Proposal: Fermat Little Theorem

John D Mangual

In high school summer camp, we had a journal club and I read a proof of **F**ermat's **L**ittle **T**heorem:

$$a^p \equiv \ a \quad (\mathrm{mod}\ p)$$

This theorem is important as soon as you need decimals. Let $a = 10$ and $p = 7$:

$$10^7 \equiv 10 \quad (\mathrm{mod}\ 7)$$

and clearly 7 does not divide 10, so we can just cancel:

$$10^6 = 1,000,000 \equiv 1 \quad (\mathrm{mod}\ 7)$$

and we solved that problem without any long division.

$$(10^6 - 1) \div 7 = 142,657$$

What is this good for?

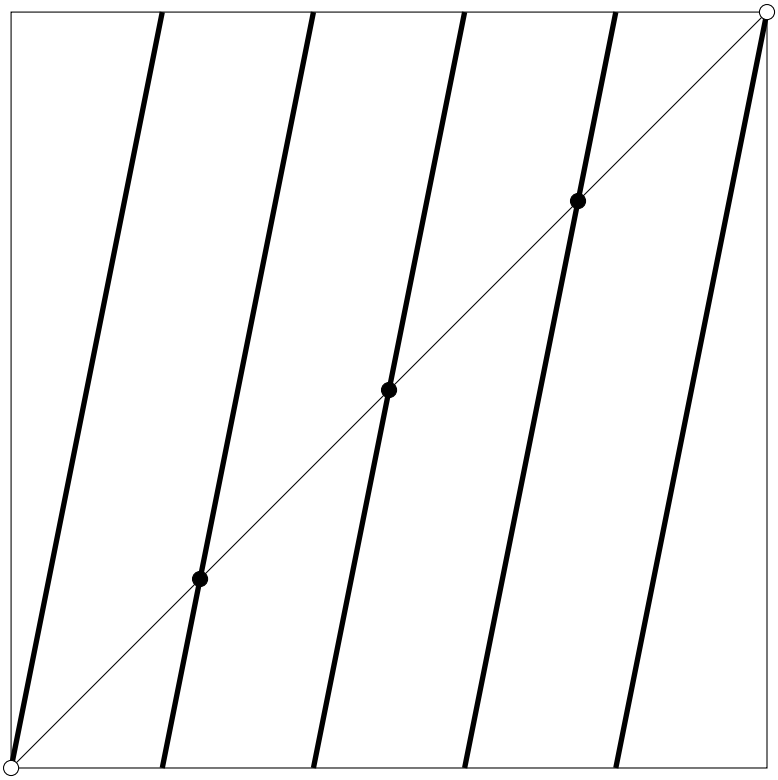
- (statistical)
  does this help us learn from real-world, empirical data?
- (number theory)
  does this help us solve other math problems?

I only know examples in the second category. And that will have to be fine.

We learned a "proof" from a short article in Mathematics Magazine. Consider the function:

$$T : x \mapsto ax \pmod{p}$$

The orbits of T^p are either cycles of order p or a fixed point. Except, we don't know what those are. Instead we can draw on a square ($p = 5$):



There are three fixed points ●. The two white circles ○ count as half. For a total of four, one less than our $p = 5$.

We can count the fixed points of $T^5 : x \mapsto a^5 x$ and subtract off the fixed points of T. This number should be divisible by 5

$$5 \Big| a^5 - a$$

and this is an instance of Fermat's Little Theorem.

Can we get more mileage out of this proof. Eventually we find out there is more:

$$15 \Big| (a^5 - a)(a^3 - a)$$

and the Math Magazine proof has appeared several times from different people (in Math Magazine).

I got a feeling there was something about our decimal system. That if we chose an interesting enough T (the dynamical system) we can get more interesting polynomial identities.

References

(1) Iga, Kevin (2003), "**A Dynamical Systems Proof of Fermat's Little Theorem**", Mathematics Magazine, 76 (1): 48-51,