Scientific Research Publishing

Advances in Pure Mathematics, 2018, 8, 41-44
http://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

A Geometric Proof of Fermat's Little Theorem

Thomas Beatty, Marc Barry, Andrew Orsini

Florida Gulf Coast University, Fort Myers, USA
Email: tbeatty@fgcu.edu

How to cite this paper: Beatty, T., Barry, M. and Orsini, A. (2018) A Geometric Proof of Fermat's Little Theorem. *Advances in Pure Mathematics*, **8**, 41-44.
https://doi.org/10.4236/apm.2018.81004

Received: December 27, 2017
Accepted: January 21, 2018
Published: January 24, 2018

Abstract

We present an intuitively satisfying geometric proof of Fermat's result for positive integers that $a^{p-1} \equiv 1$ for prime moduli p, provided p does not divide a. This is known as Fermat's Little Theorem. The proof is novel in using the idea of colorings applied to regular polygons to establish a number-theoretic result. A lemma traditionally, if ambiguously, attributed to Burnside provides a critical enumeration step.

Keywords

Fermat, Carmichael Number, Group, Permutation, Burnside's Lemma, Action, Invariant Set, Orbit, Stabilizer, Coloring, Pattern, Prime, Regular Polygon, Cyclic Group

1. Historical Background

Pierre de Fermat wrote his friend Frénicle de Bessy in 1640 stating that he had discovered that $a^{p-1} \equiv 1$ for prime moduli p, provided p did not divide a, but his proof was overlong, so he did not bother to include the details. One might wish that Fermat had been more generous in recording his notes both in this instance and that famous "margin too small to contain··· (his proof of Fermat's *Last* Theorem)". Leibniz appears to have proved the theorem prior to 1683 without publishing it, and then Euler reprised Leibniz' work in a published version. This result, christened Fermat's Little Theorem by Kurt Hensel in 1913, is the basis for a convenient method for detecting primality, or more correctly, compositeness [1] [2] [3]. If p does not divide a and a^{p-1} is not congruent to $1 \bmod p$, then p must be composite. Modular arithmetic, particularly with the aid of a computer, makes short work of calculating the residues of high powers of a needed to check this condition. Unfortunately, the invalidity of the converse to Fermat's Little Theorem (if $a^{n-1} \equiv 1 \bmod n$ with a and n coprime, then n is prime) forces it to be used in a probabilistic way for detecting primality. If

$a^{n-1} \equiv 1 \bmod n$ for lots of different admissible choices of n, then it looks more and more like n is probably prime. But there are many a for which $a^{n-1} \equiv 1 \bmod n$ and yet n is composite. Such a are called "Fermat Liars" and the n that go with them are termed pseudoprimes to the base a. A pseudoprime to every base, and they do exist but are relatively rare, is called a Carmichael number. Carmichael numbers completely defeat the usefulness of the theorem as a primality test. There is certainly no shortage of simple proofs of Fermat's Little Theorem. It may be proved with a straightforward induction on the base a to show that $a^{p-1} - 1$ is divisible by p, or by using a modular arithmetic argument. We present a proof of this useful theorem from an intuitively appealing direction based on coloring the vertices of regular polygons with prime numbers of sides.

2. Burnside's Lemma [4]

If G is a group of permutations acting on a set S, then for a particular $\pi \in G$, the invariant set of π is the collection of all elements of S that are fixed points of π, *i.e.* $\pi(s) = s$. The orbit of some $s \in S$ is the collection of elements obtained by letting every permutation in G act on that s. Intuitively, there is a broad inverse size relationship between orbits and invariant sets. If most elements are not moved by most permutations, invariant sets will be large and orbits will be small, but more numerous. In 1897, the British mathematician William Burnside published the result, with attribution to Frobenius [5], that if G is a group of permutations acting on the finite set S, then the number of orbits of S under G is given by $\frac{1}{|G|}\sum_{\pi \in G} |inv(\pi)|$, where $|inv(\pi)|$ is the size of the invariant set of the permutation $\pi \in G$. Burnside's Lemma is a direct consequence of the Orbit/Stabilizer Theorem [1] [2] [3] and was known at least as early as Cauchy, hence it is sometimes called "the lemma that is not Burnside's" [6]. We will color the elements of S, specifically the vertices of a regular polygon with a prime number of sides, and adapt Burnside's/Not Burnside's Lemma to the problem of enumerating distinct colorings.

3. Colorings

A coloring χ is a mapping from the finite set S of objects to be colored to the finite set P, consisting of the "pallette" of colors. This is just a fanciful way of thinking about the rather dry notion of an arbitrary function between two finite sets. Colorings had their origin in the effort to establish the Four-Color Theorem, and they pop up in many seemingly unrelated combinatorial settings [7] [8]. If the group G of permutations shuffles the objects of S, then those permutations will likewise shuffle the possible colorings of S. So a given $\pi \in G$ can be regarded as a mapping from the set of P-colorings of S back to itself. More mathematically, there is a group of induced maps G^* that form an action on the set of colorings P^S. Each $\pi \in G$ gives rise to a companion mapping

$\pi^* \in G^*$ that determines what happens to the available colorings whenever the underlying objects in S are permuted by π. It is clear that G^* is a group with the same order as G.

Just as the elements of S can be put into equivalence classes on the basis of whether they are in the same orbit under the action of G or not, colorings can be put into equivalence classes depending on whether they are in the same orbit under the action of G^* or not. Orbits of colorings are called patterns. Two colorings χ_1 and χ_2 are equivalent, or represent the same pattern, if there is a $\pi \in G$ such that for all $s \in S$ we have $\chi_1(s) = \chi_2(\pi(s))$. For example, if $\chi_1(a) = \text{red}$, $\chi_1(b) = \text{white}$, and $\chi_1(c) = \text{blue}$, then if the permutation $\pi = (a \quad b \quad c) \in G$, χ_1 and χ_2 are equivalent provided $\chi_2(a) = \text{blue}$, $\chi_2(b) = \text{red}$, and $\chi_2(c) = \text{white}$. You can see that $\text{red} = \chi_1(a) = \chi_2(\pi(a)) = \chi_2(b)$, and so forth. We would write $\pi^*(\chi_1) = \chi_2$ to signify this situation.

4. Proof

If we have a symmetrical object with a coloring, we can apply Burnside's Lemma to enumerate the number of distinct patterns possible for the object. Let us consider a regular p-gon, where p is prime, and color the vertices with a pallette consisting of a colors, where p does not divide a. We will admit the digon to handle the case $p = 2$. Now we are not going to tear or fold the polygon, so the only permutations of colorings allowed are going to be those induced by the rotation group of the polygon, namely the cyclic group $\mathbb{Z}_p$. The invariant set of a particular π^* induced by an element of this group is easy to characterize. The zero rotation has a^p colorings fixed by it, namely the total number of possible paint jobs or mappings from the vertices to the pallette. Every non-zero element of $\mathbb{Z}_p$ carries each pure coloring (every vertex the same color) into itself, so there would be a such colorings fixed by the action of those rotations. But none of these $p-1$ non-zero rotations can carry a non-pure coloring back to itself due to the indivisibility of p. Burnside's Lemma then gives us the total count of possible distinct patterns as $\frac{1}{|G^*|}\sum_{\pi^* \in G^*} |inv(\pi^*)| = \frac{1}{p}\left(a^p + a(p-1)\right) = \frac{a}{p}\left(a^{p-1} + (p-1)\right)$. Evidently this is a positive integer, and since p does not divide a, it must divide $\left(a^{p-1} + (p-1)\right)$. But this means $\left(a^{p-1} + (p-1)\right) \equiv a^{p-1} - 1 \equiv 0 \bmod p$, which is Fermat's Little Theorem.

5. Conclusion

We have established Fermat's Little Theorem by coloring the vertices of a regular polygon and then finding the patterns that are stable under various rotations of the polygon. When the number of vertices is prime, the set of such invariant patterns is necessarily limited. This process lends itself to intuitively satisfying visualization. Burnside's Lemma then enumerates the relatively sparse

number of invariant patterns and gives a formula that is equivalent to the modular expression of Fermat's Little Theorem. An interesting further application of this idea would be to search for other number-theoretic results using colorings of more complicated geometric objects and more general pattern enumeration methods, for example Polya's Counting Theorem.

References

[1] Dummitt, D.S. and Foote, R.M. (2004) Abstract Algebra. 3rd Edition, John Wiley & Sons, Inc.

[2] Gallian, J.A. (2010) Contemporary Abstract Algebra. 7th Edition, Brooks-Cole.

[3] Rotman, J. (1995) An Introduction to the Theory of Groups. Springer-Verlag. https://doi.org/10.1007/978-1-4612-4176-8

[4] Burnside, W. (1897) Theory of Groups of Finite Order. Cambridge University Press, Cambridge.

[5] Frobenius, F.G. (1887) Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul. *Crelle's Journal*, 288.

[6] Neumann, P.M. (1979) A Lemma That Is Not Burnside's. *The Mathematical Scientist*, **4**, 133-141.

[7] Rosyida, I., Peng, J., Chen, L., Widodo, W., Indrati, Ch.R. and Sugeng, K.A. (2016) An Uncertain Chromatic Number of an Uncertain Graph Based on Alpha-Cut Coloring. *Fuzzy Optimization and Decision Making*, 1-21. https://doi.org/10.1007/s10700-016-9260-x

[8] Chen, L., Peng, J. and Ralescu, D.A. (2017) Uncertain Vertex Coloring Problem. *Soft Computing*. https://doi.org/10.1007/s00500-017-2861-7