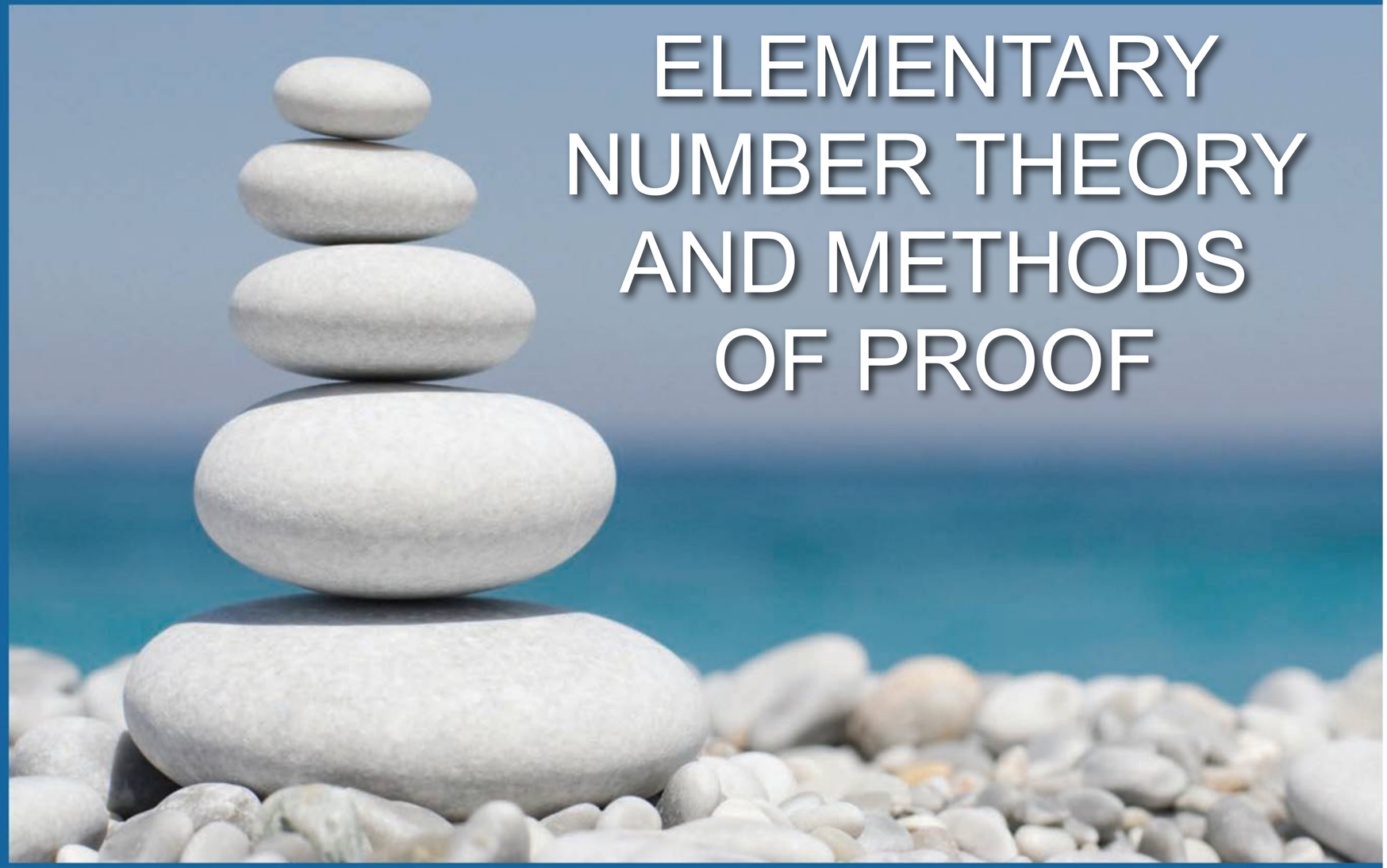
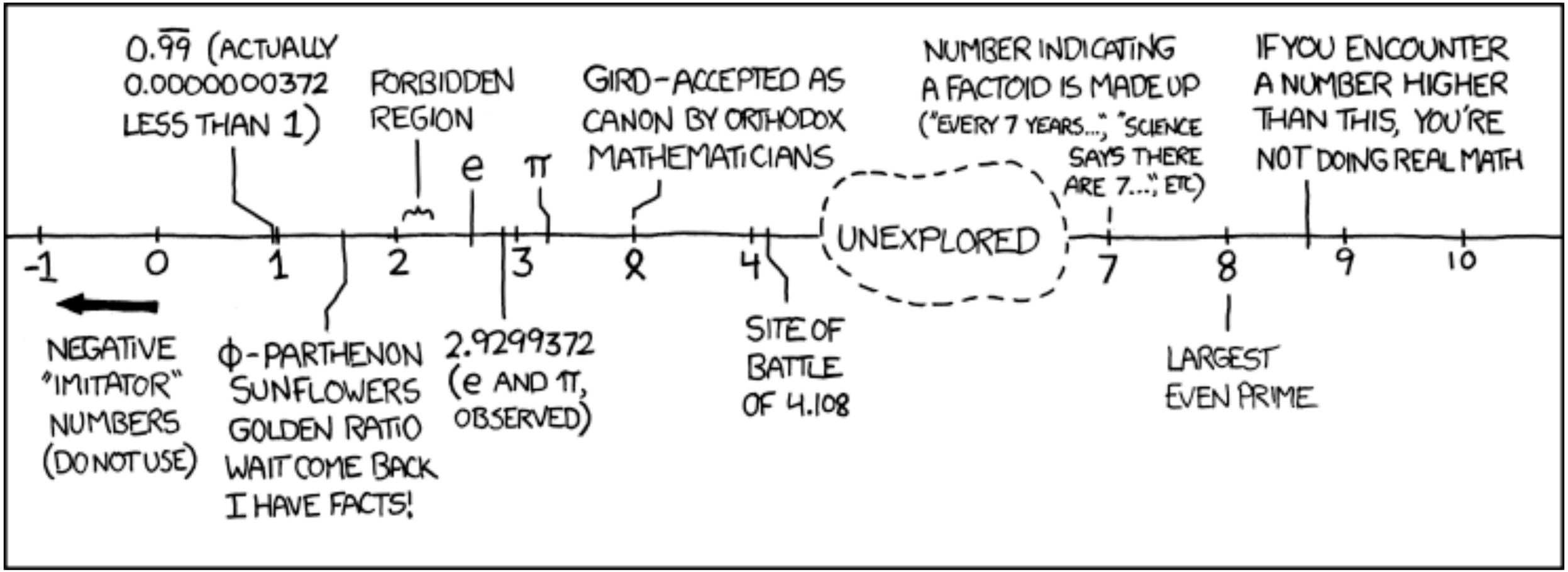
CHAPTER 4



ELEMENTARY NUMBER THEORY AND METHODS OF PROOF



SECTION 4.1

Direct Proof and Counterexample I:Introduction

Definitions

In order to evaluate the truth or falsity of a statement, you must understand the meanings of all terms that occur in the statement. Definitions make meaning clear.

• Definitions

An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

$$n \text{ is even} \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = 2k.$$

$$n \text{ is odd} \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = 2k + 1.$$

Exercise – *Even and Odd Integers*

Use the definitions of *even* and *odd* to justify your answers to the following questions.

a. Is 0 even?

b. Is −301 odd?

c. If a and b are integers, is $10a + 8b + 1$ odd?

Solution:

a.

b.

d.

Example – *Prime and Composite Numbers*

• Definition

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

$$n \text{ is prime} \Leftrightarrow \forall \text{ positive integers } r \text{ and } s, \text{ if } n = rs \text{ then either } r = 1 \text{ and } s = n \text{ or } r = n \text{ and } s = 1.$$

$$n \text{ is composite} \Leftrightarrow \exists \text{ positive integers } r \text{ and } s \text{ such that } n = rs \text{ and } 1 < r < n \text{ and } 1 < s < n.$$

a. Is 1 prime?

b. Is every integer greater than 1 either prime or composite?

Solution:

a.

Solution – *Prime and Composite Numbers*

b. Let n be any integer that is greater than 1.

Proving Existential Statements

One way to prove a statement in the form

$$\exists x \in D \text{ such that } Q(x)$$

is to find an x in D that makes $Q(x)$ true.

Another way is to give a set of directions for finding such an x.

Both of these methods are called **constructive proofs of existence**.

Example – *Constructive Proofs of Existence*

a. Prove "∃ an even integer n that can be written in two ways as a sum of two prime numbers."

b. Suppose that r and s are integers. Prove the following: "∃ an integer k such that $22r + 18s = 2k$."

Solution:

a.

b.

Proving Existential Statements

Nonconstructive proof of existence involves showing

(a) that the existence of a value of x that makes $Q(x)$ true is guaranteed by an axiom or a previously proved theorem or

(b) that the assumption that there is no such x leads to a contradiction.

The disadvantage of a nonconstructive proof is that it may give virtually no clue about where or how x may be found.

Disproving Universal Statements by Counterexample

To disprove statement

"$\forall x$ in D, if $P(x)$ then $Q(x)$",

we can prove its negation

"$\exists x$ in D such that $P(x)$ and not $Q(x)$"

by finding a *counterexample* x that makes the negation true.

Disproof by Counterexample

To disprove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$," find a value of x in D for which the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false. Such an x is called a **counterexample.**

Exercise – *Disproof by Counterexample*

Disprove the following statement by finding a counterexample:

$\forall$ real numbers a and b, if $a^2 = b^2$ then $a = b$.

Solution:

Proving Universal Statements

Universal statements of the form

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x).$$

can be proved by the method of exhaustion if

a) the domain D is finite or

b) only a finite number of elements satisfy $P(x)$.

Example: $\forall n \in \mathbf{Z}$, if n is even and $4 \leq n \leq 26$, then n can be written as a sum of two prime numbers.

Solution:

Proving Universal Statements

Powerful method to prove universal statements with arbitrary domain size of D:

Prove statement for a particular but generically chosen element $x \in D$.

Method of Generalizing from the Generic Particular

To show that every element of a set satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen* element of the set, and show that x satisfies the property.

Example – *Generalizing from the Generic Particular*

Consider a “mathematical trick” like the following:

> Let someone pick any number, add 5, multiply by 4, subtract 6, divide by 2, and subtract twice the original number.
>
> Then you astound the person by announcing that their final result was ….

Solution – *Generalizing from the Generic Particular*

Generalizing from the Generic Particular

The x in the analysis above is

- *particular* (it represents a single quantity), but it is also
- *arbitrarily chosen* or *generic* (any number whatsoever can be put in its place).

By showing a property of a particular but generic x, we can show that it holds for all possible x.

Proving Universal Statements

The principle of generalizing from the generic particular underlies the method of *direct proof*.

Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Example – *A Direct Proof of a Theorem*

Prove that

The sum of any two even integers is even.

Solution:

"$\forall$ integers m and n, if m, n are even then $m + n$ is even."

Existential Instantiation

One of the basic laws of logic, called *existential instantiation*, says, in effect, that if you know something exists, you can give it a name.

However, you cannot use the same name to refer to two different things, both of which are currently under discussion.

Existential Instantiation

If the existence of a certain kind of object is assumed or has been deduced then it can be given a name, as long as that name is not currently being used to denote something else.

Directions for Writing Proofs of Universal Statements

1. **Copy the statement of the theorem to be proved on your paper.**

2. **Clearly mark the beginning of your proof with the word <u>Proof</u>.**

3. **Make your proof self-contained.**

   Explain the meaning of each variable used in the proof.

4. **Write your proof in complete, grammatically correct sentences.**

Directions for Writing Proofs of Universal Statements

5. **Keep your reader informed about the status of each statement in your proof.**

   Use terms like *Suppose* or *Assume* or *we must show that*.

6. **Give a reason for each assertion in your proof.**

   Use terms *by definition of, by theorem,* etc.

7. **Include connective words to relate sentences.**

   Use words like *Then*, or *Thus*, or *So*, or *Hence*, or *Therefore*, or *Consequently*, or *It follows that*, etc.

8. **Display equations and inequalities on separate lines.**

Variations among Proofs

Proofs written by different people are rarely identical.

- Different mathematical reasoning
- Different notation
- Different wording
- Different depth of explanation

How detailed to make a proof can be adapted to the intended reader.

Common Mistakes

1. **Arguing from examples.**

   Examples are useful for the understanding, but often statements are true in many instances without being true in general.

2. **Using the same variable for two different things.**

3. **Jumping to a conclusion.**

   Alleging the truth of something without giving an adequate reason.

4. **Circular reasoning.**

   Assuming something that is to be proved.

Start and End of a Direct Proof

The first and the last sentence of direct proofs can usually be written even if you do not understand the theorem.

Example: “Every complete, bipartite graph is connected.”

Solution:

Rewrite the statement:

$$\forall \overbrace{\text{graphs } G}^{\text{domain}}, \text{if } \overbrace{G \text{ is complete and bipartite}}^{\text{hypothesis}}, \text{ then } \overbrace{G \text{ is connected}}^{\text{conclusion}}.$$

Proof Structure:

Suppose *G* is a graph such that *G* is complete and bipartite.

…

Therefore, *G* is connected.

Showing That an Existential Statement Is False

To prove an existential statement is false, you must prove its negation (a universal statement) is true.

Example: Disprove the following statement

$\exists n \in \mathbf{Z}^+$ such that $n^2 + 3n + 2$ is prime.

Solution:

Show that the following negation is true:

$\forall n \in \mathbf{Z}^+$, $n^2 + 3n + 2$ is not prime.

Showing That an Existential Statement Is False cont'd

Claim: "$\forall n \in \mathbf{Z}^+$, $n^2 + 3n + 2$ is not prime."

Proof:

Suppose n is any positive integer.

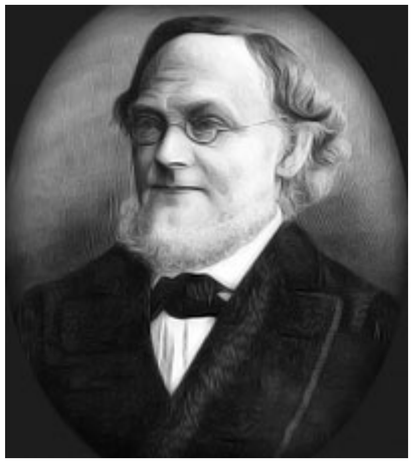
We can factor $n^2 + 3n + 2$ to obtain $n^2 + 3n + 2 = (n + 1)(n + 2)$.

Note that $n + 1$ and $n + 2$ are integers (because they are sums of integers) and that both $n + 1 > 1$ and $n + 2 > 1$ (because $n \geq 1$).

Thus $n^2 + 3n + 2$ is a product of two integers each > 1,

and so $n^2 + 3n + 2$ is not prime.

Famous Conjectures



More than 250 years ago, Christian Goldbach (1690–1764) formulated one of the oldest conjectures in mathematics that remains without proof until today, despite considerable effort.

Goldbach's conjecture:

> Every even integer greater than 2 can be expressed as the sum of two primes.

Computer-aided calculations have shown the conjecture to be true up to at least 10^{18}.

Famous Conjectures

Many other plausible conjectures in number theory have proved false.

Leonhard Euler (1707–1783), proposed in the 18th century that $a^4 + b^4 + c^4 = d^4$ had no nontrivial whole number solutions.

In 1987, Noam Elkies proved it wrong.

One counterexample, found by Roger Frye of Thinking Machines Corporation in a long computer search, is $95{,}800^4 + 217{,}519^4 + 414{,}560^4 = 422{,}481^4$.

SECTION 4.2

Direct Proof and Counterexample II: Rational Numbers

Direct Proof and Counterexample II: Rational Numbers

• Definition

A real number r is **rational** if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is **irrational.** More formally, if r is a real number, then

$$r \text{ is rational } \Leftrightarrow \exists \text{ integers } a \text{ and } b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0.$$

The word *rational* contains the word *ratio*, which is another word for quotient. A rational number can be written as a ratio of integers.

Exercise – *Determining Whether Numbers Are Rational or Irrational*

Argue for each of the following terms, whether it is a rational number or not:

a. 10/3

b. – 5/39

c. 0.281

d. 0.666…

e. 7

f. 0

g. 2/0

h. $(m + n)/mn$, where m and n are integers and neither m nor n is zero

Example – *Sum of Rationals Is Rational*

Prove the following theorem using a direct proof:

> The sum of any two rational numbers is rational.

Solution:

Formal Restatement: $\forall$ real numbers r and s, if r and s are rational then $r + s$ is rational.

Suppose r and s are rational numbers.

By definition of rational, r and s can be written as

$$r = \frac{a}{b} \quad \text{and} \quad s = \frac{c}{d} \quad \text{for some integers } a, b, c, \text{ and } d \text{ where } b \neq 0 \text{ and } d \neq 0.$$

Solution – *Sum of Rationals Is Rational*

$$r + s = \frac{a}{b} + \frac{c}{d} \qquad \text{by substitution}$$

$$= \frac{ad + bc}{bd} \qquad \text{by basic algebra.}$$

Let $p = ad + bc$ and $q = bd$. Then p and q are integers because products and sums of integers are integers and because a, b, c, and d are all integers.

Also $q \neq 0$ since $b \neq 0$ and $d \neq 0$.

Thus $r + s = \dfrac{p}{q}$ where p and q are integers and $q \neq 0$.

Therefore, $r + s$ is rational by definition of a rational number.

Deriving New Mathematics from Old

A **corollary** is a statement whose truth can be immediately deduced from a theorem that has already been proved.

Example: Derive the following as a corollary

> The double of a rational number is rational.

Solution:

Suppose r is any rational number. Then $2r = r + r$ is a sum of two rational numbers.

Hence, by Theorem X (The sum of rationals is rational), $2r$ is rational.

SECTION 4.3

Direct Proof and Counterexample III: Divisibility

Direct Proof and Counterexample III: Divisibility

Divisibility is the central concept of **number theory**, the study of properties of integers.

• Definition

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

n is **divisible by** d if, and only if, n equals d times some integer.

Instead of "n is divisible by d," we can say that

n **is a multiple of** d, or
d **is a factor of** n, or
d **is a divisor of** n, or
d **divides** n.

The notation $\mathbf{d \mid n}$ is read "d divides n." Symbolically, if n and d are integers and $d \neq 0$:

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk.$$

Exercise – *Divisibility*

a. Is 5271 divisible by 3?

b. Does 5 divide 40?

c. Does 7 | 314?

d. Is 32 a multiple of −16?

e. Is 6 a factor of 54?

f. Is 7 a factor of −7?

g. Is 798 a multiple of 17?

h. Is $n^7 - n$ divisible by 42?

Direct Proof and Counterexample III: Divisibility

Two important properties:

Theorem 4.3.1 A Positive Divisor of a Positive Integer

For all integers a and b, if a and b are positive and a divides b, then $a \leq b$.

Theorem 4.3.2 Divisors of 1

The only divisors of 1 are 1 and -1.

Exercise – *Divisibility of Algebraic Expressions*

a. If a and b are integers, is $3a + 3b$ divisible by 3?

b. If k and m are integers, is $10km$ divisible by 5?

Solution:

a.

b.

Direct Proof and Counterexample III: Divisibility

The definition of nondivisibility follows from the negation of divisibility:

For all integers n and d, $d \nmid n \Leftrightarrow \frac{n}{d}$ is not an integer.

Note that since divisibility is defined using an existential statement, nondivisibility uses a universal statement.

Example: Does 4 | 15?

Solution:

No, $\frac{15}{4} = 3.75$ which is not an integer.

Proving Properties of Divisibility

One of the most useful properties of divisibility is that it is transitive. If one number divides a second and the second number divides a third, then the first number divides the third.

Theorem 4.3.3 Transitivity of Divisibility

For all integers a, b, and c, if a divides b and b divides c, then a divides c.

Exercise – *Transitivity of Divisibility*

Prove that for all integers a, b, and c,

if $a \mid b$ and $b \mid c$, then $a \mid c$.

Solution:

Solution – *Transitivity of Divisibility*

Counterexamples and Divisibility

To show that a proposed divisibility property is not universally true, you need only find one pair of integers for which it is false.

Example: Is the following statement true or false?

For all integers a and b, if $a \mid b$ and $b \mid a$ then $a = b$.

Solution:

Proposed Divisibility Property: For all integers a and b, if $a \mid b$ and $b \mid a$ then $a = b$.

Counterexample: Let $a = 2$ and $b = -2$. Then

$$a \mid b \text{ since } 2 \mid (-2) \text{ and } b \mid a \text{ since } (-2) \mid 2, \text{ but } a \neq b \text{ since } 2 \neq -2.$$

Therefore, the statement is false.

The Unique Factorization of Integers Theorem

Theorem 4.3.5 Unique Factorization of Integers Theorem (Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k},$$

and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

Example: $588 = 3^1 * 2^2 * 7^2$

The Unique Factorization of Integers Theorem

Because of the unique factorization theorem, any integer $n > 1$ can be put into a *standard factored form* in which the prime factors are written in ascending order from left to right.

• Definition

Given any integer $n > 1$, the **standard factored form** of n is an expression of the form

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

where k is a positive integer; $p_1, p_2, \ldots, p_k$ are prime numbers; $e_1, e_2, \ldots, e_k$ are positive integers; and $p_1 < p_2 < \cdots < p_k$.

Example: $588 = 2^2 * 3^1 * 7^2$

Example – *Using Unique Factorization to Solve a Problem*

Suppose m is an integer such that

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10.$$

Does $17 \mid m$?

Solution:

SECTION 4.4

Direct Proof and Counterexample IV: Division into Cases and the Quotient-Remainder Theorem

Direct Proof and Counterexample IV: Division into Cases and the Quotient-Remainder Theorem

Theorem 4.4.1 The Quotient-Remainder Theorem

Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

Example: For each of the following values of n and d, find integers q and r such that $n = dq + r$ and $0 \leq r < d$.

a. $n = 54, d = 4$ **b.** $n = -54, d = 4$ **c.** $n = 54, d = 70$

Solution:

a.

b.

c.

div and mod

• Definition

Given an integer n and a positive integer d,

$$\begin{aligned} \textbf{\textit{n div d}} &= \text{the integer quotient obtained} \\ &\quad \text{when } n \text{ is divided by } d, \text{ and} \\ \textbf{\textit{n mod d}} &= \text{the nonnegative integer remainder obtained} \\ &\quad \text{when } n \text{ is divided by } d. \end{aligned}$$

Symbolically, if n and d are integers and $d > 0$, then

$$n \; div \; d = q \quad \text{and} \quad n \; mod \; d = r \quad \Leftrightarrow \quad n = dq + r$$

where q and r are integers and $0 \leq r < d$.

div and **mod** are built-in functions of most programming languages.

Called div and mod in Pascal, / and % in C, C++ and Java, / (or \) and mod in C#.

Exercise – *Computing div and mod*

Compute 1232 *div* 9 and 1232 *mod* 9 by hand and with a simple calculator.

Solution:

Representations of Integers

Recall the definition of even and odd

• Definitions

An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

$$n \text{ is even} \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = 2k.$$
$$n \text{ is odd} \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = 2k + 1.$$

We can use the quotient-remainder theorem to show the **parity property** of integers:

Any integer is either even or odd.

Representations of Integers

Proof.

For any integer n, by the quotient-remainder theorem (with $d = 2$), there exist unique integers q and r such that

$$n = 2q + r \text{ and } 0 \leq r < 2.$$

Thus, given any integer n, there exists an integer q with

$$n = 2q + 0 \text{ or } n = 2q + 1.$$

By definition of integer, in the first case, n is even; in the latter case, n is odd.

Because q and r are unique, n cannot be both even and odd. We have established the parity property.

Example – *Consecutive Integers Have Opposite Parity*

Two integers m, n are *consecutive* if, and only if, $n = m + 1$ or $m = n + 1$. Prove that

> Given any two consecutive integers, one is even and the other is odd.

Solution:

Solution – *Consecutive Integers Have Opposite Parity*

Proof by Division into Cases

Just applied the general rule of proof by division into cases…

Method of Proof by Division into Cases

To prove a statement of the form "If A_1 or A_2 or . . . or A_n, then C," prove all of the following:

If A_1, then C,

If A_2, then C,

⋮

If A_n, then C.

This process shows that C is true regardless of which of $A_1, A_2, \ldots, A_n$ happens to be the case.

Absolute Value and the Triangle Inequality

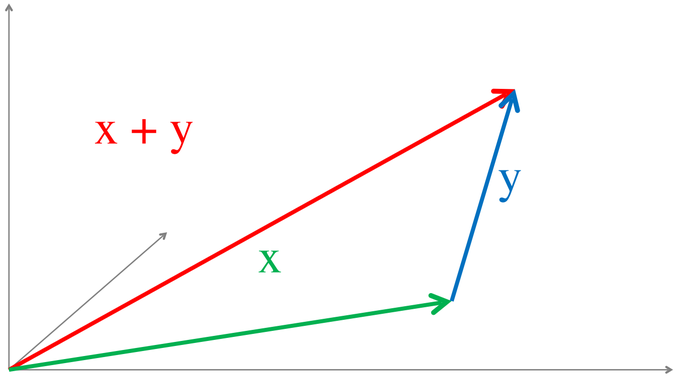
• Definition

For any real number x, the **absolute value of x**, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}.$$

Theorem 4.4.6 The Triangle Inequality

For all real numbers x and y, $|x + y| \leq |x| + |y|$.



Absolute Value and the Triangle Inequality

A **lemma** is a statement that does not have much intrinsic interest but is helpful in deriving other results.

Lemma 4.4.4

For all real numbers r, $-|r| \leq r \leq |r|$.

Lemma 4.4.5

For all real numbers r, $|-r| = |r|$.

Lemmas are often useful to break down long and complex proofs into intermediate steps, or to give a proof a more lucid structure.

Absolute Value and the Triangle Inequality

Theorem 4.4.6 The Triangle Inequality

For all real numbers x and y, $|x + y| \leq |x| + |y|$.

Proof.

Let x and y be any two real numbers.

In the case of $|x + y| = x + y$, it holds that
$|x + y| = x + y \leq |x| + y \leq |x| + |y|$, by Lemma 4.4.4.

In the case of $|x + y| = -(x + y)$, it holds that
$|x + y| = -(x + y) = (-x) + (-y) \leq |-x| + |-y|$ by Lemma 4.4.4
$= |x| + |y|$, by Lemma 4.4.5.

Hence, the inequality holds in both possible cases.

SECTION 4.6

Indirect Argument: Contradiction and Contraposition

Example – *There Is No Greatest Integer*

Prove or disprove the following:

> There is no greatest integer.

Informal Solution:

> ”If there were a greatest integer, you could add 1 to it to obtain an even greater integer. So there cannot be a greatest integer.”

Such reasoning is the heart of the type of indirect proof called proof by contradiction.

Indirect Argument by Contradiction

Method of Proof by Contradiction

1. Suppose the statement to be proved is false. That is, suppose that the negation of the statement is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

Proof by Contradiction is also known as *reductio ad impossibile* or *reductio ad absurdum*.

Note that an *argument by contradiction*, is based on the fact that either a statement is true or it is false but not both.

Example – *There Is No Greatest Integer*

Theorem 4.6.1

There is no greatest integer.

Proof:

Indirect Argument by Contraposition

Method of Proof by Contraposition

1. Express the statement to be proved in the form

   $$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x).$$

   (This step may be done mentally.)

2. Rewrite this statement in the contrapositive form

   $$\forall x \text{ in } D, \text{ if } Q(x) \text{ is false then } P(x) \text{ is false.}$$

   (This step may also be done mentally.)

3. Prove the contrapositive by a direct proof.

   a. Suppose x is a (particular but arbitrarily chosen) element of D such that $Q(x)$ is false.

   b. Show that $P(x)$ is false.

Example – *Square of an Even Integer Is Even*

Prove the following:

For all integers n, if n^2 is even then n is even.

Solution:

Contrapositive: For all integers n, if n is not even then n^2 is not even.

= $\forall n \in \mathbf{Z}$, if n is odd then n^2 is odd.

Solution – *Square of an Even Integer Is Even*

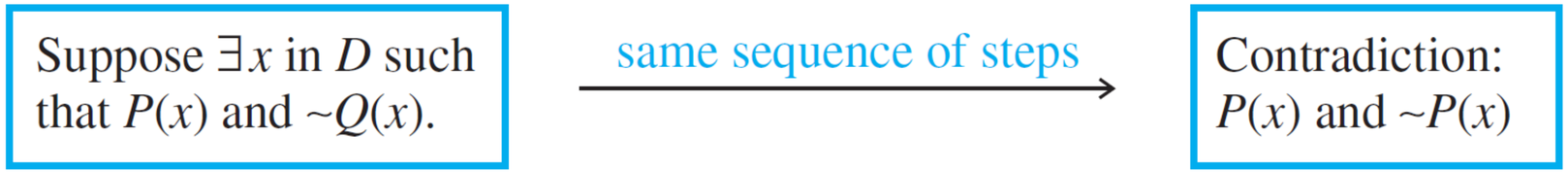
Proof (by contraposition):

Suppose n is any odd integer.

Relation between Proofs by Contradiction and by Contraposition

Any proof by contraposition can be recast in the language of proof by contradiction.

Proof by Contraposition



Proof by Contradiction

Exercise – *Square of an Even Integer Is Even*

For all integers n, if n^2 is even then n is even.

Proof (by contradiction):

For the sake of contradiction, assume:

$\exists n \in \mathbf{Z}$ such that n^2 is even and n is odd.

Relation between Proof by Contradiction and Proof by Contraposition

Proof by contraposition can only be used for statements that are universal and conditional.

Any statement that can be proved by contraposition can also be proved by contradiction. But the converse is not true.

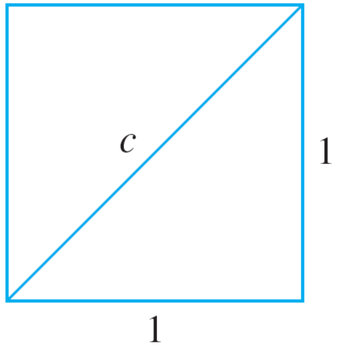
Proof by contradiction also works for other types of statements. Statements such as "$\sqrt{2}$ is irrational" can be proved by contradiction but not by contraposition.

SECTION 4.7

Indirect Argument: Two Classical Theorems

The Irrationality of $\sqrt{2}$

By the Pythagorean theorem, we know that the diagonal c of the unit square equals $\sqrt{2}$, since $c^2 = 1^2 + 1^2 = 2$, and so $c = \sqrt{2}$.



The claim is that $\sqrt{2}$ is irrational, i.e. there are no integers a and b such that

$$\frac{c}{1} = \frac{\sqrt{2}}{1} = \sqrt{2} = \frac{a}{b}.$$

The Irrationality of $\sqrt{2}$

Theorem 4.7.1 Irrationality of $\sqrt{2}$

$\sqrt{2}$ is irrational.

Proof (by contradiction):

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

Then there are integers m and n with no common factors such that

$$\sqrt{2} = m/n,$$

by dividing m and n by any common factors if necessary

Squaring both sides yields

$$2 = m^2/n^2 \Leftrightarrow m^2 = 2n^2$$

The Irrationality of $\sqrt{2}$

Note that thus m^2 is even, and therefore also m is even (as shown earlier).

By definition of even, it holds that

$m = 2k$ for some integer k.

Substituting m, we get

$m^2 = (2k)^2 = 4k^2$ and since $m^2 = 2n^2$ thus $4k^2 = 2n^2$.

It follows that $n^2 = 2k^2$, which implies that n^2 is even, and thus also n is even.

But we also know that m is even. Hence both m and n have the common factor of 2, which contradicts the supposition that m and n have no common factors.

Are There Infinitely Many Prime Numbers?

Another classical theorem can be proved by contradiction, Euclid's theorem on prime numbers:

Theorem 4.7.4 Infinitude of the Primes

The set of prime numbers is infinite.

The idea of Euclid's proof is this:

> Suppose the set of prime numbers were finite. Then you could take the product of all the prime numbers and add one, to receive another prime number, which was not in the set.

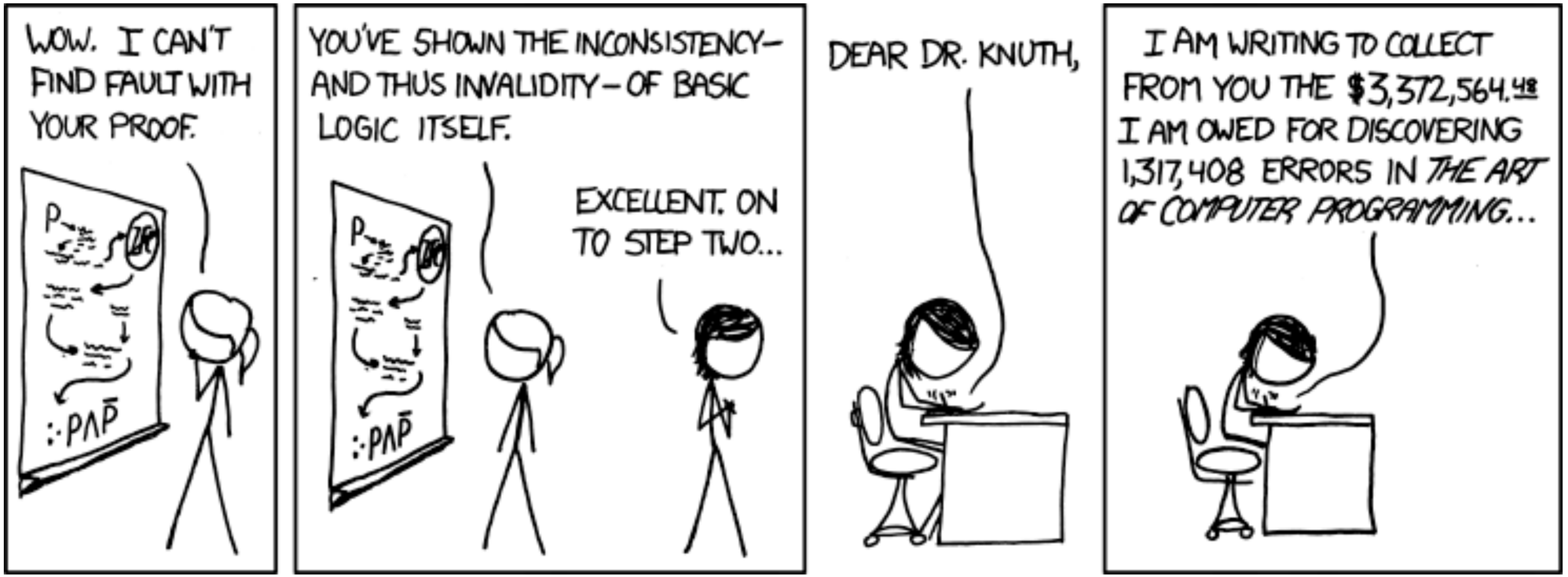
Euclid
(325–265 BC)

When to Use Indirect Proof

Many theorems can be proved either way, by direct as well as by indirect proof.

If you have no obvious clues,

- try first to prove a statement directly.
- Then, if that does not succeed, look for a counterexample.
- If the search for a counterexample is unsuccessful, look for a proof by contradiction or contraposition.



SECTION 4.8

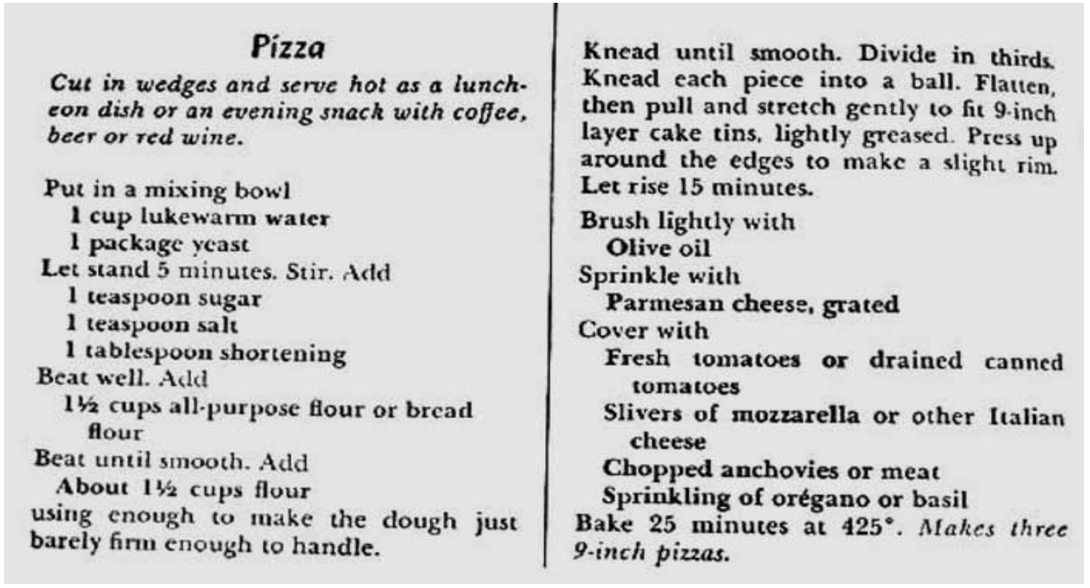
Application: Algorithms

Application: Algorithms

Algorithm ≈ step-by-step method for performing an action.

Examples:

- food recipes, directions for assembling furniture, sewing pattern instructions
- algorithms for doing arithmetic such as multidigit addition and subtraction, multiplication and division.



Pizza

Cut in wedges and serve hot as a luncheon dish or an evening snack with coffee, beer or red wine.

Put in a mixing bowl
- 1 cup lukewarm water
- 1 package yeast

Let stand 5 minutes. Stir. Add
- 1 teaspoon sugar
- 1 teaspoon salt
- 1 tablespoon shortening

Beat well. Add
- 1½ cups all-purpose flour or bread flour

Beat until smooth. Add
- About 1½ cups flour

using enough to make the dough just barely firm enough to handle.

Knead until smooth. Divide in thirds. Knead each piece into a ball. Flatten, then pull and stretch gently to fit 9-inch layer cake tins, lightly greased. Press up around the edges to make a slight rim. Let rise 15 minutes.

Brush lightly with
- Olive oil

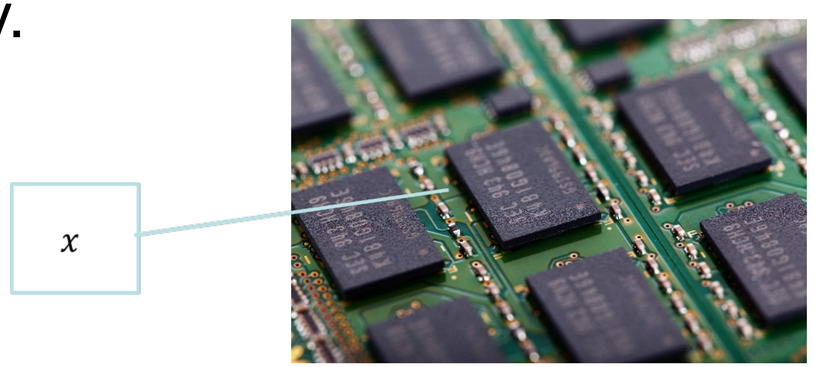
Sprinkle with
- Parmesan cheese, grated

Cover with
- Fresh tomatoes or drained canned tomatoes
- Slivers of mozzarella or other Italian cheese
- Chopped anchovies or meat
- Sprinkling of orégano or basil

Bake 25 minutes at 425°. *Makes three 9-inch pizzas.*

An Algorithmic Language

The term **variable** is used to refer to a specific storage location in a computer's memory.



An **assignment statement** gives a value to a variable. It has the form

$$x := e,$$

where x is a variable and e is an expression. This is read "x is assigned the value e" or "let x be e."

An Algorithmic Language

When an assignment statement $x := e$ is executed

- the expression e is evaluated (using the current values of all the variables in the expression), and then
- its value is placed in the memory location corresponding to x (replacing any previous content at this location).

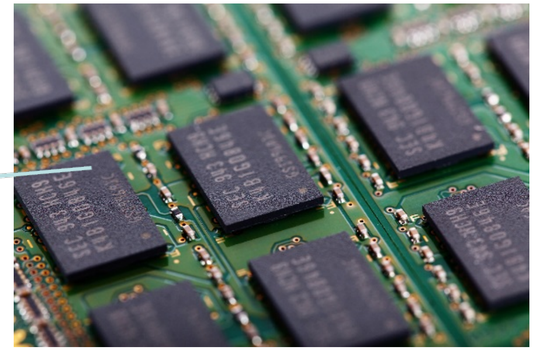
Algorithm statements are executed one after another in the order in which they are written.

Example:

$x := 2$

$y := 3$

$x := x + y$



An Algorithmic Language

Conditional statements are denoted either as

a. **if** (*condition*)
then s_1
else s_2

or

b. **if** (*condition*) **then** s_1

where *condition* is a predicate involving algorithm variables, s_1 and s_2 are algorithm statements or groups of algorithm statements.

Execution:

If the *condition* expression is evaluated to *true* then s_1 is executed; if it is evaluated to *false*, then s_2 is executed. (Or execution continues straight after the **if-then** statement)

Exercise – *Execution of if-then-else and if-then Statements*

Consider the following algorithm segments:

a. **if** $x > 2$
then $y := x + 1$
else do $x := x - 1$
$y := 3 \cdot x$ **end do**

b. $y := 0$
if $x > 2$ **then** $y := 2^x$

What is the value of y after execution of these segments for the following values of x?

i. $x = 5$

ii. $x = 2$

Solution:

a. i. $y =$ ii. $y =$

b. i. $y =$ ii. $y =$

An Algorithmic Language

Iterative statements are used when a sequence of algorithm statements is to be executed over and over again. The first type of iterative statements is the **while** loop.

```
while (condition)
    [statements that make up
    the body of the loop]
end while
```

Execution:

In every iteration, the *condition* expression is evaluated. If it is *true* then the body is executed; otherwise execution is continued after **end while**.

Example – *Tracing Execution of a while Loop*

Trace the execution of the following algorithm segment by finding the values of all the algorithm variables each time they are changed during execution:

$i := 1, s := 0$

while $(i \leq 2)$

    $s := s + i$

    $i := i + 1$

end while

Solution:

A *trace table* shows the current values of the variables during execution.

An Algorithmic Language

The second form of iteration is a **for-next** loop:

for *variable* := *initial expression* **to** *final expression*

[statements that make up
the body of the loop]

next *(same) variable*

Execution:

Initially, *variable* is assigned the value of *initial expression*.

Then, in every iteration,

- if the value of variable is ≤ value of *final expression*, the body is executed and *variable* is increased by 1 (**next**).
- if the value of *variable* is > the value of *final expression*, then execution continues after the line with **next**.

Exercise – *Trace Table for a **for-next** Loop*

Convert the **for-next** loop shown below into a **while** loop. Construct a trace table for the loop.

```
for i := 1 to 4
    x := i^2
next i
```

Solution:

Iteration Number

Variable Name	0	1	2	3	4
x		1	4	9	16
i	1	2	3	4	5

The Division Algorithm

The quotient-remainder theorem says that tan integer a can be written as $a = dq + r$ where $0 \leq r < d$.

The Division Algorithm calculates q and r for given nonegative a and d. It works by subtracting d repeatedly from a until the result is less than d but still ≥ 0.

$$0 \leq a - d - d - d - \cdots - d = a - dq < d.$$

The total number of d's that are subtracted is the quotient q. The quantity $a - dq$ equals the remainder r.

Note that the calculated q and r correspond to

$$q = a \operatorname{div} d \quad \text{and} \quad r = a \bmod d.$$

The Division Algorithm

Input: a [nonnegative integer], d [positive integer]

Algorithm body:

$r := a, q := 0$

while $(r \geq d)$
  $r := r - d$
  $q := q + 1$
end while

After execution of the **while** *loop,* $a = dq + r$

Output:

q, r [nonnegative integers]

The Euclidean Algorithm

• Definition

Let a and b be integers that are not both zero. The **greatest common divisor** of a and b, denoted $\mathbf{gcd}(\boldsymbol{a}, \boldsymbol{b})$, is that integer d with the following properties:

1. d is a common divisor of both a and b. In other words,

$$d \mid a \quad \text{and} \quad d \mid b.$$

2. For all integers c, if c is a common divisor of both a and b, then c is less than or equal to d. In other words,

$$\text{for all integers } c, \text{ if } c \mid a \text{ and } c \mid b, \text{ then } c \leq d.$$

Example – *Calculating Some gcd's*

a. Find gcd(72, 63).

b. Find gcd(10^{20}, 6^{30}).

Solution:

a.

b.

The Euclidean Algorithm

The Euclidean algorithm is based on the following two facts:

Lemma 4.8.1

If r is a positive integer, then $\gcd(r, 0) = r$.

Lemma 4.8.2

If a and b are any integers not both zero, and if q and r are any integers such that

$$a = bq + r,$$

then

$$\gcd(a, b) = \gcd(b, r).$$

Example:

$$96 = 42 \cdot 2 + 12 \rightarrow \gcd(96,42) = \gcd(42,12)$$

$$42 = 12 \cdot 3 + 6 \rightarrow = \gcd(12,6)$$

$$12 = 6 \cdot 2 + 0 \rightarrow = \gcd(6,0) = 6$$

The Division Algorithm

Input: A, B [integers with $A > B \geq 0$]

Algorithm body:

$a := A, b := B, r := B$
while $(b \neq 0)$
  $r := a \bmod b$
  $a := b$
  $b := r$
end while
$\gcd := a$

If $b \neq 0$, compute a mod b, the remainder of the integer division of a by b, and set r equal to this value.
Then repeat the process using b in place of a and r in place of b.

After execution of the **while** *loop,* $\gcd(A, B) = a$.

Output:

gcd [a positive integer]

Exercise – *Hand-Calculation of gcd's Using the Euclidean Algorithm*

Use the Euclidean algorithm to find gcd(330, 156).

$a := A, b := B, r := B$
while $(b \neq 0)$
$r := a \bmod b$
$a := b$
$b := r$
end while
gcd $:= a$

Solution:
trace table

Iteration number

Variable

The Euclidean Algorithm

Does the algorithm always **terminate**?

Yes, here is the **proof**:

Initially, it holds that $a > b \geq 0$.

In each iteration of the while loop,

- if $b = 0$, execution jumps to the last line and **terminates**
- if not, the loop body is executed with the effect that the new value of a equals b and the new value of b equals $a \bmod b$.

Since $a \bmod b < b$, and we start with $a > b$, the invariant $a > b$ holds in each iteration of the loop. Furthermore, a and b are both **decreased** in each iteration.

Since b decreases in each iteration and $a \bmod b \geq 0$, b will eventually equal 0, make the while condition false such that the execution jumps to the last line and the algorithm **terminates**.

Recap

Proof by example and counterexample

- proving existential statements and disproving universal statements

Method of direct proof

- proving universal statements
- disproving existential statements
- directions for writing (direct) proofs

Proof by division into cases, contradiction and contraposition

- analogy between contradiction and contraposition proofs

Algorithmic language and Euclidean GCD algorithm