COMP 233 Discrete Mathematics

Elementary Number Theory and Methods of Proof

4.3 Direct Proof and Counterexample III: Divisibility

Divisibility

Definition: If n and d *are* integers, and $d \neq 0$:

$d \mid n$

d **divides** n

d **is a divisor of** n

d **is a factor of** n

n **is divisible by** d

n **is a multiple of** d

$\Leftrightarrow$

n equals d times some integer

$\exists$ an integer k s.t $n = dk$.

These are different ways to describe the relationship

This is the definition

Notes

Note: $d \mid n \Leftrightarrow \exists$ an integer k such that $n = dk$.

Thus: $d \nmid n \Leftrightarrow \forall$ integers k, $n \neq dk$

$\Leftrightarrow$ n/d is not an integer

Example: Does $5 \mid 12$?

Solution: No: 12/5 is not an integer.

- 5/12 is a **number**: (five-twelfths) $5/12 \cong 0.4167$
- $5 \mid 12$ is a **sentence**: "5 divides 12."

Exercises

1. Is 18 divisible by 6?
2. Does 3 divide 15?
3. Does 5 | 30?
4. Is 32 a multiple of 8?
5. If *k* is any integer, does *k* divide 0?
6. If *m* and *n* are integers, is $10m + 25n$ divisible by 5?

$d \mid n$
d divides *n*
d is a divisor of *n*
d is a factor of *n*
n is divisible by *d*
n is a multiple of *d*

∃ an integer *k* so that $n = dk$.

Exercises

$d \mid n$

d divides n

d is a divisor of n

d is a factor of n

n is divisible by d

n is a multiple of d

$\exists$ an integer k so that $n = dk$.

1. Is 18 divisible by 6?

Answer: Yes, $18 = 6 \cdot 3$.

2. Does 3 divide 15?

Answer: Yes, $15 = 3 \cdot 5$.

3. Does $5 \mid 30$?

Answer: Yes, $30 = 5 \cdot 6$.

4. Is 32 a multiple of 8?

Answer: Yes, $32 = 8 \cdot 4$.

5. If k is any integer, does k divide 0?

Answer: Yes, $0 = k \cdot 0$.

6. If m and n are integers, is $10m + 25n$ divisible by 5?

Answer: Home Work!

Prove/disprove

The "**transitivity of divisibility**" theorem

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

- If a and b are positive integers and $a \mid b$, then $a \leq b$.

Prove: ∀ integers a, b, and c, if a | b and b | c, then a | c.

Write the first sentence (the "starting point") and the last sentence (the "conclusion to be shown") for a proof of the following statement:

∀ integers a, b, and c, if $a | b$ and $b | c$ then $a | c$.

Starting point:

Suppose a, b, and c are any *[p.b.a.c.]* integers such that $a | b$ and $b | c$.

Conclusion to be shown: $a | c$

Proof

Prove: ∀ integers *a*, *b*, and *c*, if *a* | *b* and *b* | *c*, then *a* | *c*.

(Note: The full proof is on page 151)

Starting point for this proof:

Suppose a, b, and c are [pbac – particular but arbitrarily chosen integers] such that a | b and b | c.

Ending point (what must be shown): *a* | *c*.

Since a|b and b|c *then b= as and c = bt* *for some integers s and t.*

*T*o show that a|c, we need to show that c = a·(some integer)

We know that c=bt, then we can substitute the expression for b into the equation for c. Thus, c=ast. s and t are integers, so st is an integer. Let st=k, then c=ak. Therefore a|c by definition.

Proof - Cont.

Proof:

Suppose a, b, and c are *[particular but arbitrarily chosen]* integers such that a divides b and b divides c. *[We must show that a divides c.]* By definition of divisibility,

$$b = ar \quad \text{and} \quad c = bs \quad \text{for some integers } r \text{ and } s.$$

By substitution

$$\begin{aligned} c &= bs \\ &= (ar)s \\ &= a(rs) \quad \text{by basic algebra.} \end{aligned}$$

Let $k = rs$. Then k is an integer since it is a product of integers, and therefore

$$c = ak \quad \text{where } k \text{ is an integer.}$$

Thus a divides c by definition of divisibility. *[This is what was to be shown.]*

■

Theorem: A Positive Divisor of a Positive Integer

If *a* and *b* are positive integers and *a* | *b*, then *a* ≤ *b*.

Proof1:

Let a, b, be [p.b.a.c] integers, s.t. a|b

We need to show that a<=b

b=ak, for some positive integer k

b-a=ak-a=a(k-1)

but k is a positive integer (property T25 - Appendix A)

Thus, k-1 is either 0 or >0

If k-1=0 then b=a. if k-1>0 then b-a>0 => b>a

Thus, b>=a, which is equivalent to a<=b (by definition -Appendix A)

And this is what we needed to show

T25. If $ab > 0$, then both a and b are positive or both are negative.

Theorem: A Positive Divisor of a Positive Integer

If *a* and *b* are positive integers and *a* | *b*, then *a* ≤ *b*.

Proof2:

Let a, b, be [p.b.a.c] integers, s.t. a|b

We need to show that a<=b

b = a.k

Thus 1 ≤ k

a.1 ≤ a.k multiply both sides with a.

Thus a ≤ a.k = b

Thus a ≤ b

QED

Prime and Composite Numbers

Definition:

- An integer n is **prime** if, and only if, $n > 1$ and the only positive **divisors** of n are 1 and n.

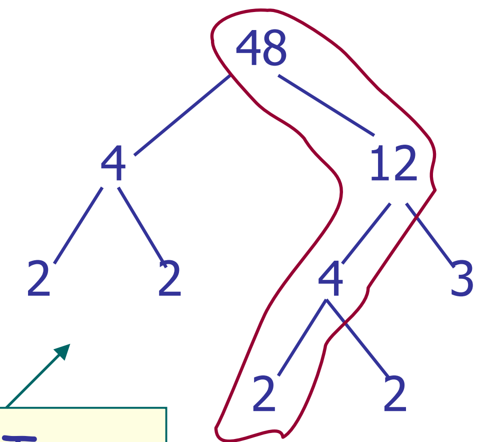
- An integer n is **composite** if, and only if, it is not prime;
  i.e., $n > 1$ and $n = rs$ for some positive integers r and s where neither r nor s is 1.

Note: An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some positive integers r and s where $1 < r < n$ *and* $1 < s < n$.

Divisibility by a Prime

Theorem (Divisibility by a Prime):

Given any integer $n > 1$, there is a prime number p so that $p \mid n$.



Factor Tree

Tracing along any other branch would also lead to a prime.

Given any integer $n > 1$, there is a prime number p so that $p \mid n$.

Idea of Proof: Suppose n is any integer with $n > 1$.

If n is prime, we are done. ← *Why?* $n = n \cdot 1$ so $n \mid n$

If not, $n = rs$, where r and s are integers with

$1 < r < n$ and $1 < s < n$. ← *Why?* def. of composite

If either r or s is prime, we are done. ← *Why?* def. of divisibility

If not, $r = r_1 s_1$, where r_1 and s_1 are integers with

$1 < r_1 < r$ and $1 < s_1 < r$.

If either r_1 *or* s_1 *is prime,* we are done. ← *Why?* transitivity of divisibility theorem

If not, repeat with r_1 in place of r. Etc.

This process must terminate eventually because each successive factor is a positive factor of n and n has only a finite number of factors.

Ref: Sec. 3.3

Counterexamples and Divisibility

Is the following **proposed divisibility property** universally true?

For all integers a and b, if a|b and b|a Then a=b.

Answer: No

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.

Unique Factorization Theorem (*aka** *Fundamental Theorem of Arithmetic*)

أي رقم أكبر من 1 اما ان يكون عدد اولي أو حصل ضرب أعداد أولية

Unique Factorization Theorem for the Integers: Given any integer $n > 1$, either n is prime or n can be written as a product of prime numbers in a way that is unique, except, possibly, for the order in which the numbers are written.

Ex. 1: $500 = 5 \cdot 100 = 5 \cdot 25 \cdot 4 = 5 \cdot 5 \cdot 5 \cdot 2 \cdot 2 = 2 \cdot 5 \cdot 5 \cdot 2 \cdot 5$

$= 2^2 5^3$ ← standard factored form

Ex. 2: $500^3 = (2^2 5^3)^3 = (2^2 5^3)(2^2 5^3)(2^2 5^3) = 2^6 5^9$

**aka: also known as*

Ref: Sec. 3.3

Standard factored form

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

Write 3300 in standard factored form.

First find all the factors of 3300. Then write them in ascending order:

$$3300 = 100 \cdot 33$$
$$= 4 \cdot 25 \cdot 3 \cdot 11$$
$$= 2 \cdot 2 \cdot 5 \cdot 5 \cdot 3 \cdot 11$$
$$= 2^2 \cdot 3^1 \cdot 5^2 \cdot 11^1.$$

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:

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 $17 \mid m$.

Example: using the Unique Factorization to Solve a Problem

Example: Find the smallest positive integer n so that $8! \cdot n$ is a perfect square.

Solution: First, suppose that m is a perfect square. That means $m = s^2$ for some integer s. By the Fundamental Theorem of Arithmetic, there is a positive integer k, primes $p_1, p_2, \ldots, p_k$ and positive integers $e_1, e_2, \ldots e_k$ such that

$$s = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}.$$

Then

$$\begin{aligned} m &= s^2 \\ &= \left[p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}\right]^2 \\ &= p_1^{2e_1} \cdot p_2^{2e_2} \cdot \cdots \cdot p_k^{2e_k}. \end{aligned}$$

The point is, the unique factorization of a perfect square has exponents that are all even numbers.

Example: using the Unique Factorization to Solve a Problem – cont.

$$\begin{aligned} 8! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \\ &= 2 \cdot 3 \cdot 2 \cdot 2 \cdot 5 \cdot 2 \cdot 3 \cdot 7 \cdot 2 \cdot 2 \cdot 2 \\ &= 2^7 \cdot 3^2 \cdot 5^1 \cdot 7^1. \end{aligned}$$

Now, we want $8! \cdot n = 2^7 \cdot 3^2 \cdot 5^1 \cdot 7^1 \cdot n$ to be a perfect square, so the smallest value of n that would do so would be $n = 2 \cdot 5 \cdot 7 = 70$. In that case, $8! \cdot n = 2^8 \cdot 3^2 \cdot 5^2 \cdot 7^2$, which is a perfect square.