Prime Numbers

Contents

1. Divisibility

2. Prime Numbers

Divisibility

Definitions

Definition 1 (Divisibility)

Let d and x be integers. To say that d *divides* x means that there exists an integer k such that $x = kd$.

- Every integer divides 0.
- 0 is the only integer that 0 divides. (If x is an integer and 0 divides x, then $x = k \cdot 0$ for some integer k, and $k \cdot 0 = 0$, so $x = 0$.)
- Let x be an integer. Then x is even iff 2 divides x.

Remarks

- Alternate expression for "d divides x": "x is divisible by d"
- "d divides x" is a sentence while "d divided into x" (x/d, for $d \neq 0$) is a number.
- **Notation.** $d \mid x$ for "d divides x." and $d \nmid x$ for "d does not divide x."
- Let m and n be integers, with $n \neq 0$. To say that the fraction m/n is in lowest terms means that for each natural number d, if d divides m and d divides n, then $d = 1$.

Examples

Example 2 (Divisibility with Natural Numbers)

Let $d, x \in \mathbb{N}$. Suppose d divides x. Then $d \leq x$.

Proof. Since d divides x, we can pick an integer k such that $x = kd$. Since k is an integer, either $k \geq 1$ or $k \leq 0$. But it is not the case that $k \leq 0$, because if $k \leq 0$, then $x = kd \leq 0$, which contradicts the fact that $x \geq 1$. Hence $k \geq 1$. Therefore $kd \geq d$. In other words, $x \geq d$. $\square$

Examples (cont')

Example 3

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

Examples (cont')

Example 4

Let $a, b, c \in \mathbb{Z}$. If a divides b and b divides a, then $b = a$ or $b = -a$.

Prime Numbers

Definitions

Definition 5 (Prime Numbers)

To say that x *is a prime number* means that $x \in \mathbb{N}$ and $x \neq 1$ and for each $a \in \mathbb{N}$, for each $b \in \mathbb{N}$, if $x = ab$, then $a = 1$ or $b = 1$.

Exercise. Write the sentence "$x \in \mathbb{N}$ and $x \neq 1$ and for each $a \in \mathbb{N}$, for each $b \in \mathbb{N}$, if $x = ab$, then $a = 1$ or $b = 1$." using symbols.

Prime Numbers as Building Blocks

Fact (Prime Factorization)

Each natural number, except 1, is prime or is a product of two or more primes.

- Proof of this fact requires complete induction.
- From this fact, it follows that for each $n \in \mathbb{N}$, if $n \neq 1$, then there exists a prime number p such that p divides n.

How Many Primes?

Theorem 6 (Euclid, circa 300 B.C.)

There are infinitely many prime numbers.