Modular Arithmetic and Floor and Ceiling Functions

250H

Modular Arithmetic

The Division Algorithm: Let a be an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r \leq d$, such that $a = dq + r$.

- d is the divisor
- a is the dividend
- q is the quotient
- r is the remainder

Modular Arithmetic

The Division Algorithm: Let a be an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r \leq d$, such that $a = dq + r$.

- d is the divisor
- a is the dividend
- q is the quotient
- r is the remainder

$$r = a \ (\mathbf{mod}\ d)$$

Modular Arithmetic

Def: If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$. We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m. We say that $a \equiv b \pmod{m}$ is a congruence and the m is its modulus.

Modular Arithmetic

We will mainly use mods like this:

$100 \equiv 2 \pmod{7}$

Ie. *Insert Really Gross Number* ≡ $x \pmod{m}$ where x in $\{0, 1, \ldots, m-1\}$

Modular Arithmetic

Theorem: Let a and b be integers, and let m be a positive integer.

Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Modular Arithmetic

Theorem: Let a and b be integers, and let m be a positive integer.

Then $a \equiv b \pmod{m}$ if and only if $a \pmod{m} = b \pmod{m}$.

Theorem: Let m be a positive integer. The integers a and b are congruent modulo

m if and only if there is an integer k such that $a = b + km$.

Modular Arithmetic

Theorem: Let a and b be integers, and let m be a positive integer.

Then $a \equiv b \pmod{m}$ if and only if $a \pmod{m} = b \pmod{m}$.

Theorem: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Theorem: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Modular Arithmetic

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$

Proof: Let m be a positive integer, $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then, $b = a + xm$ and $d = c + ym$. So, $b - xm = a$ and $d - ym = c$. Therefore,

$$a + c = (b - xm) + (d - ym)$$

$$a + c = (b + d) - xm - ym$$

$$a + c = (b + d) + m(-x - y)$$

Hence, $a + c \equiv b + d \pmod{m}$ since $(-x - y)$ is an integer. ❄️

Floor and Ceiling Functions

Def: The floor function assigns to the real number x the largest integer that is less than or equal to x. The value of the floor function at x is denoted by $\lfloor x \rfloor$.

Floor and Ceiling Functions

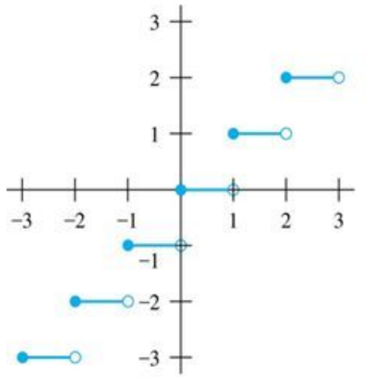
Def: The floor function assigns to the real number x the largest integer that is less than or equal to x. The value of the floor function at x is denoted by $\lfloor x \rfloor$.

Def: The ceiling function assigns to the real number x the smallest integer that is greater than or equal to x. The value of the ceiling function at x is denoted by $\lceil x \rceil$.

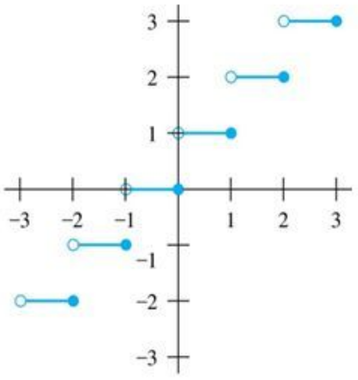
Floor and Ceiling Functions

Def: The floor function assigns to the real number *x* the largest integer that is less than or equal to *x*. The value of the floor function at *x* is denoted by $\lfloor x \rfloor$.

Def: The ceiling function assigns to the real number *x* the smallest integer that is greater than or equal to *x*. The value of the ceiling function at *x* is denoted by $\lceil x \rceil$.



(a) $y = \lfloor x \rfloor$



(b) $y = \lceil x \rceil$

Floor and Ceiling Functions

Properties of Floor and Ceiling Functions (*n* is an integer, *x* is a real number):

$\lfloor x \rfloor = n$ if and only if $n \leq x < n + 1$

$\lceil x \rceil = n$ if and only if $n - 1 < x \leq n$

Floor and Ceiling Functions

Properties of Floor and Ceiling Functions (*n* is an integer, *x* is a real number):

$\lfloor x \rfloor = n$ if and only if $n \leq x < n + 1$

$\lceil x \rceil = n$ if and only if $n - 1 < x \leq n$

$\lfloor x \rfloor = n$ if and only if $x - 1 < n \leq x$

$\lceil x \rceil = n$ if and only if $x \leq n < x + 1$

Floor and Ceiling Functions

Properties of Floor and Ceiling Functions (*n* is an integer, *x* is a real number):

$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$

Floor and Ceiling Functions

Properties of Floor and Ceiling Functions (*n* is an integer, *x* is a real number):

$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$

$\lfloor -x \rfloor = -\lceil x \rceil$

$\lceil -x \rceil = -\lfloor x \rfloor$

Floor and Ceiling Functions

Properties of Floor and Ceiling Functions (*n* is an integer, *x* is a real number):

$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$

$\lfloor -x \rfloor = -\lceil x \rceil$

$\lceil -x \rceil = -\lfloor x \rfloor$

$\lfloor x + n \rfloor = \lfloor x \rfloor + n$

$\lceil x + n \rceil = \lceil x \rceil + n$