Ken

Today:

- 4.5 Direct Proof and Counterexample V
- 4.4 Direct Proof and Counterexample IV

Last time:

- 4.3 Direct Proof and Counterexample III
- 4.4 Direct Proof and Counterexample IV

Theorem 4.4.1

For all integers m and n, if m and n are positive and m divides n, then $m \leq n$.

$\forall m \in \mathbb{Z}\, \forall n \in \mathbb{Z}\, (m > 0 \wedge n > 0 \wedge m|n \rightarrow m \leq n)$

Property T20 of $\mathbb{R}$:

If $a < b$ and $c > 0$, then $ac < bc$.

$\forall a \in \mathbb{R}\, \forall b \in \mathbb{R}\, \forall c \in \mathbb{R}\, (a < b \wedge c > 0 \rightarrow ac < bc)$

Property T25 of $\mathbb{R}$:

If $ab > 0$ then both a and b are positive or both are negative.

$\forall a \in \mathbb{R}\, \forall b \in \mathbb{R}\, (ab > 0 \rightarrow (a > 0 \wedge b > 0) \vee (a < 0 \wedge b < 0))$

Theorem 4.4.2

The only divisors of 1 are 1 and -1.

Property T12:

Rule for Multiplication with Negative Signs

$(-a)b = a(-b) = -(ab)$

$(-a)(-b) = ab$

$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$.

Proof:

$1|1$ since $1 = (1)(1)$ where $1 \in \mathbb{Z}$

$-1|1$ since $1 = (-1)(-1)$ where $-1 \in \mathbb{Z}$

Let $m|1$. By definition of divides, $1 = mk$ for some $k \in \mathbb{Z}$. By property T25 of $\mathbb{R}$, since $mk > 0$, $m > 0$ and $k > 0$ or $m < 0$ and $k < 0$. Suppose $m, k > 0$. Via Theorem 4.4.1, $m \leq 1$ also because $m, 1 > 0$. Because $m \in \mathbb{Z}$ such that $0 < m \leq 1$, $m = 1$. Suppose $m, k < 0$. Then $1 = (-m)(-k)$ where $-m > 0$ and

$-k > 0$. Since $-m > 0$ and $-m \mid 1$, $0 < -m \leq 1$ again via Theorem 4.4.1. So $-m = 1$ (again because there is $\ell \in \mathbb{Z}$ such that $0 < \ell < 1$). Thus $m = -1$. Therefore, for any $n \in \mathbb{Z}$, if $m \mid 1$ then $m = 1$ or $m = -1$. □

Note: $m \mid n$ denotes the sentence m divides n but m/n denotes the number m divided by n

~~$m \mid n = \ell$~~

---

example 4.4.5 Prime Numbers and Divisibility

$n > 1$ is prime if and only if its only positive integer divisors are 1 and n

$$n \in \mathbb{P} \iff \forall d \in \mathbb{Z}^+ (d \mid n \to d = 1 \vee d = n)$$

Theorem 4.4.3

Transitivity of Divisibility

For all integers a, b, c, if a divides b and b divides c, then a divides c.

$\forall a \in \mathbb{Z}\, \forall b \in \mathbb{Z}\, \forall c \in \mathbb{Z}\, (a|b \wedge b|c \rightarrow a|c)$

Proof?

Let $a, b, c \in \mathbb{Z}$. Suppose $a|b$ and $b|c$. So, by definition of divides, $b = ka$ and $c = \ell b$ for some integers k, ℓ. Then, by substitution,

$$c = \ell b = \ell(ka)$$
$$= (\ell k)a$$

where $\ell k \in \mathbb{Z}$ by closure under multiplication. Thus $a|c$. □

Theorem 4.4.4

Any integer $n > 1$ is divisible by a prime number.

Is it true that for all $m, n \in \mathbb{Z}$, if $m|n$ and $n|m$ then $m = n$? No, e.g. $-2|2$ and $2|-2$ but $-2 \neq 2$.

Theorem 4.4.5

The Fundamental Theorem of Arithmetic
(or Unique Factorization of Integers Theorem)

Given any integer $n > 1$, there exists a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$ and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_k$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$12 = 2^2(3)$ $p_1 = 2$, $p_2 = 3$, $\alpha_1 = 2$, $\alpha_2 = 1$

and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

Proof? Later (in the semester). ○

Note: We say $\mathbb{Z}$ is a unique factorization domain.

Definition

Given any integer $n>1$, the standard factored form of n is an expression of the form

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_K^{\alpha_K}$$

where K is a positive integer, $p_1, p_2, \ldots, p_K$ are prime numbers, $\alpha_1, \alpha_2, \ldots, \alpha_K$ are positive integers, and $p_1 < p_2 < \cdots < p_K$.

$30 = 2(3)5$ where $2<3<5$ $10|2$

T #15 For all integers a, b, c, if $a|b$ and $a|c$, then $a|(b+c)$. $4|32$ and $4|8 \rightarrow 4|(32+8)$

T #17 For all integers a, b, c, and d, if $a|c$ and $b|d$, then $ab|cd$.

T #23 A sufficient condition for an integer to be divisible by 8 is that it be divisible by 16. $\forall m \in \mathbb{Z}\,(16|m \rightarrow 8|m)$

#28 For all integers a, b, c, if $a|bc$ then

F $a|b$ or $a|c$. $6|12 \wedge 6\nmid 3 \wedge 6\nmid 4$

4.5 Direct Proof and Counterexample V

Theorem

The Quotient-Remainder Theorem

Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

$$\forall n \in \mathbb{Z}\ \forall d \in \mathbb{Z}^+\ \exists! q \in \mathbb{Z}\ \exists! r \in \mathbb{Z}\ (n = dq + r \wedge 0 \leq r < d)$$

n is called the dividend or numerator.

d is called the divisor or denominator.

q is called the quotient.

r is called the remainder.

examples:

$n = 36,\ d = 7$ $\quad 36 = 7(5) + 1$ $\quad n\ d\ q\ r$

$n = -21,\ d = 6$ $\quad -21 = 6(-4) + 3$

$n = 10,\ d = 13$ $\quad 10 = 13(0) + 10$

$10 \text{ div } 13 = 0$

$10 \bmod 13 = 10$

Definition

Given an integer n and a positive integer d,

n div d = the integer quotient obtained when n is divided by d

n mod d = the nonnegative integer remainder obtained when n is divided by d

$$\forall n \in \mathbb{Z}\, \forall d \in \mathbb{Z}^+ \exists! q \in \mathbb{Z}\, \exists! r \in \mathbb{Z}\, (n \text{ div } d \wedge n \bmod d \longleftrightarrow n = dq + r \wedge 0 \leq r < d)$$

if $m, n \in \mathbb{Z}$ s.t. $m \mid n$ then $n \bmod m = 0$ because $n = mk + 0$.

36 div 7 = 5

36 mod 7 = 1

example 4.5.4

(a) Prove that if $n \in \mathbb{Z}^+$ then n mod 10 is the digit in the ones place in the decimal representation for n.

(b) Suppose $m \in \mathbb{Z}$. If m mod 11 = 6, what is $4m$ mod 11?

(b) Suppose $m \in \mathbb{Z}$.
Suppose $m \bmod 11 = 6$.
Via Quotient-Remainder theorem,

$m = 11q + 6$ then

$$4m = 4(11q) + 4(6) = 11(4q) + 24$$

$$= 11(4q) + 11(2) + 2$$

$$= 11(4q + 2) + 2$$

so $4m \bmod 11 = 2$.

(a) Let $n \in \mathbb{Z}^+$. Then there exist
$d_i \in \{0, 1, 2, \ldots, 9\}$ and $i \in \{1, \ldots, k\}$

for some $k \in \mathbb{Z}^+$, $d_k \neq 0$, such that

$$n = d_k d_{k-1} d_{k-2} \cdots d_2 d_1$$

e.g. $n = 13578$

$d_5 = 1, d_4 = 3, d_3 = 5, d_2 = 7, d_1 = 8$

$$n = 13578 = 1(10^4) + 3(10^3) + 5(10^2) + 7(10^1) + 8$$
$$= 10\left(1(10^3) + 3(10^2) + 5(10) + 7\right) + 8$$

$$n = d_k(10^{k-1}) + d_{k-1}(10^{k-2}) + \cdots + d_2 10 + d_1$$

$$= \underbrace{10}_{d}\left(\underbrace{d_k 10^{k-2} + d_{k-1}10^{k-3} + \cdots + d_3 10 + d_2}_{q}\right) + \underbrace{d_1}_{r}$$

$$(n = dq + r)$$

so $n \bmod 10 = d_1$ (the digit in the one's place).

Method of Proof by Division into Cases

To prove a statement of the form "If A_1 or A_2 or ... or A_n, then C," prove all the following

If A_1, then C,
If A_2, then C,
$\vdots$
If A_n, then C.

This shows C is true regardless of which $A_1, \ldots, A_n$ happens to be the case.

Representations of Integers

$n \bmod 2 = 0$ or $n \bmod 2 = 1$, why?

$n = 2k$ or $n = 2k+1$

Theorem 4.5.2

The Parity Property

The parity of an integer refers to whether the integer is even or odd.

Any two consecutive integers have opposite parity.

Any two consecutive integers have opposite parity.

$$\forall m, n \in \mathbb{Z} \left(n = m+1 \longrightarrow (n \in 2\mathbb{Z} \wedge m \in \mathbb{Z} - 2\mathbb{Z}) \vee (n \in \mathbb{Z} - 2\mathbb{Z} \wedge m \in 2\mathbb{Z}) \right)$$