Chapter 4.1

Direct proof and counterexample - introduction

Number theory and methods of proof

Discrete Mathematics

Hisham Ihshaish

Based on: Epp, Discrete Mathematics with Applications, 4th ed., Section 4.1

Chapter 4.1

Direct proof and counterexample - introduction

In this session:

- Part 1: Why number theory for programmers
- Part 2: Even, odd, prime, composite
- Part 3: How to prove and disprove statements
- Part 4: Disproof by counterexample
- Part 5: Direct proofs

Chapter 4.1

Direct proof and counterexample - introduction

In this session:

Why number theory for programmers?

Software is full of integers. Loops, indices, array bounds, hash codes, modular arithmetic, cryptography, error-correcting codes - all rest on properties of integers.

Why proofs?

Bugs come from imprecise thinking. Proving a property forces you to state exactly what you assume and what you conclude.

Critical software (medical devices, payment systems, autonomous vehicles) cannot rely on testing alone - some claims must be proven correct.

Many algorithms (binary search, RSA, hashing) only work because of integer-theoretic facts. To use them safely, you need to understand the proofs.

Chapter 4.1

Direct proof and counterexample - introduction

In this session:

- Part 1: Why number theory for programmers
- **Part 2: Even, odd, prime, composite**
- Part 3: How to prove and disprove statements
- Part 4: Disproof by counterexample
- Part 5: Direct proofs

Definitions: even and odd integers

Definition

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:

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

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

Epp, Definition, p. 147

Examples: even and odd

Use the definitions to justify each answer.

(a) Is 0 even?

Yes. $0 = 2(0)$ - $k = 0$ is the witness.

(b) Is −301 odd?

Yes. $-301 = 2(-151) + 1$.

(c) If a, b are integers, is $6a^2b$ even?

Yes. $6a^2b = 2(3a^2b)$, and $3a^2b$ is an integer (product of integers).

(d) If a, b are integers, is $10a + 8b + 1$ odd?

Yes. $10a + 8b + 1 = 2(5a + 4b) + 1$, and $5a + 4b$ is an integer.

(e) Is every integer either even or odd?

Yes - we will prove this in 4.4 using the quotient-remainder theorem.

Definitions: prime and composite

Definition

An integer n is prime if, and only if, n > 1 and for all positive integers r and s, if n = rs then r = 1 and s = n, or r = n and s = 1.

An integer n is composite if, and only if, n > 1 and n = rs for some integers r, s with 1 < r < n and 1 < s < n.

Symbolically:

$$n \text{ is prime } \Leftrightarrow \forall \text{ positive integers } r, s, \text{ if } n = rs \text{ then } (r = 1 \wedge s = n) \vee (r = n \wedge s = 1)$$

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

Epp, Definition, p. 148

Examples: prime and composite

(a) Is 1 prime?

No. The definition of prime requires $n > 1$. By convention, 1 is neither prime nor composite.

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

Yes. Given any integer $n > 1$, either it has only the trivial factorisations $1 \cdot n$ and $n \cdot 1$ (so n is prime), or it has a factorisation $n = rs$ with $1 < r < n$ and $1 < s < n$ (so n is composite).

(c) First six primes

$$2,\ 3,\ 5,\ 7,\ 11,\ 13$$

(d) First six composites

$$4,\ 6,\ 8,\ 9,\ 10,\ 12$$

Important note

To show n is prime, you must rule out ALL non-trivial factorisations (universal claim).
To show n is composite, you only need to exhibit ONE non-trivial factorisation (existential claim).

Epp, Example 4.1.2, p. 148

Chapter 4.1

Direct proof and counterexample - introduction

In this session:

- Part 1: Why number theory for programmers
- Part 2: Even, odd, prime, composite
- **Part 3: How to prove and disprove statements**
- Part 4: Disproof by counterexample
- Part 5: Direct proofs

How to prove and disprove statements

Before proving or disproving, write the statement as universal or existential.

Universal: $\forall x \in D, Q(x)$

To prove

Direct proof

Take an arbitrary $x \in D$ and show $Q(x)$ holds. No specific value works - the argument must cover every x.

To disprove

Counterexample

Find one specific $x \in D$ for which $Q(x)$ fails. One counterexample is enough.

Existential: $\exists x \in D$ such that $Q(x)$

To prove

Exhibit one example

Find one specific $x \in D$ for which $Q(x)$ holds. One witness is enough.

To disprove

Negate, then prove the negation

The negation is universal: $\forall x \in D, \sim Q(x)$. Prove it by direct proof.

Chapter 4.1

Direct proof and counterexample - introduction

In this session:

- Part 1: Why number theory for programmers
- Part 2: Even, odd, prime, composite
- Part 3: How to prove and disprove statements
- **Part 4: Disproof by counterexample**
- Part 5: Direct proofs

Disproof by counterexample

Disprove by counterexample

To disprove $\forall x \in D$, if P(x) then Q(x), find one $x \in D$ for which P(x) is true but Q(x) is false. Such an x is called a **counterexample**.

Disprove the following statement:

$$\forall a, b \in \mathbb{R}, \text{ if } a^2 = b^2 \text{ then } a = b.$$

Counterexample

Let $a = 1$ and $b = -1$.

Then $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$, so $a^2 = b^2$ (the hypothesis holds).

But $a \neq b$ since $1 \neq -1$ (the conclusion fails).

Therefore the statement is false.

Epp, Example 4.1.4, p. 150

Chapter 4.1

Direct proof and counterexample - introduction

In this session:

- Part 1: Why number theory for programmers
- Part 2: Even, odd, prime, composite
- Part 3: How to prove and disprove statements
- Part 4: Disproof by counterexample
- **Part 5: Direct proofs**

Method of exhaustion

When the domain is finite, prove a universal statement by checking every case.

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

$4 = 2 + 2$	$6 = 3 + 3$	$8 = 3 + 5$	$10 = 5 + 5$
$12 = 5 + 7$	$14 = 11 + 3$	$16 = 5 + 11$	$18 = 7 + 11$
$20 = 7 + 13$	$22 = 5 + 17$	$24 = 5 + 19$	$26 = 7 + 19$

This works for finitely many cases. But for infinite domains - say, all positive integers - we cannot list every case. We need a more powerful method.

Epp, Example 4.1.5, p. 151

Generalising from the generic particular

Method of generalising from the generic particular

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

Method of direct proof

1	Express the statement to be proved in the form $\forall x \in D$, if P(x) then Q(x). (Often done mentally.)
2	Suppose x is a particular but arbitrarily chosen element of D for which P(x) holds. (Often abbreviated 'Suppose $x \in D$ and P(x).')
3	Show that Q(x) follows, using definitions, previously established results, and rules of inference.

Epp, p. 151-152

Worked direct proof: sum of two evens is even

Theorem. The sum of any two even integers is even.

Formal restatement

$\forall\, m, n \in \mathbb{Z},$ if m and n are even, then $m + n$ is even.

Proof

Suppose m and n are particular but arbitrarily chosen even integers.

[We must show that $m + n$ is even.]

By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s.

Then $m + n = 2r + 2s = 2(r + s)$ by the distributive law.

Let $t = r + s$. Then t is an integer (sum of integers is an integer), and $m + n = 2t$.

Therefore $m + n$ equals 2 times an integer, so by definition of even, $m + n$ is even.

Epp, Theorem 4.1.1, p. 154

Summary

Definitions are foundational.

Even, odd, prime, composite all have precise definitions. Memorise them word for word. Both directions of "if and only if" are used in proofs.

Statements are universal or existential.

Identify the shape first. Universal: $\forall x, Q(x)$. Existential: $\exists x, Q(x)$. The right strategy depends on the shape.

To disprove a universal, find one counterexample.

The counterexample must satisfy the hypothesis and fail the conclusion. One witness is enough.

To prove a universal, use the direct-proof template.

Suppose $x \in D$ and $P(x)$. Use definitions and prior results. Conclude $Q(x)$. The argument must work for any x.

Recommended exercises

From Epp, Exercise Set 4.1 (pp. 161-162). Grouped by skill.

Apply the definitions *Drills on even, odd, prime, composite.*	**Exercises 1, 2, 3**
Disprove by counterexample *Show that a given existential statement is false.*	**Exercises 35, 36, 37**
Direct proof - core *One-paragraph direct proofs about even and odd integers.*	**Exercises 24, 25, 27, 28, 29**
Direct proof - combined properties *Combine two integer properties (e.g. odd plus even).*	**Exercises 31, 32, 33**
Find the mistake in a proof *Read a flawed proof and identify the error. High-value for the midterm.*	**Exercises 38, 39, 40**

Next session

Chapter 4.2

Rational numbers and proving their properties

Definition of rational and irrational numbers
Theorem: every integer is rational
Theorem: the sum of any two rational numbers is rational
More practice with the direct-proof template