Lecture 25: The floor function

Monday, November 21, 2016 2:42 PM

Lemma. For any real number x, there is a unique integer n such that

$$n \le x < n+1.$$

(In mathematical language, $\forall x \in \mathbb{R}, \exists!\, n \in \mathbb{Z},\ n \le x < n+1$.)

Proof. Existence. Case 1. $x \ge 0$.

Consider the set $\{m \in \mathbb{Z} \mid 0 \le m \le x\}$. This is a finite set. So it has a maximum (this can be proved for any finite subset of $\mathbb{R}$ using induction on the cardinality of the finite set.) Let $n = \max\{m \in \mathbb{Z} \mid 0 \le m \le x\}$. So

① $0 \le n \le x$ and ② $n+1 \notin \{m \in \mathbb{Z} \mid 0 \le m \le x\}$.

② implies that either $n+1 < 0$ or $n+1 > x$.

① implies $n+1 \ge 1$. So $n+1 > x$. Hence, by ①, we get

$$n \le x < n+1.$$

Case 2. $x \in \mathbb{Z}$.

In this case $x \le x < x+1$ and $n = x$ works.

Case 3. $x < 0$ and $x \notin \mathbb{Z}$.

Lecture 25: The floor function

Monday, November 21, 2016 2:50 PM

$x<0 \Rightarrow -x>0 \Rightarrow$ by case 1, there is $m\in\mathbb{Z}$ such that

$$m \le -x < m+1.$$

Since $x \notin \mathbb{Z}$, $m \neq -x$. Hence $m < -x < m+1$. Therefore

$$-(m+1) < x < -m = -(m+1)+1.$$

$$\Rightarrow -(m+1) \le x < -(m+1)+1.$$

So $n = -(m+1)$ works.

<u>Uniqueness</u> We have to show

$$\left.\begin{array}{l} n_1 \le x < n_1+1 \\ n_2 \le x < n_2+1 \\ n_1, n_2 \in \mathbb{Z} \end{array}\right\} \Rightarrow n_1 = n_2$$

Suppose to the contrary that for some $n_1, n_2 \in \mathbb{Z}$.

we have $n_1 \neq n_2$ and $n_1 \le x < n_1+1$ and $n_2 \le x < n_2+1$.

So either $n_1 > n_2$ or $n_2 > n_1$. By symmetry, it is enough

to deal with the case $n_1 > n_2$.

$$\left.\begin{array}{l} n_1 > n_2 \\ n_1, n_2 \in \mathbb{Z} \end{array}\right\} \Rightarrow \left\{\begin{array}{l} n_1 - n_2 > 0 \\ n_1 - n_2 \in \mathbb{Z} \end{array}\right\} \Rightarrow n_1 - n_2 \ge 1 \Rightarrow n_1 \ge n_2 + 1.$$

$\Rightarrow x \ge n_1 \ge n_2+1 > x \Rightarrow x > x$ which is a contradiction. ■

Lecture 25: Division algorithm

Monday, November 21, 2016 4:02 PM

<u>Theorem (Division algorithm)</u> For any integers a and b, $b \neq 0$, there is a unique pair of integers (q, r) such that

(1) $a = bq + r$ (2) $0 \le r < |b|$.

<u>Proof</u>. <u>Case 1</u>. $b > 0$.

<u>Existence</u>. Claim $q = \lfloor a/b \rfloor$ and $r = a - bq$ is such a pair.

- q is an integer by the definition of the floor function.
- $a, b, q \in \mathbb{Z} \Rightarrow r = a - bq \in \mathbb{Z}$.
- Property (1) is clear: $r = a - bq \Rightarrow a = bq + r$.

Now we show Property (2):

$$\lfloor a/b \rfloor \le a/b < \lfloor a/b \rfloor + 1 \Rightarrow q \le a/b < q + 1.$$

Since $b > 0$, we get $bq \le a < bq + b$

$\Rightarrow \quad 0 \le a - bq < b$ (adding $-bq$ to all sides.)

$\Rightarrow \quad 0 \le r < b = |b|$.

Case 2. $b<0$.

Claim $q=-\lfloor -a/b \rfloor$, $r=a-bq$ satisfy the mentioned properties.

- As before we can see q and r are integers which satisfy the 1st property.

- Now we show Property (2):

$$\lfloor -a/b \rfloor \le -a/b < \lfloor -a/b \rfloor + 1 \Rightarrow -q \le -a/b < -q+1.$$

Since $-b>0$, we get

$$(-b)(-q) \le (-b)\left(-\frac{a}{b}\right) < (-b)(-q+1)$$

$$\Rightarrow \quad bq \le a < bq-b = bq+|b|$$

$$\Rightarrow \quad 0 \le a-bq < |b| \qquad \text{(add } -bq)$$

$$\Rightarrow \quad 0 \le r < |b|.$$

Uniqueness. We have to prove

$$\left(\begin{matrix} a=bq_1+r_1 \\ 0\le r_1<|b| \end{matrix} \quad \text{and} \quad \begin{matrix} a=bq_2+r_2 \\ 0\le r_2<|b| \end{matrix}\right) \Rightarrow \begin{cases} q_1=q_2, \\ r_1=r_2. \end{cases}$$

Lecture 25: Division algorithm

Monday, November 21, 2016 4:22 PM

$$\left.\begin{array}{l} a = bq_i + r_i \\ 0 \le r_i < |b| \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \dfrac{a}{|b|} = \dfrac{bq_i}{|b|} + \dfrac{r_i}{|b|}. \\ 0 \le \dfrac{r_i}{|b|} < 1 \end{array}\right.$$

$$\Rightarrow \quad \frac{b}{|b|} q_i \le \underbrace{\frac{b}{|b|} q + \frac{r_i}{|b|}}_{\frac{a}{|b|}} < \frac{b}{|b|} q + 1$$

Notice that $\left(\frac{b}{|b|} = 1 \text{ if } b>0\right)$ and $\left(\frac{b}{|b|} = -1 \text{ if } b<0\right)$.

In particular, $\frac{b}{|b|} q_i \in \mathbb{Z}$. So

$$\frac{b}{|b|} q_i = \lfloor a/|b| \rfloor \Rightarrow q_i = \frac{|b|}{b} \lfloor a/|b| \rfloor .$$

[These are true for $i=1$ and $i=2$.] So

$$q_1 = \frac{|b|}{b} \lfloor a/|b| \rfloor = q_2 .$$

Hence $r_1 = a - bq_1 = a - bq_2 = r_2$. ■