Modular Congruence of Flooring Division of a Value with Known Modular Congruence by a Constant

Emboss Authors

2023

Theorem 1. *Given*

$$\begin{aligned}
&a \equiv r \pmod{m} \\
&b \neq 0 \\
&a, r, m, b, s, n \in \mathbb{Z} \\
&\frac{m}{b} \in \mathbb{Z}
\end{aligned}$$

then

$$\left\lfloor \frac{a}{b} \right\rfloor \equiv \left\lfloor \frac{r}{b} \right\rfloor \pmod{\frac{m}{b}} \tag{1}$$

Proof. By the definition of modular congruence:

$$\exists x \in \mathbb{Z} : a = mx + r \tag{2}$$

$$\left\lfloor \frac{a}{b} \right\rfloor \equiv \left\lfloor \frac{r}{b} \right\rfloor \pmod{\frac{m}{b}} \Leftrightarrow \exists z \in \mathbb{Z} : \left\lfloor \frac{a}{b} \right\rfloor = \frac{m}{b}z + \left\lfloor \frac{r}{b} \right\rfloor \tag{3}$$

$$\left\lfloor \frac{a}{b} \right\rfloor \equiv \left\lfloor \frac{r}{b} \right\rfloor \pmod{\frac{m}{b}} \Leftrightarrow \exists x, z \in \mathbb{Z} : \left\lfloor \frac{mx + r}{b} \right\rfloor = \frac{m}{b}z + \left\lfloor \frac{r}{b} \right\rfloor \tag{4}$$

given that $\frac{m}{b} \in \mathbb{Z}$ and that the product of two integers is an integer:

$$\frac{m}{b}x \in \mathbb{Z} \tag{5}$$

by the known property of *floor*:

$$\forall n \in \mathbb{Z} : \lfloor c + n \rfloor = \lfloor c \rfloor + n \tag{6}$$

and (5):

$$\left\lfloor \frac{mx + r}{b} \right\rfloor = \left\lfloor \frac{mx}{b} + \frac{r}{b} \right\rfloor \tag{7}$$

$$= \left\lfloor \frac{m}{b} x + \frac{r}{b} \right\rfloor \tag{8}$$

$$= \frac{m}{b} x + \left\lfloor \frac{r}{b} \right\rfloor \tag{9}$$

substituting (9) into (4):

$$\left\lfloor \frac{a}{b} \right\rfloor \equiv \left\lfloor \frac{r}{b} \right\rfloor \pmod{\frac{m}{b}} \Leftrightarrow \exists x, z \in \mathbb{Z} : \frac{m}{b} x + \left\lfloor \frac{r}{b} \right\rfloor = \frac{m}{b} z + \left\lfloor \frac{r}{b} \right\rfloor \tag{10}$$

choosing an arbitrary integer n for x and z specializes the left equation:

$$\frac{m}{b} n + \left\lfloor \frac{r}{b} \right\rfloor = \frac{m}{b} n + \left\lfloor \frac{r}{b} \right\rfloor \Rightarrow \exists x, z \in \mathbb{Z} : \frac{m}{b} x + \left\lfloor \frac{r}{b} \right\rfloor = \frac{m}{b} z + \left\lfloor \frac{r}{b} \right\rfloor \tag{11}$$

since the equation on the left of (11) is a tautology, the equation on the right of (11) is true. By (4), this implies that (1) is true.

$\square$