

Re: FLTMA: A little group theory

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-10/msg05024.html>

- *From:* "The Dougster" <DGoncz@xxxxxxx>
 - *Date:* 18 Oct 2006 03:53:51 -0700
-

There is a problem with FLTMA1.exe, at
<ftp://users.aol.com/DGoncz/Education/NVCC>.

I compute a quotient, then take the power. It doesn't work out.

I call the quotients $qxiz$ for quotient of x divided by $y \bmod z$,
 $qyix$ similarly, and so $qzix$ and $qxix$. I call the inverse $y \bmod z$
 iyz , and so
 ixz , ixy , and iyx .

I find $(x * iyz)^n \bmod z \neq qxiz^n \bmod z$

I was confused about how Chip Eastham got to $(x/y)^n \equiv -1 \pmod z$ but it
seemed right, and I think I understand it now, but working out $y * iyz$
 $\equiv 1 \pmod z$ to solve for iyz , and computing $qxiz = (x * iyz) \bmod z$
before looking at the powers $qxiz^n \bmod z$ just doesn't seem to work.

Have I made one too many substitutions and lost the validity of the
modular arithmetic?

Most likely it's a typo but I am not seeing it.

The latest version has been uploaded.

Doug

.