Modular Congruence of the Flooring Division Remainder of Two Values with Known Modular Congruences

Emboss Authors

2023

Theorem 1. *Given*

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

then

$$a - \left\lfloor \frac{a}{b} \right\rfloor b \equiv r \pmod{G\left(m, n, s\right)} \tag{1}$$

where G is the greatest common divisor function.

Proof.

$$\text{Let } q = G\left(m, n, s\right) \tag{2}$$

by the definition of modular congruence:

$$\exists x \in \mathbb{Z} : a = mx + r \tag{3}$$

$$\exists y \in \mathbb{Z} : b = ny + s \tag{4}$$

further, let:

$$z = \frac{m}{q}x - \left\lfloor \frac{mx + r}{ny + s} \right\rfloor \left(\frac{n}{q}y + \frac{s}{q} \right) \tag{5}$$

by the definition of G and the definition of q (2):

$$\frac{m}{q}, \frac{n}{q}, \frac{s}{q} \in \mathbb{Z} \tag{6}$$

because the result of the floor function is an integer by definition:

$$\left\lfloor \frac{mx+r}{ny+s} \right\rfloor \in \mathbb{Z} \tag{7}$$

from (3), (4), and (6), because the product of two integers is an integer:

$$\frac{m}{q}x, \frac{n}{q}y \in \mathbb{Z} \tag{8}$$

from (6) and (8) because the sum of two integers is an integer:

$$\frac{n}{q}y + \frac{s}{q} \in \mathbb{Z} \tag{9}$$

from (7) and (9) because the product of two integers is an integer:

$$\left\lfloor \frac{mx+r}{ny+s} \right\rfloor \left(\frac{n}{q}y + \frac{s}{q} \right) \in \mathbb{Z} \tag{10}$$

from (8) and (10) because the sum of two integers is an integer:

$$\frac{m}{q}x - \left\lfloor \frac{mx+r}{ny+s} \right\rfloor \left(\frac{n}{q}y + \frac{s}{q} \right) \in \mathbb{Z} \tag{11}$$

$$z \in \mathbb{Z} \tag{12}$$

factoring $\frac{1}{q}$ out of (2):

$$z = \frac{mx - \left\lfloor \frac{mx+r}{ny+s} \right\rfloor (ny+s)}{q} \tag{13}$$

substituting (2), (3), and (4) into (1):

$$(mx+r) - \left\lfloor \frac{mx+r}{ny+s} \right\rfloor (ny+s) \equiv r \pmod{q} \tag{14}$$

by the definition of modular congruence, (14) is equivalent to:

$$\exists w \in \mathbb{Z} : (mx+r) - \left\lfloor \frac{mx+r}{ny+s} \right\rfloor (ny+s) = qw + r \tag{15}$$

taking $w = z$:

$$
\begin{aligned}
qw + r &= qz + r && (16)\\
&= q\frac{mx - \left\lfloor \frac{mx+r}{ny+s} \right\rfloor (ny+s)}{q} + r && (17)\\
&= mx - \left\lfloor \frac{mx+r}{ny+s} \right\rfloor (ny+s) + r && (18)\\
&= (mx+r) - \left\lfloor \frac{mx+r}{ny+s} \right\rfloor (ny+s) && (19)
\end{aligned}
$$

because $z \in \mathbb{Z}$ (12) and (19), (15) is true, so (1) is true.

$\square$