Fermat's Little Theorem:

An Exploration Through History and Applications

Zak Basta

April 2014

Abstract

The purpose of this paper is to provide an *informal* look at both the history behind, and the wide array of applications of *Fermat's Little Theorem*. We will first talk a bit about the theorem, and then state it explicitly. Then, we will examine — at the undergraduate level — the prequisite material required for a basic understanding of the *Little Theorem*. Following that, we will go over the theorem in all possible detail for this level of study. Finally, we will briefly explore a few (of the many) fields in which *Fermat's Little Theorem* applies. As an endnote, we will also get an idea as to what the student should study next to acquire a deeper understanding of the subject matter.

0.1 Introduction to Fermat's Little Theorem

Fermat's Little Theorem is widely known throughout the mathematical community. However, Fermat's lack of proof left open the opportunity for Euler to come in and provide many. But — as the student may go learn independently — this turned out to be a good thing, as Euler's many proofs of Fermat led him to search for the smallest exponent that could be used in the original theorem while it retained it's veracity. Just one of the many ways in which this "little" theorem has proven useful to Fermat's mathematical contemporaries and successors.

As a standalone, the theorem provides insight into a sort of circular repetition that can, in turn, illuminate many other areas within this most logical of disciplines. One case of the famous *Chinese Hypothesis* (now since disproven in all other cases) is simply a reiteration of *Fermat's Little Theorem* using the number two. In fact, modular arithmetic — ironically so — is on the opposite side of the ring, so to speak, to the subject of this paper. The *Little Theorem* provides a mapping to modular arithmetic, which in turn provides a mapping back to the basis of the *Little Theorem*. And it just so happens that both concepts, while fundamentally related, do indeed cover different areas of mathematics, although they overlap in obvious places.

It would be obscene to tantalize the reader any further than this point without stating *Fermat's Little Theorem* once and for all.

Theorem 0.1. *If p is a prime number, and p does not divide the integer a, then a to the power of p minus 1 is congruent to 1 modulo p.*

Now that we've seen it in plain speak, let's see what it looks like in the universal language of Mathematics:

If p **is a prime number, and** $p \nmid a$**, then** $a^{p-1} \equiv 1 \bmod p$

This leads us directly into the next section in which we gain a practical understanding of the prequisite material to *Fermat's Little Theorem*.

0.2 Prerequisite Instruction

0.2.1 Modular Arithmetic

The basics of Modular Arithmetic seem to be — for many students — similar to that of Calculus, in that it takes a bit of learning in notation before one can understand what it means. As an aside, this is the most important thing in all of mathematics, but some areas have a lot more notation dedicated to their study than do others. But Mathematics is a language. And as such, one must learn the meanings of its symbols in order to read and speak it. So, to begin, let's look at the common structure of a modulo expression: $a \equiv b \bmod n$.

This is read as "a is **congruent** to b modulo n." What it actually *means* is that the difference between a and b $(a - b)$ is a multiple of n, and therefore n divides the difference between a and b. In putting all of the more precise mathematical language together, we get:

Definition 0.2. $a \equiv b \bmod n \iff n|a - b$ in which case, n is called the **modulus** of this particular congruence statement.

Modular arithmetic is perhaps more easily understood by viewing a diagram that shows it as a cycle. Below is a quick example of how you essentially circle around back to something that is congruent to your original number.

Another example displays how modular arithmetic is *crucial* to music theory. On a normal, modern guitar, moving up five frets on one string will give you a note congruent to the string below it when played without placing a finger on it. On a piano, moving up an octave is when you exhaust all of the notes in one area and come back around to C (or wherever you prefer to start counting from, I suppose). The basic structure of music notes are as follows: C, D, E, F, G, A, B, and back again to C, where we repeat the cycle, albeit at higher notes in terms of musicality,

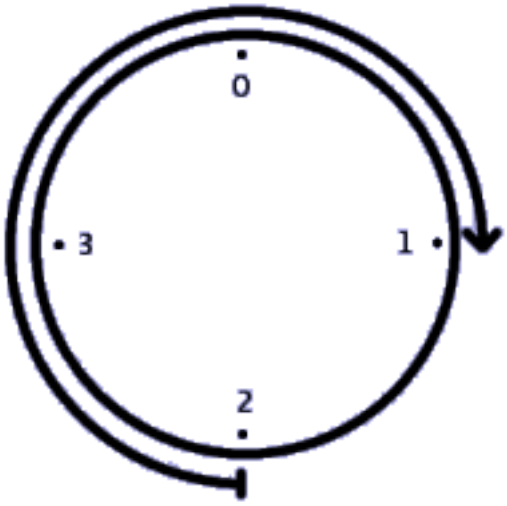

Figure 1: A Basic Modular Cycle (Mathematica.ludibunda. n.d.).

but each C is congruent to the Cs before and after, as are the Ds, Es, and so on. If you play an instrument, consider this paragraph while examining the diagram below:

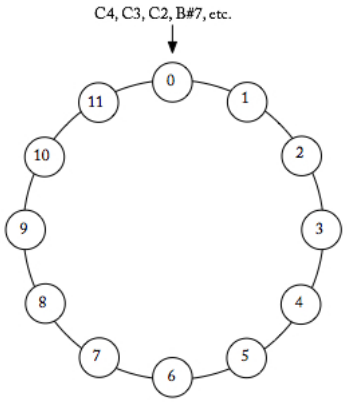

Figure 2: Music Thoery/Modular Arithmetic (futheory.briancmoseley. n.d.).

In short, there are two ways to simplify our definition of congruence within language. The first is to think of the modulus, n, as being the number which, when multiplied by some integer factor, will provide the difference between a and b. In

fact, this very *statement* is congruent with the mathematical one above that $n|a-b$.

The other simplification that can be made is one that's ultimately tied to the Euclidean Algorithm in that n is the number such that when it divides a and b separately, the solutions will have the same remainder. That is to say, the remainder of $\frac{a}{n}$ is equal to the remainder of $\frac{b}{n}$.

One needn't look far for the relation of *Fermat's Little Theorem* to Modular Arithmetic. It's actually right there in the theorem, itself. But since we shift things slightly when dealing with the *Little Theorem*, it should suffice for the student that we dissect and analyze the theorem now armed with basic modular arithmetic notation.

0.3 Examples and Proofs

0.3.1 A Step-by-Step analysis of the Theorem and First Examples

If p is a prime number, that is that only 1 and p divide p, and $p \not| a$, by which we mean that a is not an integer multiple of p, then $a^{p-1} \equiv 1 \bmod p$, which says that a multiplied by itself p minus 1 times is congruent to 1 modulo p. And of course, that last part being the most tasty morsel, we should explain it, as well. It takes a bit of doing if this is your first forray into modular arithmetic, but it can easily be done. So, if in basic modular arithmetic, $a \equiv b \bmod n$ means that the difference between a and b is divisible by n, then when we say $a^{p-1} \equiv 1 \bmod p$ we are saying that the difference between a^{p-1} and 1 is divisible by p. An equivalent statement being that $a^{p-1} - 1$ is divisible by $p \Rightarrow$ is an integer multiple of p. Or, by using the second simplification we developed above, if in modular arithmetic, $\frac{a}{n}$ and $\frac{b}{n}$ have

the same remainder, then in the *Little Theorem* $\frac{a^{p-1}}{p}$ will have the same remainder as $\frac{1}{p}$. Let's look at an example with numbers.

Example 0.3. 3 is prime, and 3 does not divide 2 $\Rightarrow 2^{3-1} = 2^2 \equiv 1 \bmod 3$. There are two conclusions we can draw from this immediately from the information contained above. Firstly, $2^2 = 4$, and $\frac{4}{3}$ has the same remainder as $\frac{1}{3}$. In plain English, 3 goes into 4 one time with a remainder of 1, while 3 goes into 1 zero times, but there's a remainder of 1 Secondly, the difference between a and b is still divisible by n, in that $\frac{a-b}{n} = \frac{4-1}{3} = \frac{3}{3} = 1 \Rightarrow a - b$ is an integer multiple of n.

We can continue on in this fashion:

$$3 \not| 4 \Rightarrow 4^{3-1} = 4^2 = 16 \equiv 1 \bmod 3$$

$$3 \not| 5 \Rightarrow 5^{3-1} = 5^2 = 25 \equiv 1 \bmod 3$$

In the case of the immediately previous examples, $\frac{16}{3} = 5$ remainder 1, and as you might have guessed, $\frac{b}{p}$ is going to stay at $\frac{1}{3}$. Similarly, $\frac{25}{3} = 8$ remainder 1, and things will be that way for every integer a that is not divisible by p.

However, when we get to an integer that p does divide, as we would have above in continuing onward to 6, *Fermat's Little Theorem* would not apply as it is explicitly stated within that p must be prime and p must not divide a. In this particular case, a would be 6, and the p that we were using was 3, which evenly divides 6, implying that it also divides 6^2. In such a case, $6^2 = 36 \equiv 0 \bmod 3$

Example 0.4. Let's consider $p = 5$. In this case, all of the integers will be congruent to either 0 mod 5, 1 mod 5, 2 mod 5, 3 mod 5, or 4 mod 5. In more precise language,

the integers will be congruent to 0 mod 5, 1 mod 5, all the way to $(p-1)$ mod 5. If we then consider the case where $a = 11$, and then multiply all of the congruence classes by a, then we end up with $0, 11, 22, 33$, and 44. We needn't regard the 0 congruence, though, as it would indicate that p in fact *does* divide a and therefore, *Fermat's Little Theorem* would not apply. But with this setup, my remainders when simplifying the a-multiplied congruence classes by mod5, I'll end up with remainders of $1, 2, 3$, and 4, respectively. This concept is important in order to better understand the following proof.

0.3.2 Analytical Proof

Proof. The student will assume that p is a prime number, and that $p \nmid a$.

For all $a \in \mathbb{Z}$, $a \equiv 0, 1, 2, 3, ..., (p-1) \bmod p$.

We will call this set X, and the elements in this set $r, s, ...$

Multiply all congruence sets (except 0 mod p) by a to get $a, 2a, 3a, ..., (p-1)a$.

First, let's try to suppose $r \cdot a \equiv 0 \bmod p$

Since $r \in X$, $r < p$.

And since $p \nmid a$, $p \nmid r \cdot a \Rightarrow r \cdot a \not\equiv 0 \bmod p$.

This shows that for all $a \in \mathbb{Z}$, $a \not\equiv 0 \bmod p$

Now let's examine two elements from the a-multiplied set of congruences, $r \cdot a$ and $s \cdot a$.

Since we do not consider the 0 mod p congruence, we know that $0 < r < p$, and $0 < s < p$. In this case, we want to show that $r \cdot a \not\equiv s \cdot a \bmod p$. In other words, we want to show that $\frac{r \cdot a}{p} \not\equiv \frac{s \cdot a}{p}$. We also want this to show that $p \nmid (r \cdot a) - (s \cdot a)$. These case requirements come straight from the definitions outlined above in both modular arithmetic and the theorem, itself. We will first look at the latter situation:

$$(r \cdot a) - (s \cdot a) = a(r - s)$$

$$p \not| (r \cdot a) - (s \cdot a) \iff p \not| a(r - s)$$

$$(AoPS.2012).$$

Due to the theorem and the fact that we are disregarding the 0 mod p congruences, we know that $p \not| a$. So our question that remains in this case is one in regard to whether or not $p|(r - s)$. So we again state that:

$$0 < r < p$$

$$0 < s < p$$

$$0 < s < p \Rightarrow -p < -s < 0$$

$$\vdots$$

$$0 < r < p \quad + \quad (-p < -s < 0)$$

$$\vdots$$

$$-p < r - s < p$$

$$\vdots$$

$$-p < r - s < p$$

$$\Rightarrow r - s > -p, \quad r - s < p$$

But since we know that r and s are distinct from one another, this cannot be congruent to 0 mod p, and therefore, $r - s$, although it is in between $-p$ and p, it is not *exactly* in the middle at 0, which would give us the 0 mod p congruence. This shows that $p \not| r - s$. What this shows is that our a-multiplied congruence set consists of

the same elements as the congruence set, itself, X.

$$X \equiv a(X)$$

$$\vdots$$

$$1, 2, 3, 4, ..., (p-1) \bmod p \equiv a, 2a, 3a, 4a, ..., (p-1)a$$

$$\vdots$$

$$(p-1)!a^{p-1} \equiv (p-1)! \bmod p$$

$$\vdots$$

$$a^{p-1} \equiv 1 \bmod p$$

□

0.3.3 Visual Intuition Into Fermat's Little Theorem

Consider the diagram below:

The necklaces above represent *Fermat's Little Theorem* just about as well as can be done visually. The way to understand this interpretation is to consider the following: The necklaces have p beads, and each bead is able to be colored in a different ways, or if you prefer, you have a options as to which bead color to use. So for our case above, we have $p = 3$, and $a = 2$. This yields a situation in which a^p is the number of "different" ways in which you can arrange the beads by color and placement on the necklace. The reason for my quotes around the word "different" will soon become apparent, especially if the reader permits him/herself to glance back at the original diagram above. Once you've arranged your beads in the way you want and affixed them to a ring of some kind (we're not really making necklaces here, so I don't care what material you use), you'll find two things out immediately.

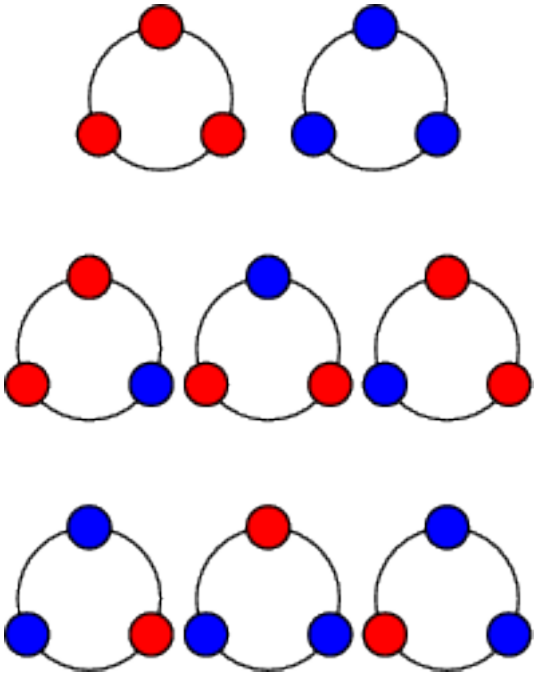

Figure 3: Beaded Necklaces in Two Colors. (AoPS. 2012).

First, you'll notice that — in exhausting all possible formations of the beads — you've created two monocolor necklaces — one all in the first color, and one all in the second. The next thing you'll notice is that, because these beads are strung together, and therefore held in their respective places in regard to one another, a certain number of rotations about the z-axis (the axis going straight through the hoop you've created) for each necklace will bring it back around to a spot where it looks identical to another (and in this case, another after that). In fact, in *any* case, the number of monocolor necklaces will be equal to a, the number of colors, and the amount of necklaces in each subgroup of rotationally identical (i.e. *congruent*) is equal to p. And so the most important element here is that, once you remove the necklaces that are made up of only a single color, or in other words, once you remove and amount of necklaces equal to a, then you are left with some number of sets that are made up of p elements. And for that in other words, you have a large group, G, the order of which is some integer, but the order of each subgroup

$(H_1, H_2, ...)$is equal to p. So you have $p(H_1, H_2, ...,)$. This is equal to p times the order of G, or $p([G])$. Now p obviously divides that. But remember that in order to get to G, we made a^p necklaces and subtracted a monocolred necklaces from that. So, for the key result:

$$p|a^p - a$$

(AoPS.2012).

In continuing the attempt at understanding this within group theory, we've discovered that, as long as p is prime, and p is the order of a subgroup, H, then there will be a number of subgroups separate from H within a larger group, G. Not only that, but it will take p rotations of each element in each subgroup before it comes back to its initial position, and there will be $(p-1)$ elements congruent to the aforementioned element, which is also the case for each other subgroup.

0.4 How We Use Fermat's Little Theorem Today, and the Future of the Result

Perhaps the most commonly known application of *Fermat's Little Theorem* in use today is the RSA public encryption system. Mathematicians and cryptographers Ron Rivest, Adi Shamir and Leonard Adleman published their algorithm in 1977. The basic concept is to use large prime numbers that are extremely difficult to make use of without proper knowledge of the RSA algorithm and its correlation to the *Little Theorem.* (Rivest. 1978). As the encryption process is public, the decryption process is kept secret in order to maintain the credibility and security of hte structure. This concept was also published by in an English mathematician named Clifford Cocks in 1973, but due to British Intelligence, it wasn't until 1997

that his result was declassified under national law.

Aside from that, *Fermat's Little Theorem* has widespread uses and consequences in the fields of Cloud computing, data servers, and it is also one of the fundamental results of Number Theory. Because of this, it definitely holds a secure placement in the future of theoretical mathematics, as well as the applied mathematics of computation and data enhancement.

Bibliography

[1] AoPS *The Art of Problem Solving – Fermat's Little Theorem* www.artofproblemsolving.com, Web. 2012

[2] Brian C. Moseley *Furman University Music Theory – Pitch* http://futheory.briancmoseley.com 2014

[3] Mathematica.ludibunda *mathematica.ludibunda– Smart Joe* http://mathematica.ludibunda.ch n.d.

[4] Paolo Ribenboim *The New Book of Prime Number Records.* Springer-Verlag, New York 3rd Edition, 1995.

[5] Rivest, R.; A. Shamir; L. Adleman *A Method For Obtaining Digital Signatures and Public-Key Cryptosystems.* Communications of the ACM. 1978