Re: FLTMA: A little group theory

Source: http://sci.tech−archive.net/Archive/sci.math/2006−10/msg01392.html

* *From*: "The Dougster" <DGoncz@xxxxxxx>
* *Date*: 5 Oct 2006 03:57:01 −0700

Hello, all. Hello, Chip.

Chip Eastham wrote:

> Doug Goncz wrote:
> It seems rather that you should be saying:
>
> (x^p + y^p) = 0 mod z, and
> (z^p − x^p) = 0 mod y, and
> (z^p − y^p) = 0 mod x
>
>> But if we look at sequences with (x,y,z) = 1, one of {x,y,z} even, and
>> x<y<z<(x+y)
>>
>> (x^n + y^n) mod z + (z^n − x^n) mod y + (z^n − y^n) mod x or
>> (x^n + y^n) mod z * (z^n − x^n) mod y * (z^n − y^n) mod x
>>
>> by hand waving arguments (call them a lemma), we find that n is always
>> 2 or composite, never an odd prime.
>> So FLT is proved.
>
> I think I'd spend a bit of time trying to search out
> a counterexample. You're conjecturing something
> stronger than FLT, which implies (though you may
> not have realized it) that the above can only occur
> if n is a power of 2.

Yes,

(x^n + y^n) == 0 mod z &
(z^n − x^n) == 0 mod y &
(z^n − y^n) == 0 mod x

is the more standard way to say this.

Now, why or how would this imply that this can only occur if n = 2^m?
Group theory?

I have solutions with n = 2 and n composite but never n odd prime.

Yes, I realize this is stronger than FLT.
You'd agree if one could prove this stronger statement, then FLT would follow, right?
And that sometimes it is easier to prove the stronger of two statements, yes?

I wonder if there is another way to say "one of {x,y.z} even" or another similar conclusion that can be drawn.

Rewriting for easier discussion:

From
(0) a^n + b^n = c^n in Z,
we have, in Z+,
(1) p prime
(2) gcd(x,y,z) = 1 or (x,y) = (y,z) = (x,z) = 1, a relation I still misunderstand....
(3) x^p + y^p = z^p
(4) one of {x,y,z} even
(5) x<y<z<(x+y)
(6) (x^p + y^p) == 0 mod z
(7) (z^p − x^p) == 0 mod y
(8) (z^p − y^p) == 0 mod x

I note that in my tests, leaving out (2), (3), (4), or (5) results in violations of (1), which does not prove that (2), (3), (4), and (5) together imply (1), just as (6), (7), and (8) do not imply (0), but are only necessary for (0).

I have "Finite Group Behavior 3.0" software to play with. :)

We are talking here about all cyclic multiplicative groups of integers with order phi(n), n in Z+, aren't we?

With x, y, and z pairwise coprime, is
phi(z) / gcd(phi(z), x) ever equal to
phi(z) / gcd(phi(z), y)? (I can start some checks)

Mantra for today:

"If I had wanted to smoke outside my home, I'd have brought my cigarettes.
Nicotrol will just have to do until I get back."

Maybe cold turkey just doesn't work for me and I can quit by stages. ;)

Doug

.