Congruence for day 11 of AoC 2022

mattiasdrp

2022-12-13 mar.

We want to prove that if $n \equiv r_1[q_1] \dots n \equiv r_n[q_n]$ and if $n \equiv N[q_1 \dots q_n]$ then $N \equiv r_1[q_1] \dots N \equiv r_n[q_n]$

Let

$$n \equiv r_1[q_1]$$
$$n \equiv r_2[q_2]$$

and

$$n \equiv N[q_1 * q_2]$$

We know that

$$a \equiv b[n] \Leftrightarrow b \equiv a[n]$$

So

$$N \equiv n[q_1 * q_2]$$

But if

$$N \equiv n[q_1 * q_2]$$

then

$$N \equiv n[q_1]$$
$$N \equiv n[q_2]$$

because

$$\begin{aligned} N &= (q_1 * q_2) * k + n & \Leftrightarrow \quad & N \equiv n[q_1 * q_2] \\ &= q_1 * (q_2 * k) + n & \Leftrightarrow \quad & N \equiv n[q_1] \\ &= q_2 * (q_1 * k) + n & \Leftrightarrow \quad & N \equiv n[q_2] \end{aligned}$$

We proved that

$$N \equiv n[q_1]$$
$$N \equiv n[q_2]$$

The transitivity of modulo says that

$$\text{if } a \equiv b[q] \text{ and } b \equiv c[q] \text{ then } a \equiv c[q]$$

Since

$$n \equiv r_1[q_1]$$
$$n \equiv r_2[q_2]$$

Then

$$N \equiv r_1[q_1]$$
$$N \equiv r_2[q_2]$$