

Re: FLTMA: A little group theory

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-10/msg00904.html>

- *From:* "The Dougster" <DGoncz@xxxxxxx>
 - *Date:* 3 Oct 2006 04:41:42 -0700
-

Chip Eastham wrote:

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 $\phi(n) = | \{ x \mid \gcd(x,n)=1, 0 < x < n \} |$.

Re: FLTMA: A little group theory

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 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?

For example, from $3^2 + 4^2 = 5^2$, with * multiplication modulo 5:

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Isn't that a 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 $\phi(15) = \phi(3)*\phi(5) = 2*4 = 8$ elements. This is not cyclic, being in fact $Z/2Z \times Z/4Z$.

I don't follow this. What is the notation Z/nZ^* ? The integers divided by the nonzero multiples of n? I can understand that $\phi(5)$ is 4, and that the table above has 4 elements.

What is the X? In our text, x is the Cartesian product...

Yes, there is some (simple?) notation I am missing to follow this.

I guess I should work out:

* is multiplication modulo 6:

*	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4

That's not even a group, much less cyclic. Hm. I have answered my own

Re: FLTMA: A little group theory

question. No, there is not such a group for *every* n.

Now, you write there is a group of the $\phi(n)$ residues coprime to n. 2 is not coprime to 6. Neither are 3 or 4. 5 and 1 are coprime to 6.

* = * mod 6
* 1 5
1 1 5
5 5 1

Hm. In FLT, for every possible $x^n + y^n = z^n$ there *is* a group G under multiplication modulo z with elements the $\phi(z)$ residues of z coprime to z, containing all possible values of x and y as elements. This group is not always cyclic, but is always Abelian. Right?

I think I am getting the content but the notation is new to me.

This group is the powers of x and y mod z only if it's cyclic. Right?

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

If z is 2, 4, p^m , or $2 \cdot p^m$, then there is a cyclic group I can call G containing all possible values of x and y for $x^p + y^p = z^p$ and all powers of x and y mod z.

Now there are also $z^p - x^p = y^p$ and $z^p - y^p = x^p$ to consider.

Is it true that for a counterexample to FLT, *at least one* of {x,y,z} must be 2, 4, p^m , or $2 \cdot p^m$?

I do notice that for all $x^2 + y^2 = z^2$, at least one of {x,y,z} seems to always be p^1 , but I don't see that that has to be true for the equation to power p.

This was not the week to try to quit smoking tobacco! Grrrr....

Thanks. Doug

.