Discrete Mathematics

Chapter 4.3

Direct Proof and Counterexample III

Divisibility

Hisham Ihshaish - Birzeit University

Based on Susanna S. Epp, Discrete Mathematics with Applications, 4th ed., Section 4.3

Chapter 4.3

Direct proof and counterexample - divisibility

In this session:

Part 1: What is divisibility

Part 2: Proving properties of divisibility

Part 3: The unique factorization theorem

Definition of divisibility

If n and d are integers and d ≠ 0, then

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

Equivalent ways to say the same thing:

- n is a multiple of d
- d is a divisor of n
- d is a factor of n
- d divides n

Notation and symbolic form

d | n is read *"d divides n".*

d | n ⇔ ∃ an integer k such that n = dk

Examples - is it divisible?

Is 21 divisible by 3?

Yes. $21 = 3 \cdot 7$

Does 5 divide 40?

Yes. $40 = 5 \cdot 8$

Does 7 | 42?

Yes. $42 = 7 \cdot 6$

Is 32 a multiple of −16?

Yes. $32 = (-16) \cdot (-2)$

Is 6 a factor of 54?

Yes. $54 = 6 \cdot 9$

Is 7 a factor of −7?

Yes. $-7 = 7 \cdot (-1)$

Does k divide 0, for every nonzero integer k?

Yes. For any nonzero integer k, $\mathbf{0 = k \cdot 0}$, and 0 is an integer.

So every nonzero integer divides 0 - but 0 divides only 0 (and we exclude that since d ≠ 0).

Caution: “a | b” versus “a / b”

a | b

is the sentence “a divides b”.

It is either true or false. There is no number called “a | b”.

Example: 3 | 12 is true; 3 | 7 is false.

a / b

is the number obtained when a is divided by b.

It may or may not be an integer.

Example: 12 / 3 = 4; 7 / 3 ≈ 2.333

Checking nondivisibility

For all integers n and d with d ≠ 0, $\mathbf{d \nmid n} \Leftrightarrow$ n / d is not an integer.

Example. Does 4 | 15 ? **No,** because 15 / 4 = 3.75, which is not an integer.

Equivalently: for every integer k, 15 ≠ 4k.

Divisibility of algebraic expressions

To prove that something is divisible by d, factor d out and show what is left is an integer.

(a) If a and b are integers, is 3a + 3b divisible by 3?

Yes. By the distributive law, $\mathbf{3a + 3b = 3(a + b)}$,

and a + b is an integer because it is the sum of two integers.

Hence 3a + 3b = 3 · (some integer), so 3 | (3a + 3b).

(b) If k and m are integers, is 10km divisible by 5?

Yes. By the associative law, $\mathbf{10km = 5 \cdot (2km)}$,

and 2km is an integer because it is the product of three integers.

Hence 10km = 5 · (some integer), so 5 | (10km).

Prime numbers, restated using divisibility

Recall (§4.1): an integer n > 1 is prime if its only positive integer factors are 1 and itself.

Equivalent definition (using "divides")

An integer n > 1 is prime if, and only if, its only positive integer divisors are 1 and n itself.

Two small consequences worth keeping in mind:

1 is not prime.

By convention. We require n > 1.

Reason: if 1 were prime, prime factorisations would not be unique - e.g. $6 = 2\cdot3 = 1\cdot2\cdot3 = 1\cdot1\cdot2\cdot3$ …

p prime ⇒ the only positive divisors of p are 1 and p.

So if d > 1 is a positive divisor of a prime p, then d = p.

This will be used in proofs about primes.

Chapter 4.3

Direct proof and counterexample - divisibility

In this session:

- Part 1: What is divisibility
- **Part 2: Proving properties of divisibility**
- Part 3: The unique factorization theorem

Theorem 4.3.1 - positive divisor of a positive integer

For all integers a and b, if a and b are positive and a | b, then a ≤ b.

Proof.

Suppose a and b are positive integers with a | b. [We must show a ≤ b.]

By definition of divisibility, b = ak for some integer k.

Since a > 0 and b > 0, the integer k must also be positive.

Every positive integer is at least 1, so 1 ≤ k.

Multiplying both sides by the positive number a preserves the inequality:

$a \cdot 1 \le a \cdot k$, i.e. $a \le ak = b$.

Therefore a ≤ b. ∎

Theorem 4.3.2 - the divisors of 1

The only divisors of 1 are 1 and −1.

Proof sketch.

$\mathbf{1 \cdot 1 = 1}$ and $\mathbf{(-1)(-1) = 1}$, so both 1 and −1 are divisors of 1.

Now suppose m is any integer with m | 1. Then 1 = mn for some integer n.

Since the product mn is positive, m and n have the same sign.

Case 1: m, n > 0.

By Theorem 4.3.1, m ≤ 1. The only positive integer ≤ 1 is 1, so m = 1.

Case 2: m, n < 0.

Then (−m)(−n) = mn = 1 with −m > 0. By Case 1, −m = 1, so m = −1.

In either case, m = 1 or m = −1. ∎

Theorem 4.3.3 - transitivity of divisibility

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

Starting point: a, b, c integers with a | b and b | c.

To show: a | c, i.e. c = a · (some integer).

Proof.

a | b ⇒	b = ar for some integer r
b | c ⇒	c = bs for some integer s
Substitute:	c = bs = (ar)s = a(rs)
Let k = rs:	c = ak where k is an integer (product of integers)
Therefore	a | c. ■

Theorem 4.3.4 - every n > 1 has a prime divisor

Any integer n > 1 is divisible by a prime number.

Idea of the proof.

- Take any n > 1. If n is prime, we are done - n itself is the prime divisor.
- If n is not prime, $n = r_0 s_0$ with $1 < r_0 < n$. Then $r_0 \mid n$.
- If r_0 is prime, done. Otherwise, $r_0 = r_1 s_1$ with $1 < r_1 < r_0$. By transitivity (4.3.3), $r_1 \mid n$.
- Continue: $n > r_0 > r_1 > r_2 > \ldots$ each strictly smaller, each > 1.
- The sequence cannot decrease forever - it must terminate at a prime r_k, and $r_k \mid n$.

This argument relies on the well-ordering principle: any decreasing sequence of positive integers must terminate.

Counterexamples and divisibility

To disprove a universal divisibility statement, exhibit one pair of integers for which it fails.

Is the following statement true or false?

$\forall$ **integers a, b, if a | b and b | a, then a = b.**

Counterexample. Take $\mathbf{a = 2}$ and $\mathbf{b = -2}$.

a | b : 2 | (−2) because $-2 = 2 \cdot (-1)$. ✓

b | a : (−2) | 2 because $2 = (-2) \cdot (-1)$. ✓

but $a \neq b$: $2 \neq -2$. ✗

Conclusion. The statement is **false.** *(The correct version: if a, b > 0 and a | b and b | a, then a = b.)*

Chapter 4.3

Direct proof and counterexample - divisibility

In this session:

- Part 1: What is divisibility
- Part 2: Proving properties of divisibility
- **Part 3: The unique factorization theorem**

The unique factorization theorem

Unique Factorization Theorem (Fundamental Theorem of Arithmetic)

Every integer n > 1 is either prime, or can be written as a product of prime numbers in a way that is unique except, perhaps, for the order of the factors.

Symbolically:

for any n > 1 there exist a positive integer k, distinct primes $p_1 < p_2 < \ldots < p_k$, and positive integers $e_1, \ldots, e_k$ such that

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

Example. 72 written as a product of primes:

$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \;=\; 2 \cdot 3 \cdot 3 \cdot 2 \cdot 2 \;=\; 3 \cdot 2 \cdot 2 \cdot 3 \cdot 2$

Three 2's and two 3's, in some order - no other multiset of primes multiplies to 72.

First proved precisely by Carl Friedrich Gauss in 1801 (Disquisitiones Arithmeticae).

Standard factored form

Definition

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

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k} \quad \text{with} \quad p_1 < p_2 < \ldots < p_k \ \text{prime.}$$

Example. Write 3,300 in standard factored form.

Step 1. $3{,}300 = 100 \cdot 33$

Step 2. $= 4 \cdot 25 \cdot 3 \cdot 11$

Step 3. $= 2 \cdot 2 \cdot 5 \cdot 5 \cdot 3 \cdot 11$

Step 4. $= 2^2 \cdot 3^1 \cdot 5^2 \cdot 11^1$ **(primes in ascending order)**

In standard factored form, $3{,}300 = 2^2 \cdot 3 \cdot 5^2 \cdot 11$.

Using unique factorization to solve a problem

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 | m ?

Solution.

- 17 is a prime factor of the right-hand side (17 itself appears).
- By the unique factorization theorem, 17 must also appear as a prime factor of the left-hand side.
- Each of 8, 7, 6, 5, 4, 3, 2 is less than 17, so its prime factors are all less than 17.
- Hence none of 2, 3, 4, 5, 6, 7, 8 contributes a factor of 17.
- The only place 17 can appear on the left is in m - so 17 is a prime factor of m.
- **Therefore 17 | m.** ▪

Summary - what we covered

Definition

- $d \mid n \Leftrightarrow \exists$ integer k with $n = dk$ $(d \neq 0)$
- Distinguish $a \mid b$ (sentence) from a/b (number)

Properties (all proved by direct proof)

- T 4.3.1. $a, b > 0 \wedge a \mid b \Rightarrow a \leq b$
- T 4.3.2. Divisors of 1 are exactly ± 1
- T 4.3.3. Transitivity: $a \mid b \wedge b \mid c \Rightarrow a \mid c$
- T 4.3.4. Every $n > 1$ has a prime divisor

Unique factorization (Gauss, 1801)

- Every $n > 1 = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$, unique up to order
- Standard factored form: primes in ascending order

Counterexample reminder

- One pair where a universal claim fails is enough to disprove it
- Always check the quantifier domain (all integers vs positive)

Next lecture

Chapter 4.4

The quotient-remainder theorem

Topics:

- Divide-with-remainder (q and r unique)
- div and mod operators (and applications)
- Parity, integers modulo 4, congruence modulo n
- Proof by division into cases
- Absolute value and the triangle inequality

Read in advance: Epp §4.4 (Examples 4.4.1–4.4.4 and Theorem 4.4.1).