

Re: valid proof? of "x = y modulo m => x, y same remainders divided by m"

Re: valid proof? of "x = y modulo m => x, y same remainders divided by m"

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-11/msg03827.html>

- *From:* magidin@xxxxxxxxxxxxxxxxxxxx (Arturo Magidin)
 - *Date:* Mon, 13 Nov 2006 20:12:29 +0000 (UTC)
-

In article <1163448534.423080.293330@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>, G Patel <gaya.patel@xxxxxxxx> wrote:

I've seen a proof of "x = y modulo m if and only if x and y have same remainders when divided by m" that was rather awkward (I've added it at end of this post for reference).

I was dissatisfied because this theorem is intuitively "obvious" and this intuition was based on something that I think leads to a different proof (the intuition doesn't related too directly with the proof I saw). Please tell me if my proof has any holes.

Proving => implication:

By division algorithm, $x = qm + r, 0 \leq r < m$

By definition of congruence, $y = x + km$, for some k in integers

therefore $y = qm + r + km, 0 \leq r < m$
 $y = (q+k)m + r, 0 \leq r < m$

By division algorithm, r must be remainder when y is divided by m.

Proving <= implication:

By division algorithm,

$x = sm + r, 0 \leq r < m$
 $y = tm + r, 0 \leq r < m$ (same remainders)

solving for r in first and subbing into second:

$y = tm + x - sm$
 $y = x + (t-s)m$ which implies $x = y \pmod{m}$

=====

Re: valid proof? of "x = y modulo m => x, y same remainders divided by m"

any holes?

As a minor nitpick, congruence is usually defined as "x = y (mod m) if and only if m|x-y". The fact that this is equivalent to "y = x + km for some integer k" is a (very, extremely) minor lemma.

Otherwise, no.

This is the book's proof:

By div. alg,

$$x = km + r, 0 \leq r < m$$

$$y = lm + s, 0 \leq s < m$$

subtract second from first:

$$(x-y) = (k-l)m + (r-s), \text{ where } -m < r-s < m$$

[proving \Leftarrow implication]

So if x, y have same remainders $(r-s) = 0$ and

$$x - y = (k-l)m \Rightarrow x = y + (k-l)m, \text{ which implies } x \equiv y \pmod{m}$$

[proving \Rightarrow implication]

if $x \equiv y \pmod{m}$, then $m|(x-y)$

$$\text{hence } m \mid [(x-y) - (k-l)m] = m|(r-s)$$

But $-m < r-s < m$, so $r-s$ has to be 0 $\Rightarrow r=s$, as required.

This is basically the same as your proof, only doing the division first. What is your objection to this?

--

=====
"It's not denial. I'm just very selective about what I accept as reality."

--- Calvin ("Calvin and Hobbes" by Bill Watterson)

=====
Arturo Magidin
magidin-at-member-ams-org

.