Modular Congruence of the Product of Two Values with Known Modular Congruences

Emboss Authors

2018

1 Introduction

Theorem 1. *Given*

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

then

$$ab \equiv rs \pmod{G\left(\frac{m}{G(m,r)}, \frac{n}{G(n,s)}\right) \cdot G(m,r) \cdot G(n,s)}$$

where G is the greatest common divisor function.

Proof.

$$\text{Let } q = G(m,r) \tag{1}$$

$$p = G(n,s) \tag{2}$$

$$z = G\left(\frac{m}{q}, \frac{n}{p}\right) = G\left(\frac{m}{G(m,r)}, \frac{n}{G(n,s)}\right) \tag{3}$$

by the definition of modular congruence:

$$\exists x \in \mathbb{Z} : a = mx + r \tag{4}$$

$$\exists y \in \mathbb{Z} : b = ny + s \tag{5}$$

multiplying $\frac{q}{q}$ and distributing $\frac{1}{q}$:

$$a = q\left(\frac{mx}{q} + \frac{r}{q}\right) \tag{6}$$

by the definition of q in (1):

$$\frac{mx}{q}, \frac{r}{q} \in \mathbb{Z} \tag{7}$$

multiplying $\frac{p}{p}$ and distributing $\frac{1}{p}$:

$$b = p\left(\frac{ny}{p} + \frac{s}{p}\right) \tag{8}$$

by the definition of p in (2):

$$\frac{ny}{p}, \frac{s}{p} \in \mathbb{Z} \tag{9}$$

multiplying $\frac{z}{z}$:

$$a = q\left(z \cdot \frac{mx}{qz} + \frac{r}{q}\right) \tag{10}$$

by the definition of z in (3):

$$\frac{mx}{qz} \in \mathbb{Z} \tag{11}$$

multiplying $\frac{z}{z}$:

$$b = p\left(z \cdot \frac{ny}{pz} + \frac{s}{p}\right) \tag{12}$$

by the definition of z in (3):

$$\frac{ny}{pz} \in \mathbb{Z} \tag{13}$$

(10) and (12):

$$ab = qp\left(z \cdot \frac{mx}{qz} + \frac{r}{q}\right)\left(z \cdot \frac{ny}{pz} + \frac{s}{p}\right) \tag{14}$$

partially distributing (14):

$$ab = qp\left(z^2 \cdot \frac{mx}{qz} \cdot \frac{ny}{pz} + z \cdot \frac{r}{q} \cdot \frac{ny}{pz} + z \cdot \frac{mx}{qz} \cdot \frac{s}{p} + \frac{r}{q} \cdot \frac{s}{p}\right) \tag{15}$$

extracting the $\frac{rs}{qp}$ term from (15) and cancelling $\frac{qp}{qp}$:

$$ab = qp\left(z^2 \cdot \frac{mx}{qz} \cdot \frac{ny}{pz} + z \cdot \frac{r}{q} \cdot \frac{ny}{pz} + z \cdot \frac{mx}{qz} \cdot \frac{s}{p}\right) + rs \tag{16}$$

factoring z from (16):

$$ab = qpz\left(z \cdot \frac{mx}{qz} \cdot \frac{ny}{pz} + \frac{r}{q} \cdot \frac{ny}{pz} + \frac{mx}{qz} \cdot \frac{s}{p}\right) + rs \tag{17}$$

because $z, \frac{r}{q}, \frac{s}{p}, \frac{mx}{qz}, \frac{ny}{pz} \in \mathbb{Z}$, per (3), (7), (9), (11), (13):

$$z \cdot \frac{mx}{qz} \cdot \frac{ny}{pz} + \frac{r}{q} \cdot \frac{ny}{pz} + \frac{mx}{qz} \cdot \frac{s}{p} \in \mathbb{Z} \tag{18}$$

by the definition of modulus:

$$ab \equiv rs \pmod{qpz} \tag{19}$$

by the definitions of q, p, and z in (1), (2), and (3):

$$ab \equiv rs \pmod{G\left(\frac{m}{G(m,r)}, \frac{n}{G(n,s)}\right) \cdot G(m,r) \cdot G(n,s)} \tag{20}$$

$\square$