Math 365 Lecture Notes for Chapter 4 Integers and Number Theory

Text 4.1 Integers and the Operations of Addition and Subtraction

Where are negative numbers used?

The **integers** are Z = {. . . , –5, –4, –3, –2, –1, 0, 1, 2, 3, 4, 5, . . . }

Negative integers are **additive inverses** (opposites) of the positive integers, also known as the natural numbers, and vice versa.

If x is an integer, what is the sign of –x?

Integer Addition

1. Chip Model (need key)

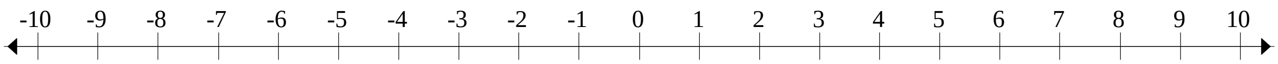
2. Charged Field Model

3. Patterns

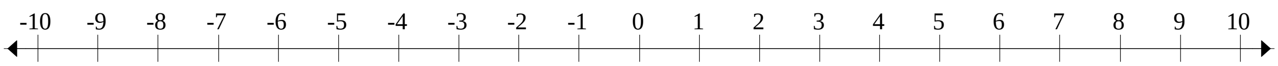
4. Number-Line Model

- Start at zero facing the positive direction
- Add means stay facing the same direction
- Subtract means turn around
- Positive number means go forwards
- Negative number means go backwards]

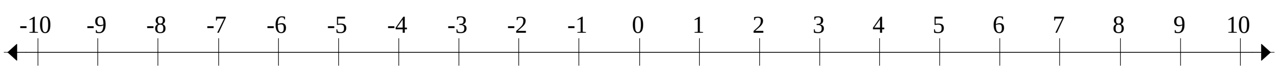
2 + 4

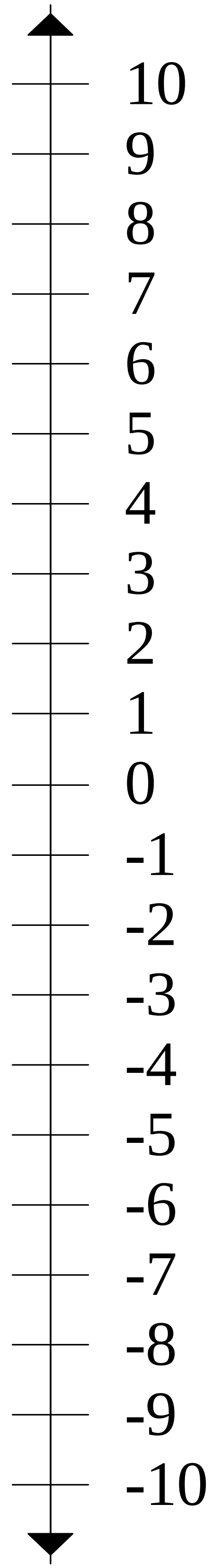


–3 + 7



$5 + {}^{-}8$



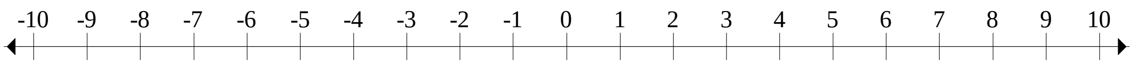

10
9
8
7
6
5
4
3
2
1
0
-1
-2
-3
-4
-5
-6
-7
-8
-9
-10

Absolute value is the distance (always nonnegative) between points.

$$|x| = \begin{cases} x \text{ if } x \geq 0 \\ -x \text{ if } x < 0 \end{cases}$$

| 5| =

| –3 | =



| 0 | =

| x – 4 | =

Integer Properties: $a, b, c \in Z$

Closure Property of Addition of Integers: a + b is a unique integer
Commutative Property of Addition of Integers: a + b = b + a
Associative Property of Addition of Integers: (a + b) + c = a + (b + c)
Identity Element of Addition of Integers: 0 is the unique integer such that, for all integers a, 0 + a = a = a + 0
Uniqueness Property of Additive Inverse: For every integer a, there exists a unique integer –a, the additive inverse of a, such that a + $^{-}$a = 0 = –a + a.

Properties of the Additive Inverse: For any integers, a and b,
1. –(–a) = a
2. –a + $^{-}$b = –(a + b)

The additive inverse of –5 is

The additive inverse of –(13 + y) is

The additive inverse of x + y is

Integer Subtraction

1. Chip Model (need key):

   a. $5 - {}^{-}3$

   b. $4 - 2$

   c. $-2 - 3$

   d. $-1 - {}^{-}4$

2. Charged-Field Model: $-5 - {}^{-}2$

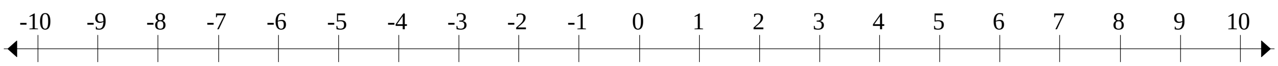
3. Patterns

4. Number-Line Model

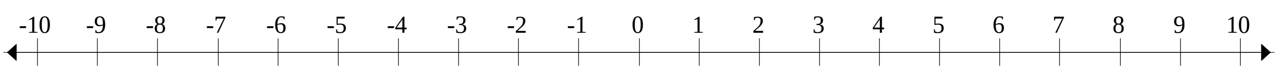
Start at zero facing the positive direction

- Add means stay facing the same direction
- Subtract means turn around
- Positive number means go forwards
- Negative number means go backwards]

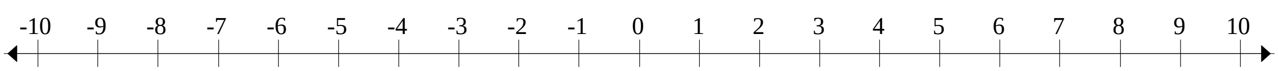
2 – 4



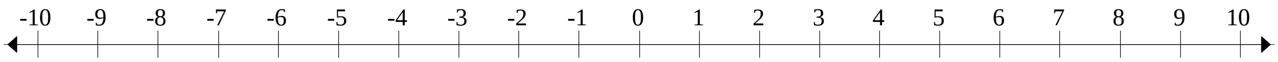
–3 – 7



$5 - {}^{-}4$



–3 – $^{-}7$



Subtraction definition: For integers a and b, a – b is the unique integer n such that a = b + n.

Thus subtraction is defined in terms of ________________________.

Use the definition of subtraction to compute 5 – 13.

Property: For all integers a and b, a – b = a + $^{-}$b.

Use the property to compute 6 – $^{-}2$.

Simplify, step by step: x – (3 – y)

Formal Justification

$$57 - 36 = (5 * 10 + 7 * 1) - (3 * 10 + 6 * 1)$$

$$= (5 * 10 + 7 * 1) + {}^{-}(3 * 10 + 6 * 1)$$

$$= (5 * 10 + 7 * 1) + ({}^{-}3 * 10 + {}^{-}6 * 1)$$

$$= (5 * 10 + {}^{-}3 * 10) + (7 * 1 + {}^{-}6 * 1)$$

$$= (5 + {}^{-}3) * 10 + (7 + {}^{-}6) * 1$$

$$= 2 * 10 + 1 * 1$$

$$= 21$$

Text 4.2 Multiplication and Division of Integers

A running back lost four yards of each of three carries in a football game.

We want the commutative property of multiplication to hold for all integers.

1. Patterns Model: –4 * 3

2. Chip Model (need key):

   a. 2 * –4

   b. –2 * –4

3. Charged-Field Model

   a. 3 * –2

   b. –3 * –2

4. Number-Line Model

- Traveling left (west) means moving in a negative direction
- Traveling right (east) means moving in a positive direction
- Time in the future is denoted by a positive value
- Time in the past is denoted by a negative value

If you are now at 0, moving west at 35 km per hour, where were you 2 hours ago?

Properties: For *whole numbers*, a and b,

1. (–a) (–b) = ab
2. (–a)(b) = b(–a) = –(ab)

Properties of Integer Multiplication

$a,b,c \in Z$

Closure Property of Multiplication of Integers: ab is a unique integer
Commutative Property of Multiplication of Integers: ab = ba
Associative Property of Multiplication of Integers: (ab)c = a(bc)
Multiplicative Identity: 1 is the unique integer such that, for all integers a,
1 * a = a = a * 1
Distributive Property of Multiplication over Addition for Integers:
a(b + c) = ab + ac and (b + c)a = ba + ca
Zero Multiplication Property: 0 is the unique integer such that for all integers a,
a * 0 = 0 = 0 * a

Show (–4)(3) = –(4 * 3).

***** ***Why is a negative integer times a negative integer a positive integer?***

Property: For every integer a, (–1)a = –a.

Note: If a = –1, then (–1)a = –a becomes –1(–1) = –(–1) = 1

For integers a and b,

(–a)(–b) = [(–1)a][(–1)b]

=(–1) (–1)ab

= 1ab

= ab

Therefore (–a)(–b) = ab.

In particular, if a, b $\in$ N $\subset$ Z, then (–a) and (–b) are negative integers. Now ab $\in$ N since multiplication of the natural numbers is closed. So (–a)(–b) = ab shows the product of two negative integers is a positive integer. [Actually (–a)(–b) = ab shows much more.]

For integers a and b,

(–a)(b) = [(–1)a]b

=(–1)(ab)

= –ab

In particular, if a, b $\in$ N $\subset$ Z, then (–a) is a negative integer and b is a positive integer. Now ab $\in$ N since multiplication of the natural numbers is closed. Thus –ab is a negative integer. So (–a)(b) = –ab shows the product of a negative integer and a positive integer is a negative integer. [Actually (–a)(b) = –ab shows much more.]

For integers a and b,

$(a)(-b) =$

Properties: For all *integers* a and b,

1. $(-a)b = -(ab)$
2. $(-a)(-b) = ab$

Distributive Property of Multiplication over Subtraction of Integers:
For any integers a, b, and c,
$a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.

$-5(3x - 6) =$

$(x + y)(x - y) =$

Difference of Squares: $(x + y)(x - y) = x^2 - y^2$

$(-3 + a)(-3 - a) =$

Factor $12z^2 - 75$.

Definition of Integer Division
If a and b are integers, with $b \neq 0$, then $a \div b$ is the unique integer c, if it exists, such that a = bc.

$26 \div -2 =$

$-24 \div -8 =$

$-20 \div 17 =$

Division Algorithm

Definition of Less Than for Integers
For any integers a and b, a is less than b, $a < b$, iff there exists a *positive* integer k such that $a + k = b$.

Using the definition of less than, prove $-5 < -3$.

Property: $a < b$ (or equivalently, $b > a$) iff $b - a > 0$.

Order of Operations
When addition, subtraction, multiplication, division, and exponents appear *without parenthesis*, first exponentiate, then multiply and divide in order of appearance from left to right, and then add and subtract in order of appearance from left to right.

$8^2 - 5 + 24 \div 8 \cdot 2 =$

Text 4.3 Divisibility

Definition: If a and b are any integers, then b divides a, written **b | a**, iff there is a unique integer c such that a = bc.

If b **|** a, then b is a **factor** or **divisor** of a, and a is a **multiple** of b.

8 **|** 16

$3 \nmid 14$

Theorem: For any integers a and d, if d **|** a and n is any integer, then d **|** na.

5 **|** 15

Theorem: For any integers a, b, and c

a. If $d \mid a$ and $d \mid b$, then $d \mid (a + b)$
b. If $d \mid a$ and $d \nmid b$, then $d \nmid (a + b)$
c. If $d \mid a$ and $d \mid b$, then $d \mid (a – b)$
d. If $d \mid a$ and $d \nmid b$, then $d \nmid (a – b)$

Examples:

Divisibility Test for 2

Divisibility Test for 5

Divisibility Test for 10

Divisibility Test for 4

Divisibility Test for 8

Divisibility Test for 3

Divisibility Test for 9

Divisibility Test for 11: An integer is divisible by 11 iff the sum of the digits in the places that are even powers of 10 minus the sum of the digits in the places that are odd powers of 10 is divisible by 11.

Divisibility Test for 6

Text 4.4 Prime and Composite Numbers

Positive Divisors - Rectangle Method

The positive divisors of 16 are

The positive divisors of 5 are

Number of Positive Factors

1	2	3	4	5	6	7	8	9
1	2	4	6	16	12		24	36
	3	9	8		18		30	
	5	25	10		20			
	7		14		28			
	11		15		32			
	13		21					
	17		22					
	19		26					
	23		27					
	29		33					
	31		34					
	37		35					

What are some patterns forming in the above table?

What other entries will be in 1 column?

What are the next three numbers in 3 column?

Find an entry for 7 column.

What kinds of numbers have an odd number of positive factors and why?

Definition: Any positive integer with exactly two distinct, positive divisors is a **prime** number.

Example:

Definition: Any integer greater than 1 that has a positive factor other than 1 and itself is a **composite** number.

Example:

The number 1 is the multiplicative identity and is neither prime nor composite.

Expressing a whole number as a product of factors is **factorization**.

Example:

A factorization containing only prime factors is **prime factorization**.

Example:

Prime Factorization Using the Divisibility Rules (downward stair-step)

756

Prime Factorization Using Factor Tree

756

Fundamental Theorem of Arithmetic: Each composite number can be written as a product of primes in one, and only one, way except for the order of the prime factors in the product.

Number of Divisors: If p is any prime and n is any natural number, then the positive divisors of p^n are $p^0, p^1, p^2, \ldots, p^n$. Thus there are n + 1 positive divisors of p^n.

What are the positive divisors of 125?

Using the *Fundamental Counting Principle*, if p and q are different primes, then $p^m q^n$ will have (m + 1) (n + 1) positive divisors.

How many positive divisors does 12 have?

The positive divisors of 12 are D_{12} =

How many positive divisors does 750,000 = $2^5 \cdot 3 \cdot 5^7$ have?

How many positive divisors does $(550)^{20}$ have?

Theorem: If d is a divisor of n, then $\frac{n}{d}$ is also a divisor of n.

Theorem: If n is composite, the n has a prime factor p such than $p^2 \le n$.

Theorem: If n is an integer greater than 1, and not divisible by any prime p, such that $p^2 \le n$, then n is prime.

Note: $p^2 \le n$ implies $p \le \sqrt{n}$. To determine if n is prime, it is enough to check if any prime less than or equal to $\sqrt{n}$ is a divisor of n.

Is 547 prime?

Is 149 prime?

Is 133 prime?

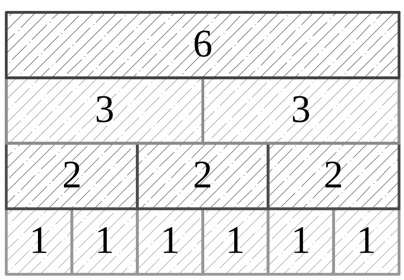
Sieve of Eratosthenes: If all the natural numbers greater than one are considered (or placed in a sieve), the numbers that are not prime are methodically crossed out (or drop through the holes of the sieve). The remaining numbers are prime.

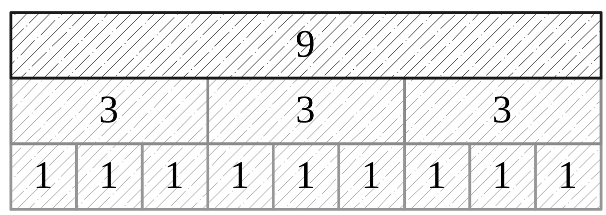
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	. . . . .

Text 4.5 Greatest Common Divisor and Least Common Multiple

The **greatest common divisor**, **GCD** or **gcd**, of two numbers a and b is the greatest integer than divides both a and b.

1. Colored Rods Model – To find gcd (6, 9) we must find the longest such rod that we can use multiples of that rod to build both the 6-rod and the 9-rod.





gcd (6, 9) =

2. Intersection-of-Sets Method – List all elements of the set of positive divisors of each of the integers that you want to find the gcd of, then find the set of all "common divisors," and then pick the greatest element from the common divisor set.

Find the gcd of 30 and 105.

3. Prime Factorization Method – To find the gcd of two or more positive integers, first find the prime factorizations of each number and then identify the common prime factor(s) of the given numbers. The gcd is the product of the common factors, each raised to the lowest power of that prime that occurs in any of the prime factorizations.

gcd (1260, 1568) =

When the gcd of two numbers is 1, the numbers are **relatively prime**. They have no common positive integer factors other than 1.

4. Calculator Method – on the TI-83 graphing calculator you can either go to the catalog and scroll down to *gcd* or you can go to *math, num, gcd*.

   gcd (1260, 1568) =

5. Euclidean Algorithm Method – ***Theorem***: If a and b are any natural numbers and $a \geq b$, then gcd (a, b) = gcd (r, b), where r is the remainder when a is divided by b.

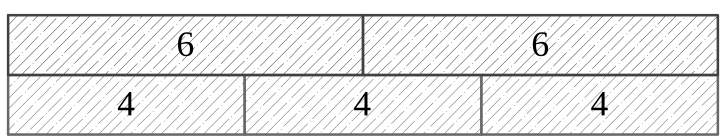
   Explanation: From ***Theorem, part c***: For any integers a, b, and c, if d **|** a and d **|** b, then d **|** (a – b). If we are finding the gcd of 13167 and 1520, then every divisor of 13167 and 1520 is also a divisor of 13167 – 1520. Thus the set of all common divisors of 13167 and 1520 is the same as the set of all common divisors of (13167 – 1520) and 1520.
   $\therefore$ gcd (13167, 1520) = gcd (13167 – 1520, 1520)
   Now continue this process until the remainder zero is reached; this is known as the **Euclidean Algorithm**.

Use the Euclidean Algorithm to find gcd (13167, 1520).

The **least common multiple**, **lcm** or **LCM**, of natural numbers a and b is the least positive integer that is simultaneously a multiple of a and a multiple of b.

1. Colored-Rods Method – build trains of each colored rod until the length of one train equals the other.

lcm (4, 6) =



2. Intersection-of-Sets Method – Find the set of all positive multiples of all numbers, then find the set of all common multiples, and then find the least common multiple

lcm (4, 6) =

3. Prime Factorization Method – Take each of the primes that are factors of any of the given numbers. The least common multiple is the product of these primes, each raised to the greatest power of the prime that occurs in any of the prime factorization.

lcm (520, 1572) =

4. Euclidean Algorithm and Theorem –

Theorem: For any two natural numbers a and b, $\gcd(a,b)\cdot lcm(a,b)=ab$.

lcm (520, 1572) =

6. Calculator - On the TI-83 graphing calculator you can either go to the catalog and scroll down to *lcm* or you can go to *math, num, lcm*.

5. Division by Primes – stop process when all numbers are relatively prime (or when have a row of ones)

lcm (280, 1210, 21) =

Text 4.6 Clock and Modular Arithmetic

For integers a and b, **a is congruent to b modulo m**, written $a \equiv b(\text{mod} \quad m)$, iff a – b is a multiple of m, where m is a natural number.

Where is 10 + 5 = 3?

$8 \oplus 6 \equiv$ (mod 12) or equivalently 8 + 6 = (mod 12)

1. clock

2. find the remainder after division of the modulo

$4 - 7 =$ (mod 12)

1. count backwards around the clock

2. make it an addition problem

3. since negative, add 12's until first get a non-negative number (or add a multiple of 12 to get a nonnegative number and then find the remainder upon division by 12)

$9 \otimes 5 \equiv$ (mod 10) or equivalently $9 \times 5 =$ (mod 10)

$9 \div 4 =$ (mod 12)

$2 \div 4 =$ (mod 6)

$6 \div 5 =$ (mod 7)