Marcelo's Discrete Mathematics, Supervision 3 Question 4

Thomas Forster

January 1, 2021

Prove the biconditional:

$$n \cdot i \equiv n \cdot j \pmod{m} \longleftrightarrow i \equiv j \pmod{m/\gcd(m,n)}$$

dddc2 put me on the spot with this one.

L $\to$ R

If i and j are congruent modulo $p \cdot q$ then they are clearly congruent mod q (fewer equivalence classes mod p than mod $p \cdot q$!). So the LHS implies that

$n \cdot i \equiv n \cdot j \pmod{m/\gcd(m,n)}$

Now n and $m/\gcd(m,n)$ are coprime. (It's easy to see this if you think of natural numbers as multisets of primes). So n has a multiplicative inverse mod $m/\gcd(m,n)$). So we can multiply both halves of the equation in the LHS by that multiplicative inverse. This gives us the RHS.

R $\to$ L

RHS implies that $i - j$ is divisible by $m/\gcd(m,n)$, which is as much as to say that $(i-j)\cdot\gcd(m,n)$ is divisible by m.

So $i\cdot\gcd(m,n) - j\cdot\gcd(m,n)$ is divisible by m.

That is to say that $i\cdot\gcd(m,n)$ and $j\cdot\gcd(m,n)$ are congruent mod m.

But always, if a and b are congruent mod x, so are ay and by for any $y \in \mathbb{N}$.

So we can multiply the two members $i\cdot\gcd(m,n)$ and $j\cdot\gcd(m,n)$ of the congruent pair by $n/\gcd(m,n)$—which is an integer—to obtain another congruent pair $n \cdot i$ and $n \cdot j$.