

Sections 8.1 and 8.2: Divisibility and primes

CS1231S Discrete Structures

Wong Tin Lok

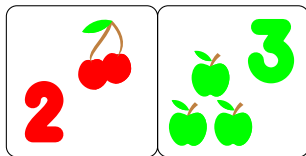
National University of Singapore

1 October 2020

Which of the following should be true?

- ▶ 0 divides 0. ✓
- ▶ 0 divides 1.
- ▶ 1 divides 0. ✓
- ▶ 1 divides 1. ✓
- ▶ 0 is even. ✓
- ▶ 0 is odd.
- ▶ 1 is prime.
- ▶ 1 is composite.

<https://tex.stackexchange.com/a/413506>



Tell me what you think at
<https://pollev.com/wtl/>.

Integers

Why integers?

- ▶ Integers are interesting mathematical objects.
- ▶ Integers arise naturally in life.
- ▶ Arithmetic on the integers is useful in life.

[V]irtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations.

Donald E. Knuth 1974

Our main aim for these two weeks is a proof of the

Fundamental Theorem of Arithmetic

Every positive integer $n \geq 2$ has a unique factorization into a product of prime numbers.

Now

- ▶ divisibility
- ▶ prime numbers

Divisibility

Definition 8.1.1

Let $n, d \in \mathbb{Z}$. Then d is said to **divide** n if

$$n = dk \quad \text{for some } k \in \mathbb{Z}.$$

We write $d \mid n$ for “ d divides n ”, and $d \nmid n$ for “ d does not divide n ”. We also say
 “ n is **divisible** by d ” or “ n is a **multiple** of d ” or “ d is a **factor/divisor** of n ”
 for “ d divides n ”.

Warning 8.1.2

Do not confuse $d \mid n$ with $\frac{d}{n}$ or d/n .

$2 \mid 4$ is a statement,
 while $2/4$ is a number.

Lemma 8.1.5

Let $n, d \in \mathbb{Z}$ with $d \neq 0$. Then $d \mid n$ if and only if $n/d \in \mathbb{Z}$.

Proof of the “only if” direction

1.1. Suppose $d \mid n$.

1.2. Use the definition of divisibility to find $k \in \mathbb{Z}$ such that $n = dk$.

1.3. Then $n/d = k \in \mathbb{Z}$.



Example 8.1.3

(1) $3 \mid 6$ because $6 = 3 \times 2$.

(2) $3 \nmid 7$ because $7 \neq 3k$ for any $k \in \mathbb{Z}$.

Divisibility

Definition 8.1.1

Let $n, d \in \mathbb{Z}$. Then d is said to **divide** n if

$$n = dk \quad \text{for some } k \in \mathbb{Z}.$$

We write $d \mid n$ for “ d divides n ”, and $d \nmid n$ for “ d does not divide n ”. We also say
 “ n is **divisible** by d ” or “ n is a **multiple** of d ” or “ d is a **factor/divisor** of n ”
 for “ d divides n ”.

Warning 8.1.2

Do not confuse $d \mid n$ with $\frac{d}{n}$ or d/n .

2 | 4 is a statement,
 while 2/4 is a number.

Lemma 8.1.5

Let $n, d \in \mathbb{Z}$ with $d \neq 0$. Then $d \mid n$ if and only if $n/d \in \mathbb{Z}$.

Proof of the “if” direction

2.1. Suppose $n/d \in \mathbb{Z}$.

2.2. Then $n = dk$, where $k = n/d$.

2.3. So it follows from the definition of divisibility that $d \mid n$.



Example 8.1.3

(1) $3 \mid 6$ because $6 = 3 \times 2$.

(2) $3 \nmid 7$ because $7 \neq 3k$ for any $k \in \mathbb{Z}$.

Zero and one

Definition 8.1.1

Let $n, d \in \mathbb{Z}$. Then d is said to *divide* n if
$$n = dk \quad \text{for some } k \in \mathbb{Z}.$$

We write $d \mid n$ for “ d divides n ”, and $d \nmid n$ for “ d does not divide n ”. We also say
“ n is *divisible* by d ” or “ n is a *multiple* of d ” or “ d is a *factor/divisor* of n ”
for “ d divides n ”.

Example 8.1.6

Let $n \in \mathbb{Z}$. Then $1 \mid n$ and $n \mid n$ because $1 \times n = n = n \times 1$.

Example 8.1.7

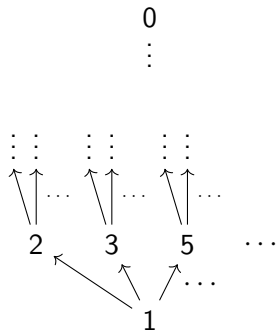
Let $d \in \mathbb{Z}$. Then $d \mid 0$ because $0 = d \times 0$.

Exercise 8.1.8

Which $n \in \mathbb{Z}$ makes $0 \mid n$?

Example 8.1.3

- (1) $3 \mid 6$ because $6 = 3 \times 2$.
- (2) $3 \nmid 7$ because $7 \neq 3k$ for any $k \in \mathbb{Z}$.



Negatives

Definition 8.1.1

Let $n, d \in \mathbb{Z}$. Then d is said to *divide* n if

$$n = dk \quad \text{for some } k \in \mathbb{Z}.$$

We write $d \mid n$ for “ d divides n ”, and $d \nmid n$ for “ d does not divide n ”. We also say

“ n is *divisible* by d ” or “ n is a *multiple* of d ” or “ d is a *factor/divisor* of n ” for “ d divides n ”.

Lemma 8.1.9

Let $d, n \in \mathbb{Z}$. If $d \mid n$, then $-d \mid n$ and $d \mid -n$ and $-d \mid -n$.

Proof

1. Use the definition of divisibility to find $k \in \mathbb{Z}$ such that $n = dk$.
2. Then

$$n = (-d)(-k) \quad \text{and} \quad -n = d(-k) \quad \text{and} \quad -n = (-d)k,$$

where $-k, k \in \mathbb{Z}$.

3. Hence $-d \mid n$ and $d \mid -n$ and $-d \mid -n$ by the definition of divisibility.



How large are the divisors?

Definition 8.1.1

Let $n, d \in \mathbb{Z}$. Then d is said to **divide** n if

$$n = dk \quad \text{for some } k \in \mathbb{Z}.$$

We write $d \mid n$ for “ d divides n ”, and $d \nmid n$ for “ d does not divide n ”. We also say

“ n is **divisible** by d ” or “ n is a **multiple** of d ” or “ d is a **factor/divisor** of n ”

for “ d divides n ”.

Proposition 8.1.10

because $\frac{n}{d}$ then d cannot be bigger if not it will be a real number

Let $d, n \in \mathbb{Z}$. If $d \mid n$ and $n \neq 0$, then $|d| \leq |n|$.

Proof

1. Since $d \mid n$, we know $|d| \mid |n|$ by Lemma 8.1.9.
2. Use this fact to find $k \in \mathbb{Z}$ such that $|n| = |d|k$.
3. Now $n \neq 0$ implies $|n| > 0$ and thus also $|d| > 0$.
4. So $k > 0$ too as $|n| = |d|k$.
5. Since $k \in \mathbb{Z}$, we deduce that $k \geq 1$.
6. Hence $|n| = |d|k \geq |d| \times 1 = |d|$.

Example 8.1.11

The only positive divisors of 6 are 1, 2, 3, 6.

Lemma 8.1.9

Let $d, n \in \mathbb{Z}$. If $d \mid n$, then $-d \mid n$ and $d \mid -n$ and $-d \mid -n$.



Transitivity

Definition 8.1.1

Let $n, d \in \mathbb{Z}$. Then d is said to *divide* n if

$$n = dk \quad \text{for some } k \in \mathbb{Z}.$$

We write $d \mid n$ for “ d divides n ”, and $d \nmid n$ for “ d does not divide n ”. We also say

“ n is *divisible* by d ” or “ n is a *multiple* of d ” or “ d is a *factor/divisor* of n ” for “ d divides n ”.

Theorem 8.1.12 (Transitivity of divisibility)

Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof

1. Assume $a \mid b$ and $b \mid c$.
2. Use the definition of divisibility to find $k, \ell \in \mathbb{Z}$ such that $b = ak$ and $c = b\ell$.
3. Then $c = b\ell = (ak)\ell = a(k\ell)$, where $k\ell \in \mathbb{Z}$.
4. Thus $a \mid c$ by the definition of divisibility.



Example 8.1.13

Since $3 \mid 6$ and $6 \mid 18$, the transitivity of divisibility tells us $3 \mid 18$.

Integer linear combinations

Definition 8.1.1

Let $n, d \in \mathbb{Z}$. Then d is said to *divide* n if
$$n = dk \quad \text{for some } k \in \mathbb{Z}.$$

We write $d \mid n$ for “ d divides n ”, and $d \nmid n$ for “ d does not divide n ”. We also say
“ n is *divisible* by d ” or “ n is a *multiple* of d ” or “ d is a *factor/divisor* of n ”
for “ d divides n ”.

Lemma 8.1.14 (Closure Lemma (non-standard name))

Let $a, b, d, m, n \in \mathbb{Z}$. If $d \mid m$ and $d \mid n$, then $d \mid am + bn$.

*integer linear
combination
of m and n*

Proof

1. Use the definition of divisibility to find $k, \ell \in \mathbb{Z}$ such that $m = dk$ and $n = d\ell$.
2. Then $am + bn = a(dk) + b(d\ell)$ by the choices of k and ℓ ;
3. $= d(ak + b\ell)$, where $ak + b\ell \in \mathbb{Z}$.
4. Thus $d \mid am + bn$ by the definition of divisibility.



Example 8.1.15

Since $3 \mid -6$ and $3 \mid 9$ and
 $-564 = 100 \times -6 + 4 \times 9$, the Closure
Lemma tells us $3 \mid -564$.

The Division Theorem

Theorem 8.1.16 (Division Theorem)

For all $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there exist unique $q, r \in \mathbb{Z}$ such that

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

Definition 8.1.17

Let $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. The unique $q, r \in \mathbb{Z}$ given by the Division Theorem such that $(*)$ holds are called the *quotient* and the *remainder* when n is divided by d , and are denoted $n \underline{\text{div}} d$ and $n \underline{\text{mod}} d$ respectively.

Warning 8.1.18

Some programming languages define their $n \underline{\text{mod}} d$ to have the same sign as n or d . Our $n \underline{\text{mod}} d$ is *always non-negative*.

Example 8.1.19

- (1) $11 \underline{\text{div}} 5 = 2$ and $11 \underline{\text{mod}} 5 = 1$ because $11 = 5 \times 2 + 1$ and $0 \leq 1 < 5$.
- (2) $-16 \underline{\text{div}} 3 = -6$ and $-16 \underline{\text{mod}} 3 = 2$ because $-16 = 3 \times -6 + 2$ and $0 \leq 2 < 3$.

The Division Theorem

Theorem 8.1.16 (Division Theorem) $\exists!$

For all $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there exist unique $q, r \in \mathbb{Z}$ such that

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

Proof

1. Let $q = \lfloor n/d \rfloor$ and $r = n - dq$.

2. (Existence)

2.1. Note that $q, r \in \mathbb{Z}$ and $n = dq + r$.

2.2. Also $q \leq n/d < q + 1$

2.3. $\therefore dq \leq n < d(q + 1)$

2.4. $\therefore dq - dq \leq n - dq < d(q + 1) - dq$ subtracting dq throughout;

2.5. $\therefore 0 \leq r < d$ by the definition of r .

3. (Uniqueness) ...

Exercise 6.1.11(1). $\lfloor x \rfloor$ is the unique $y \in \mathbb{Z}$ such that $y \leq x < y + 1$.

by the Exercise 6.1.11(1);
multiplying by d throughout;
subtracting dq throughout;
by the definition of r .

The Division Theorem

Note 8.1.20

The proof tells us $n \text{ div } d = \lfloor n/d \rfloor$.

Theorem 8.1.16 (Division Theorem)

For all $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there exist unique $q, r \in \mathbb{Z}$ such that

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

Proof

1. Let $q = \lfloor n/d \rfloor$ and $r = n - dq$.
2. (Existence) ...
3. (Uniqueness)

Exercise 6.1.11(1). $\lfloor x \rfloor$ is the unique $y \in \mathbb{Z}$ such that $y \leq x < y + 1$.

- 3.1. Suppose $q', r' \in \mathbb{Z}$ such that $n = dq' + r'$ and $0 \leq r' < d$.
- 3.2. Then $0 \leq n - dq' < d$ by the choice of q' and r' ;
- 3.3. $\therefore 0 \leq \frac{n}{d} - q' < 1$ dividing by d throughout;
- 3.4. $\therefore q' \leq \frac{n}{d} < q' + 1$ adding q' throughout;
- 3.5. $\therefore q' = \lfloor \frac{n}{d} \rfloor$ by Exercise 6.1.11(1).
- 3.6. Thus $q' = q$.
- 3.7. By the choice of r' , this implies $r' = n - dq' = n - dq = r$. □

Even and odd numbers

Theorem 8.1.16 (Division Theorem)

For all $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there exist unique $q, r \in \mathbb{Z}$ such that

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

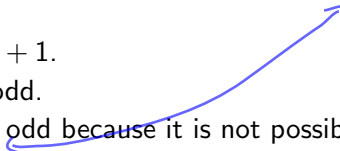
Definition 8.1.21

- (1) An integer is **even** if it is equal to $2k$ for some $k \in \mathbb{Z}$.
- (2) An integer is **odd** if it is equal to $2k + 1$ for some $k \in \mathbb{Z}$.

Corollary 8.1.22

Let $n \in \mathbb{Z}$. Then n is either even or odd, but not both.

Proof

- 1. Use the Division Theorem to find $q, r \in \mathbb{Z}$ such that $n = 2q + r$ and $0 \leq r < 2$.
 - 2. Either $r = 0$ or $r = 1$.
 - 3. So either $n = 2q$ or $n = 2q + 1$.
 - 4. So either n is even or n is odd.
 - 5. n cannot be both even and odd because it is not possible to have $k, k' \in \mathbb{Z}$ such that $2k + 0 = n = 2k' + 1$ by the uniqueness part of the Division Theorem. □
- 

Prime and composite numbers

Example 8.1.6. $1 \mid n$ and $n \mid n$ for all $n \in \mathbb{Z}$.

Definition 8.2.1

- (1) A positive integer is *prime* if it has exactly two positive divisors. $x = yz$ ($y=1 \wedge x=z$)
- (2) A positive integer is *composite* if it has (strictly) more than two positive divisors.

Remark 8.2.2

- (1) 1 is neither prime nor composite because it has exactly one positive divisor.
- (2) Every integer $n \geq 2$ is either prime or composite.

Example 8.2.3

- (1) 7 is prime because its positive divisors are 1, 7.
- (2) 9 is composite because its positive divisors are 1, 3, 9.

Definition 8.1.1.

$d \mid n \iff d$ is a divisor of n
 $\iff n = dk$ for some $k \in \mathbb{Z}$.

Divisors of composite numbers

Example 8.1.6. $1 \mid n$ and $n \mid n$ for all $n \in \mathbb{Z}$.

Definition 8.2.1

- (1) A positive integer is *prime* if it has exactly two positive divisors.
- (2) A positive integer is *composite* if it has (strictly) more than two positive divisors.

Lemma 8.2.4

An integer n is composite if and only if n has a divisor d such that $1 < d < n$.

Proof

1. ("If")

- 1.1. Let d be a divisor of n such that $1 < d < n$.
- 1.2. Then $1, d, n$ are three (distinct) divisors of n .
- 1.3. So n is composite.

2. ("Only if")

- 2.1. Suppose n is composite.
- 2.2. Then n has a positive divisor, say d , such that $1 \neq d \neq n$.
- 2.3. Now $d \mid n$ implies $d = |d| \leq |n| = n$ by Proposition 8.1.10.
- 2.4. So $1 < d < n$.

Definition 8.1.1.

$d \mid n \iff d$ is a divisor of n
 $\iff n = dk$ for some $k \in \mathbb{Z}$.

Proposition 8.1.10. Let $d, n \in \mathbb{Z}$.
If $d \mid n$ and $n \neq 0$, then $|d| \leq |n|$.




Existence of prime divisors

Lemma 8.2.5 (Prime Divisor Lemma (non-standard name))

Let $n \in \mathbb{Z}_{\geq 2}$. Then n has a prime divisor.

Proof

1. Note that n has a positive divisor strictly bigger than 1, say n .
2. Use the Well-Ordering Principle to find the smallest such divisor d of n .
3. We prove that d is prime by contradiction.
 - 3.1. Suppose d is not prime.
 - 3.2. Then d is composite by Remark 8.2.2(2). 
 - 3.3. Then d has a divisor, say c , such that $1 < c < d$, by Lemma 8.2.4.
 - 3.4. Now $c \mid d$ and $d \mid n$. So $c \mid n$ by the transitivity of divisibility.
 - 3.5. This contradicts the assumption that d is the smallest positive divisor d of n strictly bigger than 1.

Lemma 8.2.4. An integer n is composite iff n has a divisor such that $1 < d < n$.

Every integer $n \geq 2$ is either prime or composite.

Theorem 7.2.9 (Well-Ordering Principle). Every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.

Proposition 8.1.12 (transitivity of divisibility). Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

□

Sizes of prime divisors (1/2)

Lemma 8.2.5 (Prime Divisor Lemma (non-standard name))

Let $n \in \mathbb{Z}_{\geq 2}$. Then n has a prime divisor.

Proposition 8.2.6

Let n be a composite positive integer. Then n has a prime divisor $p \leq \sqrt{n}$.

Proof

1. Use Lemma 8.2.4 to find $d \mid n$ such that $1 < d < n$.
2. Use the definition of divisibility to find $k \in \mathbb{Z}$ such that $n = dk$.
3. Case 1: suppose $d \leq \sqrt{n}$.
 - 3.1. Use the Prime Divisor Lemma to find a prime $p \mid d$.
 - 3.2. Since $p \mid d$ and $d \mid n$, the transitivity of divisibility implies $p \mid n$.
 - 3.3. As $p \mid d$, we know $p = |p| \leq |d| = d \leq \sqrt{n}$ by Proposition 8.1.10.
4. Case 2: suppose $d > \sqrt{n}$

Proposition 8.1.10. Let $d, n \in \mathbb{Z}$.
If $d \mid n$ and $n \neq 0$, then $|d| \leq |n|$.

Lemma 8.2.4. An integer n is composite iff n has a divisor such that $1 < d < n$.

Example 8.2.7. The primes less than $\sqrt{101}$ are 2, 3, 5, 7, none of which divides 101. So 101 is prime.

Proposition 8.1.12 (transitivity of divisibility). Let $a, b, c \in \mathbb{Z}$.
If $a \mid b$ and $b \mid c$, then $a \mid c$.

Sizes of prime divisors (2/2)

Lemma 8.2.5 (Prime Divisor Lemma (non-standard name))

Let $n \in \mathbb{Z}_{\geq 2}$. Then n has a prime divisor.

Proposition 8.2.6

Let n be a composite positive integer. Then n has a prime divisor $p \leq \sqrt{n}$.

Proof

1. Use Lemma 8.2.4 to find $d \mid n$ such that $1 < d < n$.
2. Use the definition of divisibility to find $k \in \mathbb{Z}$ such that $n = dk$.
3. **Case 1:** suppose $d \leq \sqrt{n}$
4. **Case 2:** suppose $d > \sqrt{n}$.
 - 4.1. Note $k = n/d > n/n = 1$ as $d < n$.
 - 4.2. So $k \geq 2$ as $k \in \mathbb{Z}$.
 - 4.3. Use the Prime Divisor Lemma to find a prime $p \mid k$.
 - 4.4. Since $p \mid k$ and $k \mid n$, the transitivity of divisibility implies $p \mid n$.
 - 4.5. As $p \mid k$ and $d > \sqrt{n}$, we have $p = |p| \leq |k| = k = n/d < n/\sqrt{n} = \sqrt{n}$ by Proposition 8.1.10.

Lemma 8.2.4. An integer n is composite iff n has a divisor such that $1 < d < n$.

Example 8.2.7. The primes less than $\sqrt{101}$ are 2, 3, 5, 7, none of which divides 101. So 101 is prime.



The infinitude of primes

Theorem 8.2.8 (Euclid)

There are infinitely many prime numbers.

Proof

1. Suppose the theorem is false.
2. Let p_1, p_2, \dots, p_k be a complete (finite) list of primes.
3. Define $n = p_1 p_2 \dots p_k + 1$. Note that $n \geq 1 + 1 = 2$. using a minimal hypothesis to use the Prime Divisor Lemma since needs to be 2 to be a prime divisor
4. Use the Prime Divisor Lemma to find a prime divisor of n say p .
5. Use the hypothesis that p_1, p_2, \dots, p_k is a complete list of primes to find $i \in \{1, 2, \dots, k\}$ such that $p = p_i$.
6. As $p_1 p_2 \dots p_k / p_i \in \mathbb{Z}$, the definition of divisibility tells us that $p_i \mid p_1 p_2 \dots p_k$. using the closure lemma
7. So $p_i \mid (n - p_1 p_2 \dots p_k)$ by the Closure Lemma, as $p_i \mid n$.
8. Thus $p_i \mid 1$ by the definition of n .
9. Proposition 8.1.10 then implies $2 \leq p_i = |p_i| \leq |1| = 1$, which is a contradiction. \square

Let $d, n \in \mathbb{Z}$. If $d \mid n$ and $n \neq 0$, then $|d| \leq |n|$.

Lemma 8.2.5 (Prime Divisor Lemma). Every $n \in \mathbb{Z}_{\geq 2}$ has a prime divisor.

Lemma 8.1.14 (Closure Lemma). Let $a, b, d, m, n \in \mathbb{Z}$. If $d \mid m$ and $d \mid n$, then $d \mid am + bn$.

Summary

What we saw

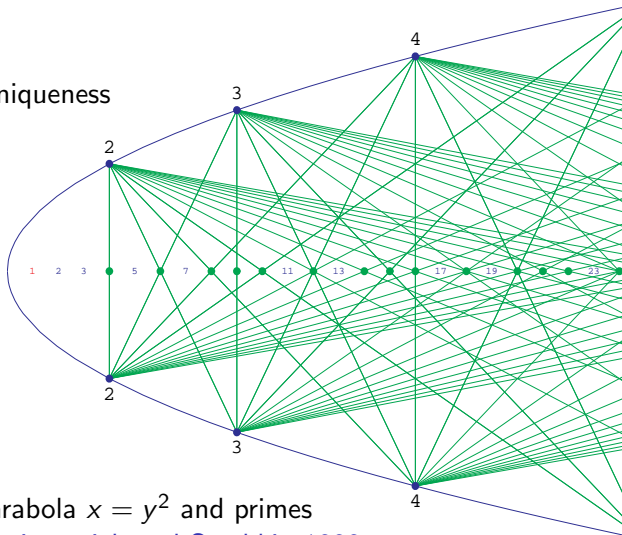
- ▶ divisibility and primes
- ▶ division theorem: the existence and uniqueness of quotient and remainder in division
- ▶ There are infinitely many primes.

The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic.

Gauss 1870

Next

- ▶ base- b representations



Parabola $x = y^2$ and primes

Matiyasevich and Stechkin 1999