MATH 035
Penn State University
Dr. James Sellers

Handout: Fermat's Little Theorem

History

Fermat's Little Theorem, as it is now called, was first stated in a letter from Pierre de Fermat dated October 18, 1640 to his friend and confidant Frénicle de Bessy. As usual, Fermat did not prove his assertion, only stating:

> "Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long."
>
> One translation of this is the following: "And this proposition is generally true for all progressions and for all prime numbers; the proof of which I would send to you, if I were not afraid to be too long."

Euler first published a proof in 1736 in a paper entitled "Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio". We can actually see images from the original paper written by Euler by visiting the online Euler Archive. But before we go to that website to see the paper, let's see if we can "discover" Fermat's Little Theorem ourselves.

Calculations

Complete each of the following congruences by filling in the blanks with the least nonnegative residues in question:

$2^6 \equiv$ _____ $(\mathrm{mod}\, 7)$ $3^6 \equiv$ _____ $(\mathrm{mod}\, 7)$ $5^6 \equiv$ _____ $(\mathrm{mod}\, 7)$

$2^4 \equiv$ _____ $(\mathrm{mod}\, 5)$ $3^4 \equiv$ _____ $(\mathrm{mod}\, 5)$ $4^4 \equiv$ _____ $(\mathrm{mod}\, 5)$

$6^4 \equiv$ _____ $(\mathrm{mod}\, 5)$ $12^4 \equiv$ _____ $(\mathrm{mod}\, 5)$ $13^4 \equiv$ _____ $(\mathrm{mod}\, 5)$

$2^{10} \equiv$ _____ $(\mathrm{mod}\, 11)$ $7^{10} \equiv$ _____ $(\mathrm{mod}\, 11)$ $8^{10} \equiv$ _____ $(\mathrm{mod}\, 11)$

$5^{10} \equiv$ _____ $(\mathrm{mod}\, 11)$ $6^{10} \equiv$ _____ $(\mathrm{mod}\, 11)$ $9^{10} \equiv$ _____ $(\mathrm{mod}\, 11)$

$4^{12} \equiv$ _____ $(\mathrm{mod}\, 13)$ $5^{12} \equiv$ _____ $(\mathrm{mod}\, 13)$ $6^{12} \equiv$ _____ $(\mathrm{mod}\, 13)$

Given all the data you just generated, can you come up with a conjectured result?

OK, what if we try to wiggle this just a bit (and loosen the restrictions on the value of 'a')? Let's try a few examples:

Lastly, what if that nice exponent/modulus relationship is wiggled? Again, let's try a few examples:

Closing questions:

- Who cares? And why?

- What if the modulus isn't a prime?