CS 3333: Mathematical Foundations

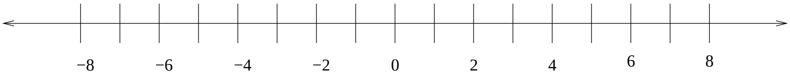
Number Theory

Number Theory

- **Integers** - Whole numbers written using the ten numerals $0, 1, 2, \ldots, 9$ where the position of a numeral dictates the value it represents.

Number Theory

- **Integers** - Whole numbers written using the ten numerals $0, 1, 2, \ldots, 9$ where the position of a numeral dictates the value it represents.
- The set of all integers is denoted by Z (i.e. $Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$).



Number Theory

- **Natural Numbers** - the set of all “counting integers”. The set of natural numbers is denoted by N.

Number Theory

- **Natural Numbers** - the set of all "counting integers". The set of natural numbers is denoted by N.
- Sometimes is the set of all positive integers (i.e. $N = \{1, 2, 3, \ldots\}$).

Number Theory

- **Natural Numbers** - the set of all "counting integers". The set of natural numbers is denoted by N.
- Sometimes is the set of all positive integers (i.e. $N = \{1, 2, 3, \ldots\}$).
- Sometimes is the set of all non-negative integers (i.e. $N = \{0, 1, 2, \ldots\}$).

Number Theory

- If a is an integer, then $|a|$ denotes the absolute value of a.

Number Theory

- If a is an integer, then $|a|$ denotes the absolute value of a.
- If a is a positive integer, then $|a| = a$ (e.g. if $a = 13$, then $|a| = 13$).

Number Theory

- If a is an integer, then $|a|$ denotes the absolute value of a.
- If a is a positive integer, then $|a| = a$ (e.g. if $a = 13$, then $|a| = 13$).
- If a is a negative integer, then $|a| = -a$ (e.g. if $a = -13$, then $|a| = 13$).

Number Theory

- Let a and b be integers such that $a \neq 0$.

Number Theory

- Let a and b be integers such that $a \neq 0$.
- **Definition**: We say a divides b if there is an integer c such that $b = ac$, denoted $a \mid b$.

Number Theory

- Let a and b be integers such that $a \neq 0$.
- **Definition**: We say a divides b if there is an integer c such that $b = ac$, denoted $a \mid b$.
- If there is no integer c such that $b = ac$ then a does not divide b, denoted $a \nmid b$.

Number Theory

- **Definition**: We say a divides b if there is an integer c such that $b = ac$, denoted $a \mid b$.

Number Theory

- **Definition**: We say a divides b if there is an integer c such that $b = ac$, denoted $a \mid b$.
- Example: Does 9 divide 36?

Number Theory

- **Definition**: We say a divides b if there is an integer c such that $b = ac$, denoted $a \mid b$.
- Example: Does 9 divide 36?
  - Yes. $36 = 9*4$ ($c = 4$).

Number Theory

- **Definition**: We say a divides b if there is an integer c such that $b = ac$, denoted $a \mid b$.
- Example: Does 9 divide 36?
  - Yes. $36 = 9*4$ ($c = 4$).
- Example: Does 11 divide 120?

Number Theory

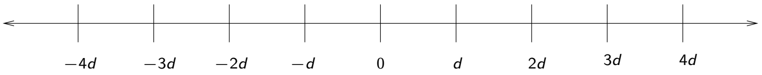
- **Definition**: We say a divides b if there is an integer c such that $b = ac$, denoted $a \mid b$.
- Example: Does 9 divide 36?
  - Yes. $36 = 9*4$ ($c = 4$).
- Example: Does 11 divide 120?
  - $11 \cdot 10 = 110$ and $11 \cdot 11 = 121$, so $11 \nmid 120$.

Number Theory

- Let n and d be positive integers. How many positive integers $\leq n$ are divisible by d?

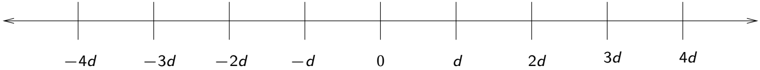
Number Theory

- Let n and d be positive integers. How many positive integers $\leq n$ are divisible by d?



Number Theory

- Let n and d be positive integers. How many positive integers $\leq n$ are divisible by d?



- We need to find an integer k such that
  1. $kd \leq n$
  2. $(k+1)d > n$

Number Theory

- Therefore we want the largest k such that $kd \leq n$.

Number Theory

- Therefore we want the largest k such that $kd \leq n$.
- $kd \leq n$

Number Theory

- Therefore we want the largest k such that $kd \leq n$.
- $kd \leq n \implies k \leq n/d$

Number Theory

- Therefore we want the largest k such that $kd \leq n$.
- $kd \leq n \implies k \leq n/d \implies k = \lfloor n/d \rfloor$.

Number Theory

- Therefore we want the largest k such that $kd \leq n$.
- $kd \leq n \implies k \leq n/d \implies k = \lfloor n/d \rfloor$.
- $\lceil x \rceil$ is the smallest integer $\geq x$ (ceiling function).

Number Theory

- Therefore we want the largest k such that $kd \leq n$.
- $kd \leq n \implies k \leq n/d \implies k = \lfloor n/d \rfloor$.
- $\lceil x \rceil$ is the smallest integer $\geq x$ (ceiling function).
- $\lfloor x \rfloor$ is the largest integer $\leq x$ (floor function).

Number Theory

- Therefore we want the largest k such that $kd \leq n$.
- $kd \leq n \implies k \leq n/d \implies k = \lfloor n/d \rfloor$.
- $\lceil x \rceil$ is the smallest integer $\geq x$ (ceiling function).
- $\lfloor x \rfloor$ is the largest integer $\leq x$ (floor function).
- Examples:
  $\lceil 11.7 \rceil = 12$; $\lfloor 11.7 \rfloor = 11$; $\lceil -5.3 \rceil = -5$; $\lfloor -5.3 \rfloor = -6$

Number Theory

- **Theorem 1**: Let a, b, and c be integers and $a \neq 0$.
  1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  2. If $a \mid b$, then $a \mid bc$.
  3. If $a \mid b$ and $b \mid c$, $b \neq 0$, then $a \mid c$.
- How can we prove Theorem 1?

Number Theory

- **Problem 8 [KR] Sec. 4.1**: Prove or disprove: if $a \mid bc$, then $a \mid b$ or $a \mid c$.

Number Theory

- **Problem 8 [KR] Sec. 4.1**: Prove or disprove: if $a \mid bc$, then $a \mid b$ or $a \mid c$.
- **False.** Counterexample: $a = 4$, $b = 2$, and $c = 6$.

Number Theory

- **Problem 7 [KR] Sec. 4.1**: Let a, b, and c be integers such that $a \neq 0$ and $c \neq 0$. Prove or disprove: if $ac \mid bc$, then $a \mid b$.

Number Theory

- **Corollary 1**: Let a, b, and c be integers such that $a \neq 0$. If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ whenever m and n are integers.

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Terminology: $a =$ dividend, $d =$ divisor, $q =$ quotient, and $r =$ remainder.

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Terminology: $a =$ dividend, $d =$ divisor, $q =$ quotient, and $r =$ remainder.
- Note: $q = \frac{a-r}{d}$.

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Terminology: $a =$ dividend, $d =$ divisor, $q =$ quotient, and $r =$ remainder.
- Note: $q = \frac{a-r}{d}$.
- $q = a \text{ div } d$ and $r = a \bmod d$.

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Examples:

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Examples:

a, d	$a = q \cdot d + r$	q and r

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Examples:

a, d	$a = q \cdot d + r$	q and r
$a = 11, d = 3$		

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Examples:

a, d	$a = q \cdot d + r$	q and r
$a = 11, d = 3$	$11 = 3 \cdot 3 + 2$	

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Examples:

a, d	$a = q \cdot d + r$	q and r
$a = 11, d = 3$	$11 = 3 \cdot 3 + 2$	$q = 3, r = 2$
$a = -11, d = 3$		

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Examples:

a, d	$a = q \cdot d + r$	q and r
$a = 11, d = 3$	$11 = 3 \cdot 3 + 2$	$q = 3, r = 2$
$a = -11, d = 3$	$-11 = -4 \cdot 3 + 1$	

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Examples:

a, d	$a = q \cdot d + r$	q and r
$a = 11, d = 3$	$11 = 3 \cdot 3 + 2$	$q = 3, r = 2$
$a = -11, d = 3$	$-11 = -4 \cdot 3 + 1$	$q = -4, r = 1$
$a = 11, d = -3$		

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Examples:

a, d	$a = q \cdot d + r$	q and r
$a = 11, d = 3$	$11 = 3 \cdot 3 + 2$	$q = 3, r = 2$
$a = -11, d = 3$	$-11 = -4 \cdot 3 + 1$	$q = -4, r = 1$
$a = 11, d = -3$	$11 = -3 \cdot -3 + 2$	

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Examples:

a, d	$a = q \cdot d + r$	q and r
$a = 11, d = 3$	$11 = 3 \cdot 3 + 2$	$q = 3, r = 2$
$a = -11, d = 3$	$-11 = -4 \cdot 3 + 1$	$q = -4, r = 1$
$a = 11, d = -3$	$11 = -3 \cdot -3 + 2$	$q = -3, r = 2$
$a = -11, d = -3$		

Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Examples:

a, d	$a = q \cdot d + r$	q and r
$a = 11, d = 3$	$11 = 3 \cdot 3 + 2$	$q = 3, r = 2$
$a = -11, d = 3$	$-11 = -4 \cdot 3 + 1$	$q = -4, r = 1$
$a = 11, d = -3$	$11 = -3 \cdot -3 + 2$	$q = -3, r = 2$
$a = -11, d = -3$	$-11 = 4 \cdot -3 + 1$	

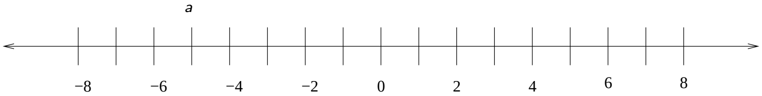
Number Theory

- **Division Algorithm**: Let a and d be integers with $d \neq 0$. Then there exist unique integers q and r, $0 \leq r < |d|$, such that $a = q \cdot d + r$.
- Examples:

a, d	$a = q \cdot d + r$	q and r
$a = 11, d = 3$	$11 = 3 \cdot 3 + 2$	$q = 3, r = 2$
$a = -11, d = 3$	$-11 = -4 \cdot 3 + 1$	$q = -4, r = 1$
$a = 11, d = -3$	$11 = -3 \cdot -3 + 2$	$q = -3, r = 2$
$a = -11, d = -3$	$-11 = 4 \cdot -3 + 1$	$q = 4, r = 1$

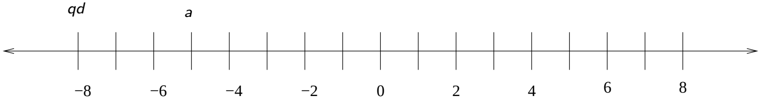
Number Theory

- The picture to have in mind:
- If $a < 0$:



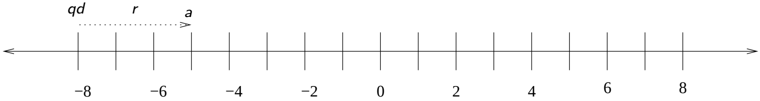
Number Theory

- The picture to have in mind:
- If $a < 0$:



Number Theory

- The picture to have in mind:
- If $a < 0$:

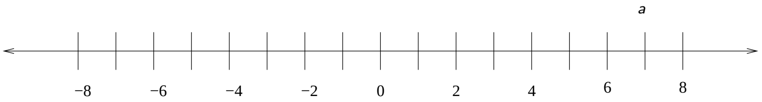


Number Theory

- The picture to have in mind:
- If $a > 0$:

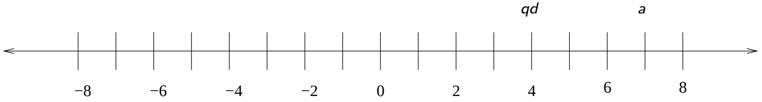
Number Theory

- The picture to have in mind:
- If $a > 0$:



Number Theory

- The picture to have in mind:
- If $a > 0$:



Number Theory

- The picture to have in mind:
- If $a > 0$: