacuous Proof Example

- Show $\neg p$ (i.e. p is false) to prove $p \rightarrow q$ is true.
- **Theorem:** (For all n) If n is both odd and even, then $n^2 = n + n$.

Proof:

The statement "*n* is both odd and even" is necessarily false, since no number can be both odd and even. So, the theorem is vacuously true. ■

Trivial Proof Example

■ Show q (i.e. q is true) to prove $p \rightarrow q$ is true.

■ **Theorem:** (For integers *n*) If *n* is the sum of two prime numbers, then either *n* is odd or *n* is even.

Proof:

Any integer *n* is either odd or even. So the conclusion of the implication is true regardless of the truth of the hypothesis. Thus the implication is true trivially. ■

1

Proof by Contradiction

- A method for proving p.
 - Assume $\neg p$, and prove both q and $\neg q$ for some proposition q. (Can be anything!)
 - Thus $\neg p \rightarrow (q \land \neg q)$
 - $-(q \land \neg q)$ is a trivial contradiction, equal to **F**
 - Thus $\neg p \rightarrow \mathbf{F}$, which is only true if $\neg p = \mathbf{F}$
 - Thus p is true



Rational Number

Definition:

The real number r is rational if there exist integers p and q with $q \ne 0$ such that r = p/q. A real number that is not rational is called *irrational*.

Proof by Contradiction Example

- **Theorem:** $\sqrt{2}$ is irrational.
 - Proof:
 - Assume that $\sqrt{2}$ is rational. This means there are integers x and y ($y \ne 0$) with no common divisors such that $\sqrt{2} = x/y$.

Squaring both sides, $2 = x^2/y^2$, so $2y^2 = x^2$. So x^2 is even; thus x is even (see earlier).

Let x = 2k. So $2y^2 = (2k)^2 = 4k^2$. Dividing both sides by 2, $y^2 = 2k^2$. Thus y^2 is even, so y is even.

But then x and y have a common divisor, namely 2, so we have a contradiction.

Therefore, $\sqrt{2}$ is irrational.



- Proving implication $p \rightarrow q$ by contradiction
 - Assume $\neg q$, and use the premise p to arrive at a contradiction, i.e. $(\neg q \land p) \rightarrow \mathbf{F}$ $(p \rightarrow q \equiv (\neg q \land p) \rightarrow \mathbf{F})$
 - How does this relate to the proof by contraposition?
 - Proof by Contraposition $(\neg q \rightarrow \neg p)$: Assume $\neg q$, and prove $\neg p$.

Proof by Contradiction Example: Implication

Theorem: (For all integers n) If 3n + 2 is odd, then n is odd.

Proof:

Assume that the conclusion is false, *i.e.*, that n is even, and that 3n + 2 is odd.

Then n = 2k for some integer k and 3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1). Thus 3n + 2 is even, because it equals 2j for an integer j = 3k + 1.

This contradicts the assumption "3n + 2 is odd".

This completes the proof by contradiction, proving that if 3n + 2 is odd, then n is odd.

Circular Reasoning

- The fallacy of (explicitly or implicitly) assuming the very statement you are trying to prove in the course of its proof. Example:
- Prove that an integer n is even, if n^2 is even.
- Attempted proof:

Assume n^2 is even. Then $n^2 = 2k$ for some integer k. Dividing both sides by n gives n = (2k)/n = 2(k/n).

So there is an integer j (namely k/n) such that n = 2j. Therefore n is even.

Circular reasoning is used in this proof.

Where?

Begs the question: How do you show that j = k/n = n/2 is an integer, without **first** assuming that n is even?

The Identity Function

- For any domain A, the *identity function* I: $A \rightarrow A$ (also written as I_A , $\mathbf{1}$, $\mathbf{1}_A$) is the unique function such that $\forall a \in A$: I(a) = a.
- Note that the identity function is always both one-to-one and onto (i.e., bijective).
- For a bijection $f: A \rightarrow B$ and its inverse function $f^{-1}: B \rightarrow A$,

$$f^{-1} \circ f = I_A$$

Some identity functions you've seen:

$$-+0$$
, \times 1, \wedge T, \vee F, \cup \emptyset , \cap U .



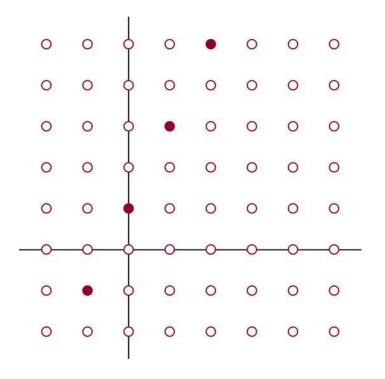
Graphs of Functions

- We can represent a function $f: A \to B$ as a set of ordered pairs $\{(a, f(a)) \mid a \in A\}$. ← The function's graph.
- Note that $\forall a \in A$, there is only 1 pair (a, b).
- For functions over numbers, we can represent an ordered pair (x, y) as a point on a plane.
- A function is then drawn as a curve (set of points), with only one *y* for each *x*.



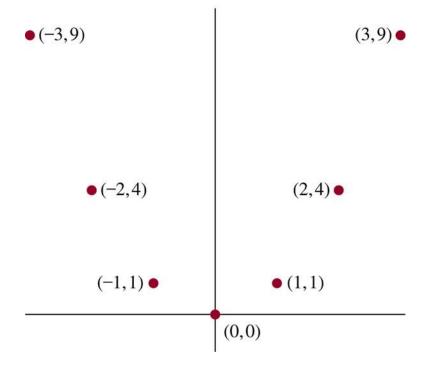
Graphs of Functions: Examples

© The McGraw-Hill Companies, Inc. all rights reserved.



The graph of f(n) = 2n + 1 from **Z** to **Z**

© The McGraw-Hill Companies, Inc. all rights reserved.



The graph of $f(x) = x^2$ from **Z** to **Z**

Floor&Ceiling Functions

In discrete math, we frequently use the following two functions over real numbers:

The floor function $[\cdot]: R \to Z$, where [x] ("floor of x") means the largest integer ≤ x, i.e., $[x] = max(\{i \in Z \mid i \le x\})$.

E.g.
$$\lfloor 2.3 \rfloor = 2$$
, $\lfloor 5 \rfloor = 5$, $\lfloor -1.2 \rfloor = -2$

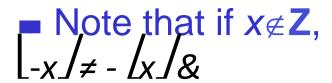
The ceiling function $[\cdot]: R \to Z$, where $[\cdot]x$ ("ceiling of x") means the smallest integer $\geq x$, i.e., $[\cdot]x = min(\{i \in Z \mid i \geq x\})$

E.g.
$$[2.3] = 3$$
, $[5] = 5$, $[-1.2] = -$



Visualizing Floor & Ceiling

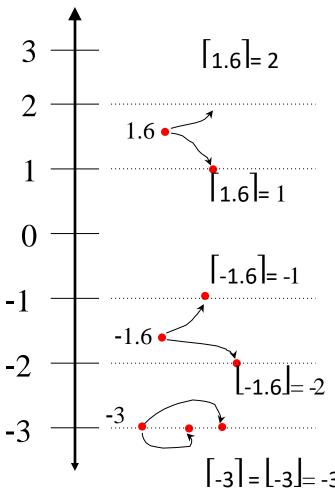
Real numbers "fall to their floor" or "rise to their ceiling."



$$\left[-x \right] \neq - \left[x \right]$$

■■ Note that if $x \in \mathbb{Z}$,

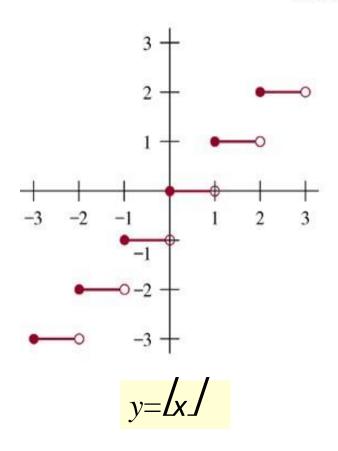
$$\lfloor x \rfloor = \lceil x \rceil = x$$
.

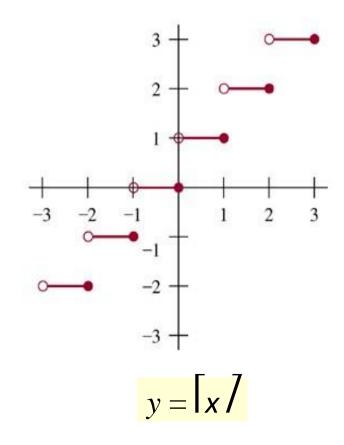




Plots with Floor/Ceiling: Example

© The McGraw-Hill Companies, Inc. all rights reserved.







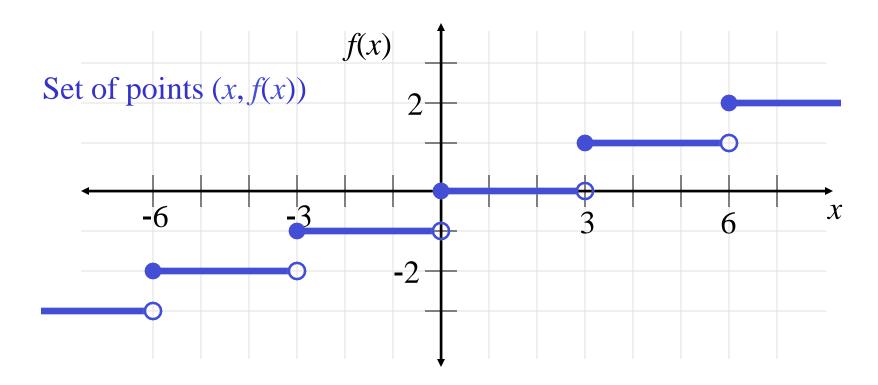
Plots with Floor/Ceiling

- Note that for $f(x) = \leq \lfloor xf \rfloor$, the graph of f includes the point (a, 0) for all values of a such that $0 \le a < 1$, but not for the value a = 1.
- •• We say that the set of points (a, 0) that is in f does not include its *limit* or *boundary* point (a,1).
- Sets that do not include all of their limit points are called open sets.
- In a plot, we draw a limit point of a curve using an open dot (circle) if the limit point is not on the curve, and with a closed (solid) dot if it is on the curve.



Plots with Floor/Ceiling: Another Example

Plot of graph of function $f(x) = \le \lfloor x/3f \rfloor$:





2.4 Sequences and Summations

- Sequences are ordered lists of elements, represents solutions to certain counting problems.
- A sequence is a discrete structure used to represent an ordered list.
- A sequence is a function from a subset of the set of integers.
- ■Notation an to denote the image of the integer n. an a term of the sequence.
- A summation is a compact notation for the sum of the terms in a (possibly infinite) sequence.

Sequences

- A sequence or series {a_n} is identified with a generating function f: I → S for some subset I⊆N and for some set S.
- •• Often we have I = N or $I = Z^+ = N \{0\}$.
- If f is a generating function for a sequence $\{a_n\}$, then for $n \in I$, the symbol a_n denotes f(n), also called **term** n of the sequence.
- The *index* of a_n is n. (Or, often i is used.)
- A sequence is sometimes denoted by listing its first and/or last few elements, and using ellipsis (...) notation.
- *E.g.*, " $\{a_n\}$ = 0, 1, 4, 9, 16, 25, ..." is taken to mean $\forall n \in \mathbb{N}, a_n = n^2$.

Sequence Examples

- Some authors write "the sequence $a_1, a_2,...$ " instead of $\{a_n\}$, to ensure that the set of indices is clear.
- Be careful: Our book often leaves the indices ambiguous.
- An example of an infinite sequence:
- Consider the sequence $\{a_n\} = a_1, a_2, ..., where (\forall n \ge 1) a_n = f(n) = 1/n$.
- •• Then, we have $\{a_n\} = 1, 1/2, 1/3,...$
- Called "harmonic series"

Example with Repetitions

- Like tuples, but unlike sets, a sequence may contain *repeated* instances of an element.
- Consider the sequence $\{b_n\} = b_0, b_1, \dots$ (note that 0 is an index) where $b_n = (-1)^n$.
- Thus, $\{b_n\} = 1, -1, 1, -1, \dots$
- Note repetitions!
- This {*b_n*} denotes an infinite sequence of 1's and -1's, *not* the 2-element set {1, -1}.

Geometric Progression

- A geometric progression is a sequence of the form
- $a, ar, ar^2, ..., ar^n, ...$

where the *initial term a* and the *common ratio r* are real numbers.

- A geometric progression is a discrete analogue of the exponential function $f(x) = ar^x$
- Examples
 - $-\{b_n\}$ with $b_n = (-1)^n$
 - $-\{c_n\}$ with $c_n = 2 \cdot 5^n$
 - $\{d_n\}$ with $d_n = 6 \cdot (1/3)^n$

Assuming n = 0, 1, 2,...

initial term 1, common ratio −1

initial term 2, common ratio 5

initial term 6, common ratio 1/3

Arithmetic Progression

- An arithmetic progression is a sequence of the form
- a, a+d, a+2d, ..., a+nd,...
- where the *initial term a* and the *common* difference d are real numbers.
- An arithmetic progression is a discrete analogue of the linear function f(x) = a + dx
- Examples

Assuming n = 0, 1, 2,...

- $-\{s_n\}$ with $s_n = -1 + 4n$ initial term -1, common diff. 4
- $-\{t_n\}$ with $t_n = 7 3n$ initial term 7, common diff. -3

Recognizing Sequences (I)

- Sometimes, you're given the first few terms of a sequence,
- and you are asked to find the sequence's generating function,
- or a procedure to enumerate the sequence.
- Examples: What's the next number?
 - **1**, **2**, **3**, **4**, ... 5 (the 5th smallest number > 0)
 - **1**, 3, 5, 7, 9,... 11 (the 6th smallest odd number >
 - **2**, **3**, **5**, **7**, **11**,... 0) 13 (the 6th smallest prime number)

Recognizing Sequences (II)

- General problems
- Given a sequence, find a formula or a general rule that produced it
- Examples: How can we produce the terms of a sequence if the first 10 terms are
- **1**, 2, 2, 3, 3, 3, 4, 4, 4, 4?

Possible match: next five terms would all be 5, the following six terms would all be 6, and so on.

5, 11, 17, 23, 29, 35, 41, 47, 53, 59?

Possible match: *n*th term is 5 + 6(n - 1) = 6n - 1 (assuming n = 1, 2, 3,...)

Special Integer Sequences

A useful technique for finding a rule for generating the terms of a sequence is to compare the terms of a sequence of interest with the terms of a well-known integer sequences (e.g. arithmetic/geometric progressions, perfect squares, perfect cubes, etc.)

© The McGraw-Hill Companies, Inc. all rights reserved.

nth Term	First 10 Terms
620.	1 4 0 16 25 26 40 64 01 100
n^2	1, 4, 9, 16, 25, 36, 49, 64, 81, 100,
n^3	1, 8, 27, 64, 125, 216, 343, 512, 729, 1000,
n^4	1, 16, 81, 256, 625, 1296, 2401, 4096, 6561, 10000,
2^n	2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,
3 ⁿ	3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049,
n!	1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800,

Coding: Fibbonaci Series

- Series $\{a_n\} = \{1, 1, 2, 3, 5, 8, 13, 21, ...\}$
- Generating function (recursive definition!):
 - $a_0 = a_1 = 1$ and
 - $a_n = a_{n-1} + a_{n-2}$ for all n > 1
- Now let's find the entire series {a_n}:

```
int [] a = new int [n];
a[0] = 1;
a[1] = 1;
for (int i = 2; i < n; i++) {
   a[i] = a[i-1] + a[i-2];
}
return a;</pre>
```

Coding: Factorial Series

- Factorial series $\{a_n\} = \{1, 2, 6, 24, 120, ...\}$
- Generating function:
- $a_n = n! = 1 \times 2 \times 3 \times ... \times n$

This time, let's just find the term a_n:

```
int an = 1;
for (int i = 1; i <= n; i++) {
an = an * i;
}
return an;</pre>
```



Summation Notation

■ Given a sequence $\{a_n\}$, an integer *lower bound* (or *limit*) $j \ge 0$, and an integer *upper bound* $k \ge j$, then the *summation of* $\{a_n\}$ *from* a_j *to* a_k is written and defined as follows:

$$\sum_{i=j}^{k} a_i = a_j + a_{j+1} + \dots + a_k$$

Here, i is called the index of summation.

$$\sum_{i=j}^{k} a_i = \sum_{m=j}^{k} a_m = \sum_{l=j}^{k} a_l$$



Generalized Summations

For an infinite sequence, we write:

$$\sum_{i=j}^{\infty} a_i = a_j + a_{j+1} + \cdots$$

To sum a function over all members of a set $X = \{x_1, x_2,...\}$:

$$\sum_{x \in X} f(x) = f(x_1) + f(x_2) + \cdots$$

 \blacksquare Or, if $X = \{x \mid P(x)\}$, we may just write:

$$\sum_{P(x)} f(x) = f(x_1) + f(x_2) + \cdots$$



Simple Summation Example

$$-\sum_{i=2}^{4} (i^2 + 1) =$$

$$-1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{100} = \sum_{i=1}^{100} \frac{1}{i}$$



More Summation Examples

An infinite sequence with a finite sum:

$$\sum_{i=0}^{\infty} 2^{-i} = 2^0 + 2^{-1} + \dots = 1 + \frac{1}{2} + \frac{1}{4} + \dots = 2$$

Using a predicate to define a set of elements to sum over:

$$\sum_{\substack{(x \text{ is prime}) \land \\ x < 10}} x^2 = 2^2 + 3^2 + 5^2 + 7^2$$

$$= 4 + 9 + 25 + 49 = 87$$



- Some handy identities for summations:
 - Summing constant value

$$\sum_{n=i}^{j} c = (j-i+1) \cdot c$$

Number of terms in the summation

$$\sum_{n=1}^{3} 2 = 0$$

$$\sum_{n=-1}^{2} 2i$$

$$=4\oplus(2i)=8i$$



Distributive law

$$\sum_{n=i}^{j} cf(n) = c \sum_{n=i}^{j} f(n)$$

$$\sum_{n=1}^{3} (4 \cdot n^{2}) = 4 \cdot 1^{2} + 4 \cdot 2^{2} + 4 \cdot 3^{2}$$

$$= 4 \cdot (1^{2} + 2^{2} + 3^{2})$$

$$= 4 \sum_{n=1}^{3} n^{2}$$

An application of commutativity

$$\sum (f(n) + g(n)) = \sum_{n=i}^{j} f(n) + \sum_{n=i}^{j} g(n)$$

$$\sum_{n=2}^{4} (n+2n) = (2+2\cdot2) + (3+2\cdot3) + (4+2\cdot4)$$

$$= (2+3+4) + (2\cdot2+2\cdot3+2$$

$$\cdot 4)$$

$$= \sum_{n=2}^{4} n + \sum_{n=2}^{4} n$$

Index Shifting

$$\sum_{i=j}^{m} f(i) = \sum_{k=j+n}^{m+n} f(k-n)$$

$$\sum_{i=1}^{4} i^2 = 1^2 + 2^2 + 3^2 + 4^2$$

Let k = i + 2, then i = k - 2

$$\sum_{k=1+2}^{4+2} (k-2)^{2} = \sum_{k=3}^{6} (k-2)^{2}$$

$$= (3-2)^{2} + (4-2)^{2} + (5-2)^{2} + (6-2)^{2}$$

Sequence splitting

$$\sum_{i=j}^{k} f(i) = \sum_{i=j}^{m} f(i) + \sum_{i=m+1}^{k} f(i) \quad \text{if } j \le m < k$$

$$\sum_{i=0}^{4} i^3 = 0^3 + 1^3 + 2^3 + 3^3 + 4^3$$

$$= (0^3 + 1^3 + 2^3) + (3^3 + 4^3)$$

$$= \sum_{i=0}^{2} i^3 + \sum_{i=3}^{4} i^3$$



Order reversal

$$\sum_{i=0}^{k} f(i) = \sum_{i=0}^{k} f(k-i)$$

$$\sum_{i=0}^{3} i^3 = 0^3 + 1^3 + 2^3 + 3^3$$

$$= (3-0)^3 + (3-1)^3 + (3-2)^3 + (3-3)^3$$

$$= \sum_{i=0}^{3} (3-i)^3$$

Example: Geometric Progression

- A geometric progression is a sequence of the form a, ar, ar^2 , ar^3 , ..., ar^n ,... where a, $r \in \mathbb{R}$.
- The sum of such a sequence is given by:

$$S = \sum_{i=0}^{n} ar^{i}$$

We can reduce this to *closed form* via clever manipulation of summations...

THEOREM 1

If a and r are real numbers and $r \neq 0$, then

$$\sum_{j=0}^{n} ar^{j} = \begin{cases} \frac{ar^{n+1} - a}{r - 1} & \text{if } r \neq 1\\ (n+1)a & \text{if } r = 1. \end{cases}$$

Proof: Let

$$S_n = \sum_{j=1}^n ar^j.$$



To compute S, first multiply both sides of the equality by r and then manipulate the resulting sum as follows:

$$rS_n = r\sum_{j=0}^n ar^j$$
 substituting summation formula for S

$$= \sum_{j=0}^n ar^{j+1} \qquad \text{by the distributive property}$$

$$= \sum_{k=1}^{n+1} ar^k \qquad \text{shifting the index of summation, with } k = j+1$$

$$= \left(\sum_{k=0}^n ar^k\right) + (ar^{n+1} - a) \qquad \text{removing } k = n+1 \text{ term and adding } k = 0 \text{ term}$$

$$= S_n + (ar^{n+1} - a) \qquad \text{substituting } S \text{ for summation formula}$$

From these equalities, we see that

$$rS_n = S_n + (ar^{n+1} - a).$$

Solving for S_n shows that if $r \neq 1$, then

$$S_n = \frac{ar^{n+1} - a}{r - 1}.$$

If r = 1, then the $S_n = \sum_{j=0}^n ar^j = \sum_{j=0}^n a = (n+1)a$.



Gauss' Trick, Illustrated

Consider the sum:

$$(1)+(2)+(n/2)+((n/2)+1)+...+(n-1)+(n-1)+(n-1)$$
 $(n+1)$
 $(n+1)$

We have n/2 pairs of elements, each pair summing to n+1, for a total of (n/2)(n+1).



TABLE 2 Some Useful Summation Formulae.

Sum	Closed Form
$\sum_{k=0}^{n} ar^k \ (r \neq 0)$	$\frac{ar^{n+1}-a}{r-1}, r \neq 1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, x < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty}, kx^{k-1}, x < 1$	$\frac{1}{(1-x)^2}$

Geometric sequence

Gauss' trick

Quadratic series

Cubic series

Copyright © The McGraw-Hill Companies, in Permission required for reproduction or display

Using the Shortcuts

Example: Evaluate

$$\sum_{k=50}^{100} k^2$$

- Use series splitting.
- Solve for desired summation.
- rule.
- **Apply** quadratic series =338,350-40,425=297,925.

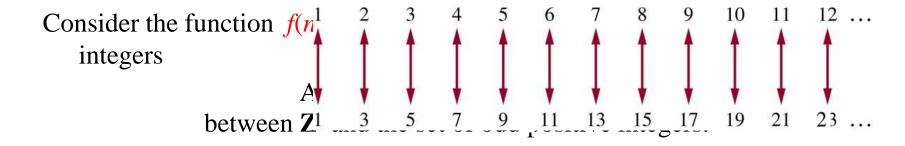
Evaluate.

k = 50

Cardinality

- The sets A and B have the same cardinality if and only if there is a one-to-one correspondence from A to B.
- A set that is either finite or has the same cardinality as the set of positive integers is called countable.
- A set that is not countable is called uncountable.
- Example: Show that the set of odd positive integers is a countable set.

© The McGraw-Hill Companies, Inc. all rights reserved.



Useful identities:

$$\sum_{i=j}^{k} f(i) = \sum_{i=j}^{m} f(i) + \sum_{i=m+1}^{k} f(i) \quad \text{if } j \le m < k$$
(Sequence splitting.)
$$\sum_{i=0}^{k} f(i) = \sum_{i=0}^{k} f(k-i) \quad \text{(Order reversal.)}$$

$$\sum_{i=0}^{2k} f(i) = \sum_{i=0}^{k} \left(f(2i-1) + f(2i) \right) \quad \text{(Grouping.)}$$