جامعة بيرزيت
BIRZEIT UNIVERSITY

FACULTY OF ENGINEERING AND TECHNOLOGY

COMPUTER SCIENCE DEPARTMENT

COMP233
Discrete Mathematics

CHAPTER 4

Elementary Number Theory and Methods of Proof

Number Theory

- Direct Proof and Counterexamples
- Rational Numbers
- Divisibility
- Division into Cases and the Quotient-Remainder Theorem

Number Theory

- Direct Proof and Counterexamples
- Rational Numbers
- Divisibility
- Division into Cases and the Quotient-Remainder Theorem

Divisibility

- Introduction
- Proving Properties of Divisibility
  - *Positive Divisors of Positive Numbers*
  - *Divisors of 1*
  - *Transitivity of Divisibility*
  - *Divisibility by a Prime*
- Counterexamples and Divisibility
- The Unique Factorization Theorem

Motivation

- When you were first introduced to the concept of division in elementary school, you were probably taught that 12 divided by 3 is 4 because if you separate 12 objects into groups of 3, you get 4 groups with nothing left over.

- The notion of divisibility is the central concept of one of the most beautiful subjects in advanced mathematics: **number theory,** the study of properties of integers.

Divisibility

- Introduction
- Proving Properties of Divisibility
  - *Positive Divisors of Positive Numbers*
  - *Divisors of 1*
  - *Transitivity of Divisibility*
  - *Divisibility by a Prime*
- Counterexamples and Divisibility
- The Unique Factorization Theorem

Definition and Terminology

- 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
  - d ***is a factor of*** n
  - d ***is a divisor of*** n
  - d ***divides*** n.

- The notation $\boldsymbol{d|n}$ is read "d divides n."

- Symbolically, if n and d are integers and $d \neq 0$:

$$d\,|n \leftrightarrow \exists \text{ an integer } k \text{ such that } n = dk$$

Examples

a. Is 21 divisible by 3?

   Yes, $21 = 3 \cdot 7$.

b. Does 5 divide 40?

   Yes, $40 = 5 \cdot 8$.

c. Does $7 \mid 42$?

   Yes, $42 = 7 \cdot 6$.

Examples – cont.

d. Is 32 a multiple of -16?

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

e. Is 6 a factor of 54?

Yes, $54 = 6 \cdot 9$.

f. Is 7 a factor of -7?

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

Divisors of Zero

- If k is any nonzero integer, does k divide 0?
  - *Yes, because* $0 = k \cdot 0$.

Divisibility of Algebraic Expressions

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

Yes. By the distributive law of algebra, $3a + 3b = 3(a + b)$ *and* $a + b$ *is an integer because it is a sum of two integers.*

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

Yes. By the associative law of algebra, $10km = 5 \cdot (2km)$ *and* $2km$ *is an integer because it is the product of three integers.*

Indivisibility

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

Since the negation of an existential statement is universal, it follows that d does not divide n (denoted $d \nmid n$) if, and only if, $\forall$ integers k, $n \neq dk$, or, in other words, the quotient n/d is not an integer.

$$\forall \text{ integers } n \text{ and } d, \qquad d \nmid n \leftrightarrow \frac{n}{d} \text{ is not an integer}$$

Example

- Does $4 \mid 15$?

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

Divisibility and Prime Numbers

- An alternative way to define a prime number is to say that

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

Divisibility

- Introduction
- Proving Properties of Divisibility
  - *Positive Divisors of Positive Numbers*
  - *Divisors of 1*
  - *Transitivity of Divisibility*
  - *Divisibility by a Prime*
- Counterexamples and Divisibility
- The Unique Factorization Theorem

Positive Divisors of Positive Numbers

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

- Suppose a and b are positive integers and a divides b. We must show that $a \leq b$.
- Then there exists an integer k so that $b = ak$, and k must be positive because both a and b are positive. It follows that

$$1 \leq k$$

because every positive integer is greater than or equal to 1.

- Multiplying both sides by a gives

$$a \leq ka = b$$

because multiplying both sides of an inequality by a positive number preserves the inequality.

- Thus, $a \leq b$, which we needed to show.

Divisibility

Divisors of 1

The only divisors of 1 are 1 and -1.

- Since $1 \cdot 1 = 1$ and $(-1)(-1) = 1$, both 1 and -1 are divisors of 1.
- Now suppose m is any integer that divides 1. Then there exists an integer n such that $1 = mn$.
- Either both m and n are positive or both m and n are negative.
- If both m and n are positive, then m is a positive integer divisor of 1. By the theorem we just proved, $m \leq 1$, and, since the only positive integer that is less than or equal to 1 is 1 itself, it follows that $m = 1$.
- On the other hand, if both m and n are negative, then $(-m)(-n) = mn = 1$. In this case $-m$ is a positive integer divisor of 1, and so, by the same reasoning, $-m = 1$ and thus $m = -1$.
- Therefore, there are only two possibilities: either $m = 1$ or $m = -1$. So the only divisors of 1 are 1 and -1.

Divisibility

- Introduction
- Proving Properties of Divisibility
  - *Positive Divisors of Positive Numbers*
  - *Divisors of 1*
  - *Transitivity of Divisibility*
  - *Divisibility by a Prime*
- Counterexamples and Divisibility
- The Unique Factorization Theorem

Transitivity of Divisibility

Prove that for all integers a, b, and c, if $a|b$ and $b|c$, then $a|c$.

- Suppose a, b, and c are particular but arbitrarily chosen integers such that $a|b$ and $b|c$.
- We need to show that $a|c$. In other words, we need to show that

$$c = a \cdot (some\ integer)$$

- But since $a \mid b$, $b = ar$ for some integer r
- And since $b \mid c$, $c = bs$ for some integer s
- By substitution,

$$c = (ar)s = a(rs)$$

- Let $k = rs$. Then k is an integer since it is a product of integers, and therefore $c = ak$ where k is an integer.
- Thus, a divides c by definition of divisibility, and this is what was to be shown.s

Divisibility

- Introduction
- Proving Properties of Divisibility
  - *Positive Divisors of Positive Numbers*
  - *Divisors of 1*
  - *Transitivity of Divisibility*
  - *Divisibility by a Prime*
- Counterexamples and Divisibility
- The Unique Factorization Theorem

Divisibility by a Prime

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

- Suppose n is a particular but arbitrarily chosen integer that is greater than 1.
- We must show that there is a prime number that divides n.

- If n is prime, then n is divisible by a prime number (namely itself), and we are done.

Divisibility by a Prime – cont.

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

- If n is not prime, then,

  $n = r_0 s_0$ where r_0 and s_0 are integers and $1 < r_0 < n$ and $1 < s_0 < n$.

  It follows by definition of divisibility that $r_0 | n$.

- If r_0 is prime, then r_0 is a prime number that divides n, and we are done.

Divisibility by a Prime – cont.

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

- If r_0 is not prime, then

  $r_0 = r_1 s_1$ where r_1 and s_1 are integers and $1 < r_1 < r_0$ and $1 < s_1 < r_0$.

  It follows by definition of divisibility that $r_1 | r_0$.

- But we already know that $r_0 | n$. Consequently, by transitivity of divisibility, $r_1 | n$.

- If r_1 is prime, then r_1 is a prime number that divides n, and we are done.

Divisibility by a Prime – cont.

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

- If r_1 is not prime, then

  $r_1 = r_2 s_2$ where r_2 and s_2 are integers and $1 < r_2 < r_1$ and $1 < s_2 < r_1$.

  It follows by definition of divisibility that $r_2 | r_1$.
- But we already know that $r_1 | n$. Consequently, by transitivity of divisibility, $r_2 | n$.

- If r_2 is prime, then r_2 is a prime number that divides n, and we are done.

Divisibility by a Prime – cont.

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

- If r_2 is not prime, then we may repeat the previous process by factoring r_2 as $r_3 s_3$.
- We may continue in this way, factoring successive factors of n until we find a prime factor. We must succeed in a finite number of steps because each new factor is both less than the previous one (which is less than n) and greater than 1, and there are fewer than n integers strictly between 1 and n.

Divisibility by a Prime – cont.

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

- Thus, we obtain a sequence

$$r_0, r_1, r_2, \ldots, r_k$$

- where $k \geq 0$, $1 < r_k < r_{k-1} < \cdots < r_2 < r_1 < r_0 < n$, and $r_i | n$ for each $i = 0, 1, 2, \ldots, k$. The condition for termination is that r_k should be prime.
- Hence r_k is a prime number that divides n.
- And this is what we were to show.

Divisibility

- Introduction
- Proving Properties of Divisibility
  - *Positive Divisors of Positive Numbers*
  - *Divisors of 1*
  - *Transitivity of Divisibility*
  - *Divisibility by a Prime*
- Counterexamples and Divisibility
- The Unique Factorization Theorem

Counterexamples and Divisibility

- Is the following statement true or false?

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

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

$$a|b \text{ since } 2|(-2)$$

and

$$b|a \text{ since } (-2)|2,$$

but $a \neq b$ since $2 \neq -2$. Therefore, the statement is false.

Divisibility

- Introduction
- Proving Properties of Divisibility
  - *Positive Divisors of Positive Numbers*
  - *Divisors of 1*
  - *Transitivity of Divisibility*
  - *Divisibility by a Prime*
- Counterexamples and Divisibility
- The Unique Factorization Theorem

The Unique Factorization of Integers Theorem

- This theorem is also called the *fundamental theorem of arithmetic.*

- The unique factorization of integers theorem says that any integer greater than 1 either is prime or can be written as a product of prime numbers in a way that is unique except, perhaps, for the order in which the primes are written.

- For example,

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

  and so forth.

- The three 2's and two 3's may be written in any order, but any factorization of 72 as a product of primes must contain exactly three 2's and two 3's.

The Unique Factorization of Integers Theorem

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

Standard Factored Form

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

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

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

Writing Integers in Standard Factored Form

- Write 3,300 in standard factored form.

First find all the factors of 3,300. Then write them in ascending order:

$$
\begin{aligned}
3{,}300 &= 100 \cdot 33 \\
&= 4 \cdot 25 \cdot 3 \cdot 11 \\
&= 2 \cdot 2 \cdot 5 \cdot 5 \cdot 3 \cdot 11 \\
&= 2^2 \cdot 3^1 \cdot 5^2 \cdot 11^1
\end{aligned}
$$

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 $17|m$?

- Since 17 is one of the prime factors of the right-hand side of the equation, it is also a prime factor of the left-hand side (by the unique factorization of integers theorem).
- But 17 does not equal any prime factor of $8, 7, 6, 5, 4, 3$, or 2 (because it is too large).
- Hence 17 must occur as one of the prime factors of m, and so $17|m$.