Introduction to Number Theory

Ian Ludden

Learning Objectives

By the end of this lesson, you will be able to:

Learning Objectives

By the end of this lesson, you will be able to:

- Recall basic definitions from number theory.

Learning Objectives

By the end of this lesson, you will be able to:

- Recall basic definitions from number theory.
- Apply the definition of “divides” in direct proofs.

Learning Objectives

By the end of this lesson, you will be able to:

- Recall basic definitions from number theory.
- Apply the definition of “divides” in direct proofs.
- State the Division Algorithm theorem.

What is number theory?

What is number theory?

Definition

Number theory is the study of integers and integer-valued functions.

What is number theory?

Definition

Number theory is the study of integers and integer-valued functions.

Quote

"Mathematics is the queen of the sciences, and number theory is the queen of mathematics." – Gauss

Motivation

Number theory applications:

Motivation

Number theory applications:

- RSA Encryption

Motivation

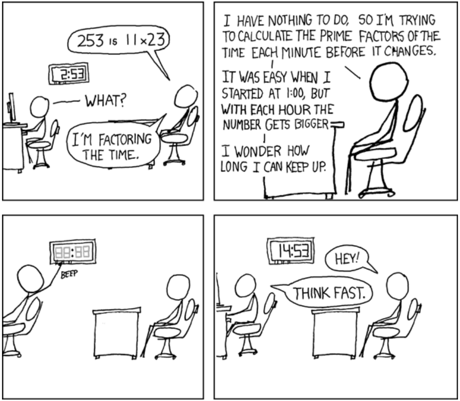
Number theory applications:

- RSA Encryption
- Bitcoin

Motivation

Number theory applications:

- RSA Encryption
- Bitcoin



Source: `https://xkcd.com/247/`

Basic definitions

Basic definitions

Definition

An integer n is *even* if there exists an integer m such that $n = 2m$.

Basic definitions

Definition

An integer n is *even* if there exists an integer m such that $n = 2m$.
An integer n is *odd* if there exists an integer m such that $n = 2m + 1$.

Basic definitions

Definition

An integer n is *even* if there exists an integer m such that $n = 2m$.
An integer n is *odd* if there exists an integer m such that $n = 2m + 1$.

Examples

- 0 is even, because $0 = 2 \cdot 0$

Basic definitions

Definition

An integer n is *even* if there exists an integer m such that $n = 2m$.
An integer n is *odd* if there exists an integer m such that $n = 2m + 1$.

Examples

- 0 is even, because $0 = 2 \cdot 0$
- 173 is odd, because $173 = 2 \cdot 86 + 1$

Basic definitions

Definition

An integer n is *even* if there exists an integer m such that $n = 2m$.
An integer n is *odd* if there exists an integer m such that $n = 2m + 1$.

Examples

- 0 is even, because $0 = 2 \cdot 0$
- 173 is odd, because $173 = 2 \cdot 86 + 1$
- -128 is even, because $-128 = 2(-64)$

Basic definitions

Basic definitions

Definition

For integers a and b, we say a *divides* b, written $a \mid b$, if there exists an integer n such that $b = an$.

Basic definitions

Definition

For integers a and b, we say a *divides* b, written $a \mid b$, if there exists an integer n such that $b = an$.
We call a a *factor* of b and b a *multiple* of a.

Basic definitions

Definition

For integers a and b, we say a *divides* b, written $a \mid b$, if there exists an integer n such that $b = an$.
We call a a *factor* of b and b a *multiple* of a.

Examples

- $3 \mid 6$

Basic definitions

Definition

For integers a and b, we say a *divides* b, written $a \mid b$, if there exists an integer n such that $b = an$.
We call a a *factor* of b and b a *multiple* of a.

Examples

- $3 \mid 6$
- $6 \nmid 3$

Basic definitions

Definition

For integers a and b, we say a *divides* b, written $a \mid b$, if there exists an integer n such that $b = an$.
We call a a *factor* of b and b a *multiple* of a.

Examples

- $3 \mid 6$
- $6 \nmid 3$
- $51 \mid 0$

Basic definitions

Definition

For integers a and b, we say a *divides* b, written $a \mid b$, if there exists an integer n such that $b = an$.
We call a a *factor* of b and b a *multiple* of a.

Examples

- $3 \mid 6$
- $6 \nmid 3$
- $51 \mid 0$
- $0 \mid 0$

Basic definitions

Definition

For integers a and b, we say a *divides* b, written $a \mid b$, if there exists an integer n such that $b = an$.
We call a a *factor* of b and b a *multiple* of a.

Examples

- $3 \mid 6$
- $6 \nmid 3$
- $51 \mid 0$
- $0 \mid 0$
- $(-5) \mid 30$

Basic definitions

Definition

For integers a and b, we say a *divides* b, written $a \mid b$, if there exists an integer n such that $b = an$.
We call a a *factor* of b and b a *multiple* of a.

Examples

- $3 \mid 6$
- $6 \nmid 3$
- $51 \mid 0$
- $0 \mid 0$
- $(-5) \mid 30$
- $11 \mid (-121)$

Basic definitions

Definition

For integers a and b, we say a *divides* b, written $a \mid b$, if there exists an integer n such that $b = an$.
We call a a *factor* of b and b a *multiple* of a.

Examples

- $3 \mid 6$
- $6 \nmid 3$
- $51 \mid 0$
- $0 \mid 0$
- $(-5) \mid 30$
- $11 \mid (-121)$

Basic definitions

Definition

For integers a and b, we say a *divides* b, written $a \mid b$, if there exists an integer n such that $b = an$.
We call a a *factor* of b and b a *multiple* of a.

Examples

- $3 \mid 6$
- $6 \nmid 3$
- $51 \mid 0$
- $0 \mid 0$
- $(-5) \mid 30$
- $11 \mid (-121)$

Warning

Tempting: "a divides b if $\frac{b}{a}$ is an integer." ***Don't do this.*** Breaks for $a = 0$; also, see Section 4.3 of the textbook.

Direct proofs using divides

Example

Claim: For all integers m and n, if m is even and $m \mid n$, then n is even.

Direct proofs using divides

Example

Claim: $\forall p, q, r \in \mathbb{Z}, (p \mid q) \wedge (q \mid r) \rightarrow (p \mid r)$.
(Transitive property of divides.)

The Division Algorithm

The Division Algorithm

Theorem

For any integers a *and* b*, where* $b > 0$*, there exist a unique quotient* $q \in \mathbb{Z}$ *and remainder* $r \in \mathbb{Z}$ *such that*

1. $a = bq + r$ *and*
2. $0 \leq r < b$.

The Division Algorithm

Theorem

For any integers a and b, where $b > 0$, there exist a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ such that

1. $a = bq + r$ *and*
2. $0 \leq r < b$.

Examples

- $a = 173$, $b = 5$

The Division Algorithm

Theorem

For any integers a and b, where $b > 0$, there exist a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ such that

1. $a = bq + r$ *and*
2. $0 \leq r < b$.

Examples

- $a = 173$, $b = 5$
- $a = -20$, $b = 4$

The Division Algorithm

Theorem

For any integers a and b, where $b > 0$, there exist a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ such that

1. $a = bq + r$ *and*
2. $0 \leq r < b$.

Examples

- $a = 173$, $b = 5$
- $a = -20$, $b = 4$
- $a = 12$, $b = 97$

Recap: Learning Objectives

By the end of this lesson, you will be able to:

- Recall basic definitions from number theory.
- Apply the definition of “divides” in direct proofs.
- State the Division Algorithm theorem.