

Re: FLTMA: A little group theory

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-10/msg00647.html>

- *From:* "Chip Eastham" <hardmath@xxxxxxxxxx>
 - *Date:* 2 Oct 2006 05:11:45 -0700
-

The Dougster wrote:

Hello. I have completed the first of three tests in the abstract algebra course at the CoCo. We are up to cyclic subgroups in Fraleigh's seventh edition of A First Course in Abstract Algebra.

From FLT we have, by way of contradiction (I think that is how you say

it)

$$a^n + b^n = c^n$$

and so

$x^p + y^p = z^p$ where $\gcd(x,y,z)=1$, one of $\{x,y,z\}$ is even, p is prime, and $x < y < z < (x+y)$.

I'd like to look at $(x^p + y^p) \pmod{z}$. This implies $x^p \equiv -y^p \pmod{z}$. x^p is the additive inverse of y^p , in addition modulo z .

Hi, Doug:

I don't see what Fermat's Last Theorem has to do with any of the rest of your post.

In cyclic group notation in our text we write $\langle x \rangle$ for all the powers of x modulo some implied z . $\langle x \rangle$ is the cyclic subgroup generated by x .

The phi function is written $\phi(n) = |\{x \mid \gcd(x,n)=1, 0 < x < n\}|$. That is, the measure of the set of numbers coprime to n . We have a theorem in our text that if element a generates G , that is, $\langle a \rangle = G$, then $|\langle a^s \rangle| = n / (\gcd(n,s))$. Each of $\langle a^s \rangle$ is a subgroup of G , and

Re: FLTMA: A little group theory

so contains the inverse of element a^s under the group operation, which we call $*$. There are $\phi(n)$ generators of an arbitrary group isomorphic to Z_n .

For every z , is there an Abelian group, $Z_z - 0$, of numbers from 1 to $z-1$ under multiplication modulo z , with associativity, an identity, 1, in the group, and a multiplicative inverse for every element in the group?

So, for arbitrary n , there is a multiplicative group Z/nZ^* consisting of the $\phi(n)$ residues coprime to n . This group is cyclic only in some special cases. Consider for example the multiplicative group $Z/15Z^*$ which has $\phi(15) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8$ elements. This is not cyclic, being in fact $Z/2Z \times Z/4Z$.

The cases where the multiplicative group Z/nZ^* is cyclic are:

$n = 2$, $n = 4$, $n = p^m$, $n = 2 \cdot p^m$

for odd prime p and integer $m > 0$.

regards, chip

.