Useful theorems and proofs for morpho-utils

Morpho Labs

This document aims to provide useful theorems and proofs for morpho-utils.

Overflow prevention

Lemma 1.

$$\forall n \in \mathbb{N}, \forall x \in \mathbb{R}, \lfloor x \rfloor < n \Leftrightarrow x < n$$

Proof. Let $n \in \mathbb{N}$, $x \in \mathbb{R}$. We suppose that $x < n$. Then because $\lfloor x \rfloor \leq x$, we have $\lfloor x \rfloor < n$.

Now, we suppose that $\lfloor x \rfloor < n$. We have:

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$$

Also, because $\lfloor x \rfloor$ is an integer, we have:

$$\lfloor x \rfloor + 1 \leq n$$

So:

$$x < n$$

□

Theorem 1.

$$\forall (x, y, M) \in \mathbb{N}^3, x > \lfloor M/y \rfloor \Leftrightarrow x \times y > M$$

Proof. Let $M \in \mathbb{N}, (x, y) \in \mathbb{N}^{*2}$, the case where x or y equals to 0 being trivial. With lemma 1, we have:

$$x > \lfloor M/y \rfloor \Leftrightarrow x > M/y$$

So:

$$\begin{aligned} x > \lfloor M/y \rfloor &\Leftrightarrow x \times y > M \\ &\Leftrightarrow x \times y > M \end{aligned}$$

□

Example

$$\forall (x,y) \in \mathbb{N}^{*2}, x > \frac{2^{256} - 1 - \frac{10^{18}}{2}}{y} \Leftrightarrow x \times y + \frac{10^{18}}{2} > 2^{256} - 1$$