

Re: FLTMA: A little group theory

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-10/msg05096.html>

- *From:* "Chip Eastham" <hardmath@xxxxxxxxxx>
 - *Date:* 18 Oct 2006 08:02:39 -0700
-

The Dougster wrote:

There is a problem with FLTMA1.exe, at
<ftp://users.aol.com/DGoncz/Education/NVCC>.

I compute a quotient, then take the power. It doesn't work out.

I call the quotients $qxizy$ for quotient of x divided by $y \bmod z$,
 $qyixz$ similarly, and so $qzixy$ and $qxixy$. I call the inverse $y \bmod z$
 iyz , and so
 ixz , ixy , and iyx .

I find $(x * iyz)^n \bmod z \neq qxizy^n \bmod z$

I was confused about how Chip Eastham got to $(x/y)^n \equiv -1 \pmod z$ but it
seemed right, and I think I understand it now, but working out $y * iyz$
 $= 1 \pmod z$ to solve for iyz , and computing $qxizy = (x * iyz) \bmod z$
before looking at the powers $qxizy^n \bmod z$ just doesn't seem to work.

Have I made one too many substitutions and lost the validity of the
modular arithmetic?

Most likely it's a typo but I am not seeing it.

A couple of points. First, for some values of x, y, z there
will not be a solution for $(x/y)^n \equiv -1 \pmod z$, so your code
will have to report these failures "nicely". This contrasts
with congruences $(z/y)^n \equiv 1 \pmod x$ and $(z/x)^n \equiv 1 \pmod y$
which are always solvable, resp. by some divisors of
 $\phi(x)$ and $\phi(y)$. I.e. elements of a multiplicative group
must have an order.

What I noted about cases when $(x/y)^n \equiv -1 \pmod z$ does
have a solution is that then n is half the order of (x/y) in
 $\mathbb{Z}/z\mathbb{Z}^*$.

The converse is not true, though. Consider the residue

Re: FLTMA: A little group theory

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 .

So my recommendation for solving $(x/y)^n = -1 \pmod{z}$ is to compute the order of (x/y) in $\mathbb{Z}/z\mathbb{Z}^*$ just as you would for the other two congruences. If this order is not even, you are done in that there is no solution. If the order is even, you must verify whether or not half the order gives $(x/y)^n = -1 \pmod{z}$.

Finally we have three simultaneous congruences for the exponents n (assuming the third condition here can be satisfied at all):

n is a multiple of the order of (z/y) in $\mathbb{Z}/x\mathbb{Z}^*$
 n is a multiple of the order of (z/x) in $\mathbb{Z}/y\mathbb{Z}^*$
 n is an odd multiple of half the order of (x/y) in $\mathbb{Z}/z\mathbb{Z}^*$ (if a solution exists)

regards, chip

.