

Re: FLTMA: A little group theory

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-10/msg05416.html>

- *From:* "Chip Eastham" <hardmath@xxxxxxxxxx>
 - *Date:* 19 Oct 2006 19:42:44 -0700
-

The Dougster wrote:

Chip Eastham wrote:

The converse is not true, though. Consider the residue in $\mathbb{Z}/15\mathbb{Z}$. The order of residue 4 is 2, but clearly half that order does not give a power of 4 equal to -1 in $\mathbb{Z}/15\mathbb{Z}$. In fact you can run through all possible powers of 4 in $\mathbb{Z}/15\mathbb{Z}$ without getting to -1 .

That follows from 2 prime, I think, if the above was valid.

More directly, if the order of an element $w \pmod z$ is 2, then the only possible solution is the trivial one:

$$w^1 = w = -1 \pmod z.$$

since the sequence of positive powers of w repeats:

$$w, 1, w, 1, \dots$$

Other prime orders are oddly enough, odd, and we know if some power of w is -1 , then the order of w must be divisible by the order of -1 , which is 2 (in that $z > 2$).

However w may fail to have a power equal to -1 in spite of the order of $w \pmod z$ being even and composite. For example in $\mathbb{Z}/15\mathbb{Z}^*$, the powers of 2 are:

$$2, 4, 8, 1, (\text{repeat})$$

so the order of 2 is 4, but no power of 2 is -1 .

regards, chip

Re: FLTMA: A little group theory