

Re: FLTMA: A little group theory

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-10/msg05767.html>

- *From:* "The Dougster" <DGoncz@xxxxxxx>
 - *Date:* 20 Oct 2006 15:56:49 -0700
-

Chip Eastham wrote:

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, (repeat)

Re: FLTMA: A little group theory

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

regards, chip

Ah. The order of -1 is 2. $|\langle -1 \rangle| = 2$. $\langle -1 \rangle = \{ -1, 1 \}$.

How do we know that if $w^n \equiv -1 \pmod z$ that $|\langle -1 \rangle|$ divides $|\langle w \rangle|$?

I am fairly sure $\langle x/y \rangle$ and $\langle y/x \rangle$ are cyclic subgroups of the set of numbers relatively prime to z, and $\langle z/x \rangle$ of the set ... y, and $\langle z/y \rangle$ of the set... x.

Groups of prime order are always cyclic. Are these cyclic subgroups of prime order? It can go either way. There are, of course groups of composite order that are cyclic.

From

$$x^n + y^n \equiv 0 \pmod z$$

we have both

$$(x/y)^n \equiv -1 \pmod z \text{ and}$$

$$(y/x)^n \equiv -1 \pmod z.$$

The n in both expressions is the same, but we do not know $x/y = y/x$. We do know $|\langle x/y \rangle| = |\langle y/x \rangle|$, though.

To prove that

(1) $\gcd(x,y,z) = 1$, (2) $x < y < z < x+y$, (3) exactly one of $\{x, y, z\}$ is even,

$$(4) (x/y)^n \equiv -1 \pmod z,$$

$$(5) (z/x)^n \equiv 1 \pmod y, \text{ and}$$

$$(6) (z/y)^n \equiv 1 \pmod x$$

implies

$$(7) n \text{ is } 2 \text{ or composite}$$

might be done 4 ways, right?

Directly: (1) & (2) & (3) & (4) & (5) & (6) \implies (7)

Indirectly: $\sim(7) \implies !(1) \vee !(2) \dots$

By contradiction: ?

By induction: Er, well, not by induction, I certainly don't think so.

Doug

.