Prime Numbers

Contents

Divisibility

Definitions

preamble (sets the context of defin)

Syn.: x is divisible by d.

Definition 1 (Divisibility)

Let d and x be integers. To say that $\boxed{d \text{ divides } x}$ means that there exists an integer k such that $x = kd$.

$(\exists k \in \mathbb{Z})(x = kd)$

- Every integer divides 0. $\left(\overset{x}{0} = \overset{k}{0} \cdot d, \text{ for any } d \in \mathbb{Z} \right)$
- 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 $x = 0$.)

  $(\exists ! x)(x = k \cdot 0)$

  - Take $x = 0$. Then $0 = k \cdot 0 = 0$. ✓
  - Uniqueness?
- Let x be an integer. Then x is even iff 2 divides x.

  $(\exists k \in \mathbb{Z})(x = 2k)$ $\quad$ $(\exists k \in \mathbb{Z})(x = k \cdot 2)$

$x = 6$ is divisible by

$1, 2, 3, 6$

$-1, -2, -3, -6$

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.

  or "x divided by d"
- **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 $d = 1$.

  $(\forall d \in \mathbb{N})\ \left[(d \mid m) \wedge (d \mid n) \Rightarrow d = 1\right]$

$a \leq b$

$\Downarrow$

$ac \leq bc$

where $c > 0$.

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 $k \leq \cancel{1}$ 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, $x \geq d$. $\square$

$k \geq 1$

$d > 0$

$k \cdot d \geq 1 \cdot d$

<u>Example</u> ($d, x \in \mathbb{Z}$) $\quad d \mid x$

$$\begin{cases} x = -6. \\ d = -6, -3, -2, -1, 1, 2, 3, 6 \end{cases}$$

$x \leq d$

<u>Example</u> ($d, x \in \mathbb{N}$) $\quad d \mid x$

$$\begin{cases} x = 6 \\ d = 1, 2, 3, 6 \end{cases}$$

$d \leq x$

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 $b - c$.

Proof. Suppose $a \mid b$ and $a \mid c$.

Since $a \mid b$, we can find an integer k such that $b = ka$.

Since $a \mid c$, we can find an integer l such that $c = la$.

Then

$$b \pm c = ka \pm la = (k \pm l)a.$$

But then $k \pm l$ is an integer, so $a \mid b \pm c$. $\square$

Example 4

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

Hint

$$\begin{cases} b = ka \\ a = lb \end{cases}$$

$\rightarrow$ plug in 2nd line into 1st line

$$b = k(lb)$$

Prime Numbers

Definitions

Definition 5 (Prime Numbers)

To say that $\boxed{x \textit{ is a prime number}}$ 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.

Exercise : Write down what it means to say that
(HW)
"x is not prime"

Prime Numbers as Building Blocks

$6 = 2 \cdot 3$, $14 = 2 \cdot 7$

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.

Proof (Contradiction) Suppose there are finitely many prime number

$p_1, p_2, \cdots, p_m$.

Let $x = \underbrace{p_1 p_2 \cdots p_m}_{\text{prod. of all primes}} + 1$.

Claim None of $p_1, \cdots, p_m$ divides x.

proof Suppose otherwise, that is, one of $p_1, \cdots, p_m$ divides x.
Call it p_i. But then p_i divides $x-1 = p_1 \cdots p_m$.

Then p_i divides $x-(x-1)=1$, which is impossible.

This is a contradiction. $\square$