Scientific Research Publishing

Advances in Pure Mathematics, 2024, 14, 797-805
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

Small Modular Solutions to Fermat's Last Theorem

Thomas Beatty

Department of Mathematics, Florida Gulf Coast University, Fort Myers, FL, USA
Email: tbeatty@fgcu.edu

How to cite this paper: Beatty, T. (2024) Small Modular Solutions to Fermat's Last Theorem. *Advances in Pure Mathematics*, **14**, 797-805.
https://doi.org/10.4236/apm.2024.1410044

Received: July 12, 2024
Accepted: October 28, 2024
Published: October 31, 2024

Abstract

The proof by Andrew Wiles of Fermat's Last Theorem in 1995 resolved the existence question for non-trivial solutions in integers x, y, z to the equation $x^n + y^n = z^n$ for $n > 2$. There are none. Surprisingly, there are infinitely many solutions if the problem is recast in terms of modular arithmetic. Over a hundred years ago Issai Schur was able to show that for any n there is always a sufficiently large prime p_0 such that for all primes $p \geq p_0$ the congruence $x^n + y^n \equiv z^n \pmod{p}$ has a non-trivial solution. Schur's argument was non-constructive, and there is no systematic method available at present to construct specific examples for small primes. We offer a simple method for constructing all possible solutions to a large class of congruences of this type.

Keywords

Fermat's Last Theorem, Modular Arithmetic, Congruences, Prime Numbers, Primitive Roots, Indices, Ramsey Theory, Schur's Lemma in Ramsey Theory

1. Introduction

We will call a congruence of the form $x^n + y^n \equiv z^n \pmod{p}$ for prime p a *modular Fermat equation (MFE)*. An MFE is non-trivial if no term is zero and we regard $x^n + y^n \equiv z^n \pmod{p}$ and $y^n + x^n \equiv z^n \pmod{p}$ .as the same solution. Some examples are $2^3 + 3^3 \equiv 7^3 \pmod{11}$, $7^5 + 12^5 \equiv 34^5 \pmod{37}$, $12^9 + 13^9 \equiv 17^9 \pmod{23}$ and even $3^{101} + 4^{101} \equiv 27^{101} \pmod{29}$. The reason this can occur so frequently with modular arithmetic can be understood by studying the bijectivity of the familiar function $\phi : \mathbb{Z}_p \to \mathbb{Z}_p$ given by $\phi(x, n, p) = x^n \bmod p$. This is not the Frobenius endomorphism, which would send an element of $\mathbb{Z}_p$ to its p^{th} power. Since the characteristic of $\mathbb{Z}_p$ is p the

Frobenius mapping would certainly be bijective, but we are interested in applying arbitrary n^{th} powers to the elements of $\mathbb{Z}_p$ and still retaining bijectivity. We assume $p \geq 3$. Even values of n interfere with the bijectivity of ϕ, so our discussion will be confined to odd $n \geq 3$. We also note in passing that every Pythagorean triple generates a solution to an MFE with $n = 2$.

Since $\phi(0, n, p) = 0$, we can limit our attention to the set $\mathbb{Z}_p^*$ of non-zero residues modulo p. If ϕ is bijective, then $\phi(\mathbb{Z}_p^*)$ returns a permuted copy of $\mathbb{Z}_p^*$ as the set of n^{th} power residues modulo p. It follows that for arbitrary $x, y \in \mathbb{Z}_p^*$, the sum $x^n + y^n \pmod p = \zeta$, where ζ is guaranteed to be another n^{th} power residue, say $\zeta = z^n \in \mathbb{Z}_p^+$. Then we have the MFE $x^n + y^n \equiv z^n \pmod p$. This matching process is essentially an application of the pigeonhole principle to the range of $\phi(x, n, p)$. For any sum of two n^{th} powers modulo p, there is a pigeon at home with that same address among the permuted n^{th} residues. We arbitrarily rule out $x = y$ as not being an (esthetically) proper solution. Also it is clear that if $x = z$ or $y = z$, then y or x, respectively, would be forced to be zero, violating non-triviality. Now if ϕ fails to be bijective, this guarantee is no longer assured, as ζ may not be among the n^{th} power residues. In the sequel we offer an example where the bijectivity of ϕ fails so drastically that no MFE can be constructed, and another where it fails only moderately but still allows the construction of an MFE. Our goal is to develop a criterion for (n, p) pairs that guarantees $\phi(x, n, p)$ is a bijection and will therefore support the formation of MFEs using the pigeonhole strategy.

2. Historical Note

In 1916 Issai Schur proved the combinatorial result known as Schur's Lemma in Ramsey Theory [1] [2]. This asserts that given a palette of k colors with $k \geq 2$, there is always an $n \geq 4$ such that a k-coloring of the set $\{1, 2, \cdots, n\}$ would yield a monochromatic triple $\{i, j, k\}$ satisfying the algebraic property $i + j = k$. As a corollary of this result he was able to show that Fermat's Last Theorem is false in the context of modular arithmetic. Specifically, he established that for any $n \geq 1$ there is a prime p_0 such that for all $p \geq p_0$ the equation $x^n + y^n \equiv z^n \pmod p$ has a solution. His proof is based on a Ramsey theory type argument which is summarized in [3]. As such, it is non-constructive, but it clarifies that for any n there are only finitely many moduli p for which an MFE cannot be constructed. It is not obvious that there is a general pattern among the (n, p) pairs for which this is true. Our focus is on the territory where $p < p_0$. Here solutions may or may not exist for specific (n, p) pairs. We develop a simple criterion that allows us to select those (n, p) pairs which guarantee that explicit solutions exist.

3. The Compatibility Criterion

A joint selection of n and p that assures the bijectivity of $\phi(x, n, p)$ will be called

compatible. We now turn to developing a practical criterion for identifying compatible (n, p) pairs. Before proving the general result we explore a motivating case with small n and p. Let $n=5$ and $p=13$. We have purposely chosen n and p such that $\gcd(n, p-1)=\gcd(5,12)=1$. Note that 2 is a primitive root of 13 and recall that the various powers of a primitive root for prime p generate the numbers 1 through $p-1$ in some order [4]. The index I of such a number is its logarithm with respect to the primitive root as a base. For example, since $2^4 \equiv 3 \pmod{13}$, the index $I_2(3)=4$.

Example 1 We construct Table 1 as follows for the purpose of finding all solutions to $x^5+y^5 \equiv z^5 \pmod{13}$. The elements x of $\mathbb{Z}_{13}^* = \{1,2,\cdots,12\}$ are listed in order in Column 1. Their respective fifth powers reduced modulo 13 are listed in Column 2. Note that the entries in Column 2 repeat all of the entries in Column 1 but in a different order. This is a consequence of the fact that $\phi(x,5,13)=x^5 \bmod 13$ is a permutation on $\mathbb{Z}_{13}^*$. In general this need not be the case for arbitrary n and p. Then Column 3 lists their respective indices relative to the primitive root 2 of 13. For example, if $x=5$, we have $2^9 \equiv 5 \pmod{13}$, so $I_2(5)=9$. Finally, in Column 4 we list the respective indices of the fifth powers of x, again relative to the primitive root 2 of 13. Recall that if $I_2(x)=k$, then $I_2(x^5)=5k \pmod{12}$, since indices are always reduced modulo $(p-1)$.

Table 1. $n=5$, $p=13$.

Column 1	Column 2	Column 3	Column 4
x	$x^5 \pmod{13}$	$I_2(x)$	$I_2(x^5) \pmod{12}$
1	1	0	0
2	6	1	5
3	9	4	8
4	10	2	10
5	5	9	9
6	2	5	1
7	11	11	7
8	8	3	3
9	3	8	4
10	4	10	2
11	7	7	11
12	12	6	6

Table 1 explains why there are many guaranteed solutions to $x^5+y^5 \equiv z^5 \pmod{13}$. To successfully use the matching strategy based on the pigeonhole principle described previously, we require that the fifth powers listed in Table 1, Column 2 be the numbers 1, 2, …, 12 in some order. Here is the chain of logic which shows this to be true in this case: The numbers 1, 2, …, 12 (Column 1) are given as distinct. Their respective indices relative to the primitive root 2 of 13 are distinct (Column 3) by the bijectivity of the index function (which is what

makes the primitive root primitive). The respective indices of the fifth powers (Column 4) are calculated in turn from the entries in Column 3 by the Discrete Logarithm Rule which states that $I_2\left(x^5\right)=5I_2\left(x\right)\left(\mathrm{mod}12\right)$. This rule is injective provided the $\gcd\left(5,12\right)=1$, which we confirm. Thus the entries in Column 4 are distinct. Finally, we again appeal to the bijectivity of the index function to conclude that the inverse mapping $I_2\left(x^5\right)\left(\mathrm{mod}12\right)\to x^5\left(\mathrm{mod}13\right)$ establishes that the entries in Column 2 are the distinct numbers 1, 2, …, 12 in some order.

Now that we have shown that the fifth powers modulo 13 are the complete set of positive least residues, we can easily build all non-trivial solutions to $x^5+y^5\equiv z^5\left(\mathrm{mod}13\right)$. Pick two different numbers from Column 1, say 5 and 11. Find their fifth powers modulo 13 in Column 2 and add. This gives 5 + 7 = 12. By the matching strategy we are guaranteed to find the number in Column 1 corresponding to 12 in Column 2. We conclude $5^5+11^5=12^5\left(\mathrm{mod}13\right)$. There are $\binom{12}{2}=66$ choices of two different numbers from Column 1, and each pair gives a distinct proper solution to $x^5+y^5\equiv z^5\left(\mathrm{mod}13\right)$.

We use a generalization of this argument to find a criterion for the compatibility of the pair $\left(n,p\right)$.

Theorem 1 *(Criterion for Compatible Powers and Primes)* Given $n\ge 3$ and p an odd prime, the function $\phi\left(x,n,p\right)=x^n\left(\mathrm{mod}\,p\right)$ permutes the set of residues $\left\{1,2,\cdots,p-1\right\}$ provided $\gcd\left(n,p-1\right)=1$. In particular, if x_1 and x_2 are not congruent modulo p, then neither are x_1^n and x_2^n.

Proof: Every prime has a primitive root, so let α be a primitive root of p. All indices will be calculated with respect to α. The elements x of $\mathbb{Z}_p^*=\left\{1,2,\cdots,p-1\right\}$ are listed in order in Table 2, Column 1. Their respective n^{th} powers reduced modulo p are listed in Column 2. Their respective indices relative to the primitive root α are listed in Column 3. Finally, the indices relative to α of their respective n^{th} powers are listed in Column 4, reduced modulo $\left(p-1\right)$.

Table 2. For Theorem 1.

Column 1	Column 2	Column 3	Column 4
x	$x^n\ (\mathrm{mod}p)$	$I_\alpha(x)$	$I_\alpha(x^n)\ (\mathrm{mod}(p-1))$
1	1	0	0
2	$2^n\ (\mathrm{mod}p)$	$I_\alpha(2)$	$nI_\alpha(2)$
3	$3^n\ (\mathrm{mod}p)$	$I_\alpha(3)$	$nI_\alpha(3)$
⋮	⋮	⋮	⋮
x_1	$x_1^n\ (\mathrm{mod}p)$	$I_\alpha(x_1)=r$	$I_\alpha(x_1^n)=rn$
⋮	⋮	⋮	⋮
x_2	$x_2^n\ (\mathrm{mod}p)$	$I_\alpha(x_2)=s$	$I_\alpha(x_2^n)=sn$
⋮	⋮	⋮	⋮
$(p-1)$	$(p-1)^n\ (\mathrm{mod}p)$	$I_\alpha(p-1)$	$nI_\alpha(p-1)$

Suppose x_1 and x_2 are distinct least residues modulo p from Column 1 but for the sake of contradiction their n^{th} powers are congruent modulo p in Column 2. So $x_1^n \equiv x_2^n \pmod{p}$. We know x_1 and x_2 are powers of the primitive root α, so suppose further that in Column 3 $I_\alpha(x_1) = r$ and $I_\alpha(x_2) = s$. It follows in Column 4 that $I_\alpha(x_1^n) = rn$ and $I_\alpha(x_2^n) = sn$. These two indices in Column 4 must be congruent modulo $(p-1)$. So we now have $rn \equiv sn(\bmod(p-1))$ which implies $(r-s)n \equiv 0(\bmod(p-1))$. By assumption, $\gcd(n, p-1) = 1$, and since $1 \le r, s \le p-1$, it must be the case that $(r-s) = 0$ and evidently $r = s$. This forces $x_1 \equiv \alpha^r = \alpha^s \equiv x_2$, which contradicts the assumption that x_1 and x_2 are distinct least residues modulo p. We conclude that x_1^n and x_2^n cannot be congruent modulo p, and the function $\phi(x, n, p) = x^n \pmod{p}$ is injective on the finite set $\mathbb{Z}_p^*$, and therefore bijective, as claimed. ■

This theorem establishes a sufficient condition for the bijectivity of $\phi(x, n, p)$, which, coupled with the matching strategy described above, allows the generation of explicit MFE's in the manner illustrated.

Corollary 1-1 There are infinitely many primes for which MFEs are constructible

Proof: There are infinitely many odd primes and for each odd prime p, we may factor $p-1$ into a product of primes to various powers according to the Fundamental Theorem of Arithmetic. Then we may choose any odd $n \ge 3$ that does not share any of the primes in this product. This construction will ensure $\gcd(n, p-1) = 1$ validating application of the theorem. We conclude there are infinitely many primes for which MFEs can be formed. ■

Of course, Schur's Theorem says the same thing, in fact it does so more inclusively since n need not be odd. But it offers no clue for constructing an example.

Corollary 1-2: Provided n and p are compatible, MFEs of the form $a^n + b^n \equiv c^n \pmod{p}$ with $0 < a, b < c < p$ exist.

Proof: Given $1^n + 2^n \equiv c^n$ we can always find $c \ge 3$. Otherwise we are forced to conclude either 1^n or $2^n = 0$. ■

This is purely an esthetic nod to the classical form of Pythagorean triples.

Corollary 1-3: If $a^n + b^n \equiv c^n \pmod{p}$, then

$(a + pi)^n + (b + pj)^n \equiv (c + pk)^n \pmod{p}$ for any triple $(i, j, k) \in \mathbb{N}_0^3$.

Proof: Note that $(a + pi)^n = \sum_{r=0}^{n} a^r (pi)^{n-r} \equiv a^n \pmod{p}$ and likewise for the other terms. ■

We have thus far dealt with compatible (n, p) pairs that have allowed construction of MFE solutions. We now briefly explore how incompatible (n, p) pairs can affect the existence of solutions.

4. Failed Bijectivity of ϕ

As indicated earlier, if $\gcd(n, p-1) > 1$ the set of n^{th} power residues modulo p

can shrink markedly from the full set $\mathbb{Z}_p^*$. Here is a catastrophic case where it is impossible to form any MFE's. Let $n=9$ and $p=13$, so $\gcd(9,12)=3$. We use the primitive root $x=2$ again and generate the powers and indices in Table 3.

Table 3. An unsuccessful case.

Column 1	Column 2	Column 3	Column 4
x	$x^9 \pmod{13}$	$I_2(x)$	$I_2(x^9) \pmod{12}$
1	1	0	0
2	5	1	9
3	1	4	0
4	12	2	6
5	5	9	9
6	5	5	9
7	8	11	3
8	8	3	3
9	1	8	0
10	12	10	6
11	8	7	3
12	12	6	6

It is readily apparent from Table 3, Column 2 above that the ninth powers of the integers 1, 2, …, 12 are not distinct modulo 13. The respective indices relative to the primitive root 2 are listed in Column 3, and the injectivity of the index function ensures that there are no repeated values. However, in Column 4 we observe a collapse of injectivity. This is caused by the fact that $\gcd(9,12)=3$. Since indices are computed modulo $(p-1)=12$ in this case, and $I_2(x^9)\equiv 9I_2(x)\pmod{12}$, we see the values of $I_2(x^9)$ repeating in cycles whenever $9I_2(x)$ equals a multiple of 12. Table 4 makes the pattern obvious. Row 1 lists the indices of the various elements of $\mathbb{Z}_{13}^*$ *in the order of increasing index*. Row 2 lists the indices of the corresponding ninth powers.

Table 4. Cyclic indices for x^9.

$I_2(x)$	1	2	3	4	5	6	7	8	9	10	11	12
$I_2(x^9)$	9	6	3	0	9	6	3	0	9	6	3	0

It is easy to see what goes wrong. If 9 (=n) and 12 (=$p-1$) were coprime there would only be one cycle terminating when $I_2(x)=12$. The repeating cycles have length $\frac{p-1}{\gcd(n,p-1)}=\frac{12}{3}=4$ in this example. It follows again from the injectivity of the index function that the corresponding ninth power residues must repeat in the same pattern as their indices. We are left with only $\{1,5,8,12\}$ as the set of

distinct ninth power residues modulo 13. By inspection it is clear that the matching strategy completely fails with only the numbers in this set available. We conclude that there is no admissible solution to an MFE of the form $x^9 + y^9 \equiv z^9 \pmod{13}$. The general result follows.

Theorem 2 (*Counting Distinct n^{th} Power Residues Modulo p*) With the usual notation, the population of distinct n^{th} power residues modulo p is $\dfrac{p-1}{\gcd(n, p-1)}$.

Proof: Referring again to Table 2 above (used to prove Theorem 1), suppose α is a primitive root of p. Suppose further that x_1 and x_2 are two distinct least residues modulo p with $x_1 = \alpha^i$ and $x_2 = \alpha^j$. We claim that if i and j differ by the integer $\dfrac{p-1}{\gcd(n, p-1)} = m$, then $x_1^n = x_2^n$. Assuming $i > j$ we can write $I(\alpha^i) - I(\alpha^j) = i - j = m$. Then $I(\alpha^{ni}) - I(\alpha^{nj}) = ni - nj = n(i-j) = nm$. This is certainly a multiple of $(p-1)$, and it follows that $I(\alpha^{ni}) - I(\alpha^{nj}) \equiv 0 \bmod (p-1)$. We conclude $I(\alpha^{ni}) \equiv I(\alpha^{nj}) \pmod{(p-1)}$, and since $0 \le I(\alpha^{ni}), I(\alpha^{nj}) < (p-1)$, we have $I(\alpha^{ni}) = I(\alpha^{nj})$, which by injectivity of the index mapping implies $x_1^n = x_2^n$, establishing the claim. So the n^{th} powers repeat in cycles of length $\dfrac{p-1}{\gcd(n, p-1)}$ and obviously there can only be $\dfrac{p-1}{\gcd(n, p-1)}$ distinct n^{th} power residues modulo p. ■

Intuitively, we might suspect that the larger $\gcd(n, p-1)$ is relative to p, the less likely it would be that the population of n^{th} power residues can support construction of MFEs by the matching strategy. Here is an example where $\gcd(n, p-1) > 1$ but corresponding MFEs exist. Let $n = 5$ and $p = 31$. So $\gcd(5, 30) = 5$. By Theorem 2 we would expect to find a fairly thin subset of six fifth power residues, and we easily determine that set to be $\{1, 5, 6, 25, 26, 30\}$. There are several matches we can make with this reduced set, unlike the earlier case for $n = 9$ and $p = 13$. For example, 1 + 5 = 6, 1 + 25 = 26, and 5 + 25 = 30. Now $\mathbb{Z}_{31}^*$ can be partitioned into six equivalence classes where the elements within a class have equal 5th power residues modulo 31, namely the six distinct residues above. Each equivalence class has five members so there are apparently 375 distinct MFEs that can assembled from the three previous addition formulas. This clashes with our intuition. Only a fifth of $\mathbb{Z}_{31}^*$ is available for piecing together fifth power MFEs, while a third of $\mathbb{Z}_{13}^*$ is available for assembling ninth power MFEs. The smaller fraction leads to a profusion of MFEs, yet the larger fraction leads to none. Our sufficiency condition of Theorem 1 is far from being necessary.

The constraint we have presented on the number of n^{th} power residues for a given prime p interacts with Schur's Theorem in an interesting way. It may happen that an incompatible (n, p) pair may have $n = \dfrac{p-1}{2}$. Then $\gcd(n, p-1) = n$

which implies there are $\frac{p-1}{n}=2$ n^{th} power residues modulo p. The only non-trivial MFEs that could be formed under these circumstances would be of the "improper" form $x^n+x^n\equiv y^n \pmod p$. Recalling Schur's Theorem which states that there are solutions to $x^n+y^n\equiv z^n \pmod p$ for any n and all primes p exceeding some threshhold p_0, we remark that cases could be constructed where $\gcd(n,p-1)=n$. This implies that the MFEs guaranteed by Schur's theorem would necessarily be of the improper type.

5. Beyond MFEs

Finally, we note that the matching construction described above allows considerable extension [5] of the basic modular Fermat equation $x^n+y^n\equiv z^n \pmod p$. As long as the function $\phi(x,n,p)$ is bijective, the matching strategy will work and equations like $\left(\sum_{i=1}^{N-1}x_i^n=x_N^n\right)\pmod p$ will have solutions. For example, $2^3+3^3+4^3\equiv 10^3 \bmod 17$. We can also extend this by changing terms to their additive inverses relative to p and then moving them to the other side of the equation. Since $4\equiv -13 \bmod 17$, the previous example can be written $2^3+3^3-13^3\equiv 10^3 \bmod 17$ and rearranged to $2^3+3^3\equiv 10^3+13^3 \bmod 17$. The odd parity of admissible n always permits this.

6. Summary

It has long been established by a non-constructive argument that the modular version of Fermat's Last Theorem is false. Evidently solutions do exist for any exponent n and all sufficiently large prime moduli $p\geq p_0$, where p_0 is a threshhold implied by Schur's Theorem. However, there does not appear at present to be an efficient and transparent method for constructing solutions for small prime moduli. We have furnished this for a large class of compatible exponent/modulus pairs. Moreover, we have outlined directions for application of the method to additional modular Fermat-like equations.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Schur, I. (1916) Über die Kongruenz $x^m+y^m\equiv z^m \bmod p$, Jahresbericht der Deutschen Mathematiker-Vereinigung, 114-116. (European Mathematics Digital Library)

[2] Steed, M. (2015) Some Theorems and Applications of Ramsey Theory. University of Chicago Press, Chicago.

[3] Fox, J. and Sudakov, B. (2008) Induced Ramsey-type Theorems. *Advances in Mathematics*, 1771-1800.

[4] Hardy, G.H. and Wright, E.M. (1979) An Introduction to the Theory of Numbers.

Clarendon Press, Oxford

[5] Silverman, J.H. (2001) A Friendly Introduction to Number Theory. Prentice Hall, Upper Saddle River.