INTEGERS THAT SATISFY A FERMAT'S CONGRUENCE OF HIGHER POWER

GLENN J. FOX

In memory of William R. Alford

ABSTRACT. We consider positive integers n that satisfy congruences of the form $a^{n-1} \equiv 1 \pmod{n^m}$, where a and m are integers with $(a, n) = 1$, $|a| > 1$, and $m \geq 2$.

1. INTRODUCTION

Fermat's little theorem states that any prime number p must satisfy $a^{p-1} \equiv 1 \pmod{p}$ for any integer a with $(a, p) = 1$. A generalization of this congruence, applying to prime and composite integers, is known as Euler's theorem, which states that any positive integer n must satisfy $a^{\phi(n)} \equiv 1 \pmod{n}$ for any integer a with $(a, n) = 1$. Here, ϕ denotes Euler's phi function, for which $\phi(n)$ yields the number of integers in the set $\{1, 2, \ldots, n\}$ that are relatively prime to n.

If we replace the prime number p in Fermat's little theorem with a positive composite integer n so that $a^{n-1} \equiv 1 \pmod{n}$ with $(a, n) = 1$, then this congruence is not true in general, although it can hold for some values of n, given a. However, when $|a| \neq 1$, such occurrences appear to be fairly rare in comparison with the frequency of occurrence of the prime numbers. Thus, the fulfillment of this congruence is often used as an initial test of primality for a large integer because it is inexpensive to implement this test, with respect to time and memory. Any positive composite integer n that satisfies this congruence is known as a Fermat pseudoprime, or, more commonly, a pseudoprime to the base a.

For integers a and n, with $(a, n) = 1$ and $|a| > 1$, we refer to a congruence of the form $a^{n-1} \equiv 1 \pmod{n}$ as a Fermat's congruence to the base a.

A Wieferich prime to the base a is a prime number p for which $a^{p-1} \equiv 1 \pmod{p^2}$. For $|a| \neq 1$, such primes are observed to be extremely rare, especially as p increases. However, a heuristic argument indicates that there may be infinitely many Wieferich primes for a given base a (see [2]). A more prominant result about Wieferich primes concerns the first case of Fermat's last theorem, which states that there exist no integers x, y, z with $x^p + y^p + z^p = 0$, where p is an odd prime and $(xyz, p) = 1$. If the first case of Fermat's last theorem is false for the prime exponent p, then it has been proven that p must be a Wieferich prime to the base 2 [7]. A number of similar results, corresponding to additional bases, have been proven by others. Another result, involving Wieferich primes, addresses the divisibilty properties of Mersenne numbers. If n is a positive integer, then a number of the form $2^n - 1$ is known as a Mersenne number. When n is prime, the Mersenne number $2^n - 1$ must be a prime number or a Fermat pseudoprime to the base 2. If a Mersenne number is divisible by the square of a prime, then that prime number must be a Wieferich prime to the base 2 [6].

For integers $m > 2$, there is no particular name given for primes p that satisfy the congruence $a^{p-1} \equiv 1 \pmod{p^m}$, where a is an integer with $(a, p) = 1$ and $|a| > 1$. If a prime number satisfies this congruence for a particular positive integer m, then it must also satisfy it for any

smaller positive integer. Thus, we would expect the number of prime numbers that satisfy such a congruence to decrease as the exponent of the modulus increases. For any $a \neq 0$, there are infinitely many prime numbers p that satisfy $a^{p-1} \equiv 1 \pmod{p}$, as the only restriction on such prime numbers is that $(a, p) = 1$. However, for $|a| > 1$, it has not been proven whether or not there are infinitely many prime numbers that satisfy $a^{p-1} \equiv 1 \pmod{p^m}$ for any $m > 1$. By observation, the occurrence of such primes has been found to be less frequent as m or p increase.

If a prime p satisfies a congruence of the form $a^{p-1} \equiv 1 \pmod{p^m}$, where a and m are integers with $(a, p) = 1$, $|a| > 1$, and $m \geq 1$, then we shall say that p satisfies a Fermat's congruence to the base a of power m.

Example 1.1. For prime numbers that satisfy a Fermat's congruence of higher power, note that 1093 satisfies $2^{1093-1} \equiv 1 \pmod{1093^2}$, 1889 satisfies $13275^{1889-1} \equiv 1 \pmod{1889^3}$, 59 satisfies $11550^{59-1} \equiv 1 \pmod{59^4}$, and 7 satisfies each of $1353^{7-1} \equiv 1 \pmod{7^5}$ and $1354^{7-1} \equiv 1 \pmod{7^5}$.

For certain integer bases a, with $|a| > 1$, there are also positive composite integers n that satisfy $a^{n-1} \equiv 1 \pmod{n^m}$ for some integer $m > 1$. Because $a^{n-1} \equiv 1 \pmod{n^m}$ implies that $a^{n-1} \equiv 1 \pmod{n}$, it is necessary that any composite integer n that satisfies this congruence of higher order must also be a Fermat pseudoprime to the base a.

If a positive integer n satisfies a congruence of the form $a^{n-1} \equiv 1 \pmod{n^m}$, where a and m are integers with $(a, n) = 1$, $|a| > 1$, and $m \geq 2$, then we shall say that n satisfies a Fermat's congruence to the base a of power m.

Example 1.2. For Fermat pseudoprimes that satisfy a Fermat's congruence of higher power, note that $1026787777 = 17 \cdot 37 \cdot 97 \cdot 16829$ satisfies $46663^{1026787777-1} \equiv 1 \pmod{1026787777^2}$, $969 = 3 \cdot 17 \cdot 19$ satisfies $13717^{969-1} \equiv 1 \pmod{969^3}$, and $15 = 3 \cdot 5$ satisfies $8749^{15-1} \equiv 1 \pmod{15^4}$.

In an effort to characterize the properties of those positive composite integers n that satisfy a Fermat's congruence of higher power, we have derived the following equivalent condition.

Theorem 1.3. *Let a, m, and n be integers with $(a, n) = 1$, $|a| > 1$, $n > 1$, and $m \geq 1$. Then $a^{n-1} \equiv 1 \pmod{n^m}$ if and only if for each prime divisor p of n, there exists a positive integer g_p, with $g_p | (p-1, n-1)$, such that $a^{g_p} \equiv 1 \pmod{p^{mk}}$, where k is a positive integer with $p^k || n$.*

Here, we are using the notation $p^k \,||\, n$ to indicate that $p^k \mid n$ but $p^{k+1} \nmid n$.

Example 1.4. We have seen that $969 = 3 \cdot 17 \cdot 19$ satisfies $13717^{969-1} \equiv 1 \pmod{969^3}$. By the results of Theorem 1.3, we know that this is equivalent to the following: for the prime divisor $p = 3$, there exists an integer $g_3 | (3 - 1, 969 - 1) = 2$, 2 has factors 1 and 2, and $13717^1 \equiv 13717^2 \equiv 1 \pmod{3^3}$, so we can take either $g_3 = 1$ or $g_3 = 2$; for the prime divisor $p = 17$, there exists an integer $g_{17} | (17 - 1, 969 - 1) = 8$, 8 has factors 1, 2, 4, and 8, and $13717^4 \not\equiv 13717^8 \equiv 1 \pmod{17^3}$, so we take $g_{17} = 8$; and for the prime divisor $p = 19$, there exists an integer $g_{19} | (19 - 1, 969 - 1) = 2$, 2 has factors 1 and 2, and $13717^1 \not\equiv 13717^2 \equiv 1 \pmod{19^3}$, so we take $g_{19} = 2$.

Note that this result correlates a congruence on a positive composite integer n with a collection of congruences—one for each distinct prime divisor of n. As a result of this, we can obtain a characterization of those prime numbers that can divide n, and thus, increase the efficiency of deriving such integers.

2. Pseudoprimes and Fermat's Congruences of Higher Power

There is no apparent special property, independent of the base a, concerning whether or not a positive composite integer n satisfies $a^{n-1} \equiv 1 \pmod{n^m}$. Each positive composite integer satisfies such a congruence for some base. If n is a positive composite integer, then n satisfies $(n^m+1)^{n-1} \equiv 1 \pmod{n^m}$, which has base $a = n^m + 1$.

Before we prove our main result, we will need the following lemma.

Lemma 2.1. *Let a, n, r, and s be integers with $(a,n) = 1$ and n positive. $a^r \equiv 1 \pmod{n}$ and $a^s \equiv 1 \pmod{n}$ if and only if $a^g \equiv 1 \pmod{n}$, where $g = (r,s)$.*

Proof. The necessary condition: Let $g = (r,s)$. Then, there exist integers x and y such that $g = rx + sy$. Therefore, $a^g = a^{rx+sy} = (a^r)^x (a^s)^y \equiv 1 \pmod{n}$.

The sufficient condition: Because $g = (r,s)$, we see that there exist integers b and c such that $r = bg$ and $s = cg$. Therefore, $a^r = (a^g)^b \equiv 1 \pmod{n}$ and $a^s = (a^g)^c \equiv 1 \pmod{n}$. □

We now present the proof of our main result.

Proof. Let a, m, and n be integers with $(a,n) = 1$, $|a| > 1$, $n > 1$, and $m \geq 1$.

The necessary condition: Suppose that $a^{n-1} \equiv 1 \pmod{n^m}$. If p is a prime divisor of n and if k is a positive integer such that $p^k || n$, then $a^{n-1} \equiv 1 \pmod{p^{mk}}$. By Euler's theorem, we also have $a^{p^{mk-1}(p-1)} \equiv 1 \pmod{p^{mk}}$, because $\phi(p^{mk}) = p^{mk-1}(p-1)$.

Let $g_p = (p^{mk-1}(p-1), n-1)$. Because $(p, n-1) = 1$, this simplifies to $g_p = (p-1, n-1)$. Note that g_p must be positive, and by Lemma 2.1, $a^{g_p} \equiv 1 \pmod{p^{mk}}$.

The sufficient condition: Now suppose that for each prime divisor p of n, there exists a positive integer g_p with $g_p | (p-1, n-1)$ such that $a^{g_p} \equiv 1 \pmod{p^{mk}}$, where k is a positive integer with $p^k || n$. Because $g_p | (n-1)$, we can raise each side of this congruence to the integer power $(n-1)/g_p$ to obtain $a^{n-1} \equiv 1 \pmod{p^{mk}}$. The powers p^k are pairwise relatively prime, and because they collectively multiply to make n, we obtain $a^{n-1} \equiv 1 \pmod{n^m}$. □

Now, examine how Theorem 1.3 may be applied to determine those composite integers n that satisfy $a^{n-1} \equiv 1 \pmod{n^m}$, when a and m are integers with $|a| > 1$ and $m \geq 1$.

Corollary 2.2. *Let a, m, and n be integers with $(a,n) = 1$, $|a| > 1$, $n > 1$, and $m \geq 1$. If $a^{n-1} \equiv 1 \pmod{n^m}$, then for each prime divisor p of n, $a^{p-1} \equiv 1 \pmod{p^{mk}}$, where k is a positive integer with $p^k || n$.*

Proof. Let p be a prime divisor of n, and let a and m be integers with $(a,n) = 1$, $|a| > 1$, and $m \geq 1$, such that $a^{n-1} \equiv 1 \pmod{n^m}$. From Theorem 1.3, there exists an integer g_p, with $g_p | (p-1, n-1)$, such that $a^{g_p} \equiv 1 \pmod{p^{mk}}$, where k is a positive integer with $p^k || n$. Thus, $g_p | (p-1)$ and $a^{g_p} \equiv a^{p-1} \equiv 1 \pmod{p^{mk}}$. □

Example 2.3. The converse of this is not true, in general. In the case of $a = 82$ and $n = 15 = 3 \cdot 5$, we have $82^{3-1} \equiv 1 \pmod{3^2}$ and $82^{5-1} \equiv 1 \pmod{5^2}$. However, $82^{15-1} \equiv 199 \not\equiv 1 \pmod{15^2}$.

Example 2.4. For the base $a = 82$, the only prime numbers $p < 2^{32}$ that satisfy $82^{p-1} \equiv 1 \pmod{p^r}$, for $r > 1$, are the prime numbers 3 and 5, in which case the prime 3 satisfies this congruence for $r = 2$, 3, and 4, and the prime 5 satisfies this congruence for $r = 2$. Neither 3 nor 5 satisfy this congruence for larger corresponding values of r. Now, suppose that n is a positive composite integer, and that $82^{n-1} \equiv 1 \pmod{n^2}$. Note that Corollary 2.2 implies that if p is a prime such that $p^k || n$, then it must be true that $82^{p-1} \equiv 1 \pmod{p^{2k}}$. Thus, $3^k | n$ implies that $k \leq 2$, and $5^k | n$ implies that $k \leq 1$. Therefore, the only integers n that could

possibly be Fermat pseudoprimes to the base 82, having prime factors less than 2^{32}, and that satisfy $82^{n-1} \equiv 1 \pmod{n^2}$ consist of the composite integers $9 = 3^2$, $15 = 3 \cdot 5$, and $45 = 3^2 \cdot 5$. Of these, only 9 and 45 actually satisfy $82^{n-1} \equiv 1 \pmod{n^2}$. None of these three can satisfy $82^{n-1} \equiv 1 \pmod{n^3}$.

By letting $n = p^k$, k a positive integer in Theorem 1.3, we obtain a divisibility property of Fermat pseudoprimes to the base a.

Corollary 2.5. *Let p be a prime number, and let a and m be integers, with $(a, p) = 1$, $|a| > 1$, and $m \geq 1$. $a^{p^k-1} \equiv 1 \pmod{p^{mk}}$ if and only if $a^{p-1} \equiv 1 \pmod{p^{mk}}$, where k is a positive integer.*

Thus, p^k satisfies a Fermat's congruence to the base a of power mk if and only if p satisfies a Fermat's congruence to the base a of power mk.

For the case of $k = 2$ and $m = 1$, we find that p^2 is a pseudoprime to the base a if and only if p is a Weiferich prime to the base a.

Example 2.6. The only prime numbers p that satisfy $2^{p-1} \equiv 1 \pmod{p^2}$, that are less than the bound 6.7×10^{15}, are the primes 1093 and 3511 (see [3]). Thus, by Corollary 2.5, any Fermat pseudoprime to the base 2, having all of its prime factors less than 6.7×10^{15}, must be square-free, except for those that have 1093^2 or 3511^2 as a divisor, in which case these would be the only divisors that consist of the square of a prime. Note that the smallest Fermat pseudoprime to the base 2 that has 1093^2 as a divisor is $1194649 = 1093^2$, and the smallest such pseudoprime that has 3511^2 as a divisor is $12327121 = 3511^2$. The smallest Fermat pseudoprime to the base 2 that has both 1093^2 and 3511^2 as divisors is the integer $45786271241569458 61 = 29 \cdot 71 \cdot 151 \cdot 1093^2 \cdot 3511^2$. Because neither 1093 nor 3511 satisfy $2^{p-1} \equiv 1 \pmod{p^3}$, there can be no Fermat pseudoprimes to the base 2 that have divisors that consist of the cube of a prime for any prime that is less than 6.7×10^{15}.

3. The Expected Number of Integers that Satisfy a Fermat's Congruence of a Given Power

We modify and extend a heuristic argument found in [2].

Let p be prime, and let n and t be positive integers. In [4, p. 55], we find the following result:

If $e = (t, p^{n-1}(p-1))$, then the congruence $x^t \equiv 1 \, (mod\ p^n)$ will have e different roots. (3.1)

Consider now, the expected number of occurrences of positive composite integers n consisting of a power of a prime p, $n = p^k$, where k is an integer with $k > 1$, satisfying $a^{n-1} \equiv 1 \pmod{n^m}$, where a is a random integer with $(a, n) = 1$, $|a| > 1$, and m is a positive integer. We can obtain an upper bound on the expected number ${N_a}^{(mk)}$ of such composite integers n by summing the probability that $n = p^k$ satisfies this congruance for each possible prime p:

$$ {N_a}^{(mk)} = \sum_{\substack{p \text{ prime} \\ (a,p)=1}} Pr\left(a^{p^k-1} \equiv 1 \ \left(\text{mod } (p^k)^m\right)\right). $$

By Theorem 1.3, we know that $a^{p^k-1} \equiv 1 \pmod{p^{mk}}$ if and only if $a^{g_p} \equiv 1 \pmod{p^{mk}}$, where $g_p | (p^k - 1, p - 1) = p - 1$. Therefore, for the congruence $a^{g_p} \equiv 1 \pmod{p^{mk}}$, the value e from (3.1) is given by $e = (g_p, p^{mk-1}(p-1)) = g_p$, and

$$ {N_a}^{(mk)} = \sum_{\substack{p \text{ prime} \\ (a,p)=1}} Pr\left(a^{g_p} \equiv 1 \pmod{p^{mk}}\right) = \sum_{\substack{p \text{ prime} \\ (a,p)=1}} \frac{g_p}{p^{mk}}. $$

Now, $g_p|(p-1)$, so that $g_p \leq p-1$, and

$$N_a{}^{(mk)} \leq \sum_{\substack{p \text{ prime} \\ (a,p)=1}} \frac{p-1}{p^{mk}},$$

with this sum diverging when $mk \leq 2$ and converging for all integers $mk > 2$. Because $m > 0$ and $k > 1$, this implies that the sum diverges when $m = 1$ and $k = 2$, and that it converges whenever $m \geq 2$ or whenever $k \geq 3$.

Therefore, we would expect up to infinitely many composite integers n consisting of the square of exactly one prime factor, satisfying $a^{n-1} \equiv 1 \pmod{n^m}$, where a is a random integer with $(a, n) = 1$, $|a| > 1$, and $m = 1$. If $m \geq 2$, we would expect only finitely many such n. Also, if $n = p^k$ for some prime p and some integer $k > 2$, then we would expect only finitely many n such that $a^{n-1} \equiv 1 \pmod{n^m}$ for any integer $m > 0$.

Recall, from Corollary 2.5, that $a^{p^k-1} \equiv 1 \pmod{p^{mk}}$ if and only if $a^{p-1} \equiv 1 \pmod{p^{mk}}$, whenever a is an integer with $(a, p) = 1$, $|a| > 1$, p is prime, and m and k are positive integers. Therefore, we expect up to infinitely many prime numbers p such that $a^{p-1} \equiv 1 \pmod{p^k}$, whenever $k = 2$, and only finitely many prime numbers p such that $a^{p-1} \equiv 1 \pmod{p^k}$, whenever $k > 2$.

Now, suppose that n is a composite integer of the form $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, where $p_1, p_2, \ldots, p_r$ are prime numbers, with $p_i \neq p_j$, and k_1, k_2, …, k_r are positive integers. We define the integer s as the product of those prime divisors p_i of n that have greatest power 1:

$$s = \prod_{\substack{p_i|n \\ k_i=1}} p_i,$$

and the integer $b = n/s$, so that

$$b = \prod_{\substack{p_i|n \\ k_i>1}} p_i^{k_i}.$$

Then $n = sb$, $(s, b) = 1$, and s is square-free. Note that if p is prime and if $p|b$, then $p^e|b$ for some integer $e \geq 2$. If n is such that $a^{n-1} \equiv 1 \pmod{n^m}$, where a is a random integer with $(a, n) = 1$, $|a| > 1$, and m is an integer with $m \geq 2$, then, for $m = 2$, we would expect the existence of up to infinitely many primes that can be used to produce an integer with the same factorization structure as s (square-free – the product of a finite number of distinct primes), and we would expect the existence of only finitely many primes that can be used to produce an integer with the same factorization structure as b (the product of a finite number of distinct prime powers, where the powers are each at least 2). If $m > 2$, then we would expect the existence of only finitely many primes that can be used to produce an integer with the same factorization structure as n.

4. Generating Pseudoprimes that Satisfy a Fermat's Congruence of Higher Power

Because of the results given in Corollary 2.2, once the Wieferich primes that correspond to a given base have been found, we have an efficient method for searching for pseudoprimes n that satisfy $a^{n-1} \equiv 1 \pmod{n^m}$, given a and $m \geq 2$.

(1) The prime numbers p that satisfy $a^{p-1} \equiv 1 \pmod{p^2}$, up to a bound B, must be generated: p_1, p_2, …, p_r, with r a nonnegative integer.
(2) For each $i = 1, 2, \ldots, r$, find those prime numbers p_i for which $a^{p_i-1} \equiv 1 \pmod{p_i^m}$. List these as q_1, q_2, …, q_s, where s is a nonnegative integer with $s \leq r$.

(3) For each $i = 1, 2, \ldots, s$, the largest integer k_i for which $a^{q_i - 1} \equiv 1 \pmod{q_i^{mk_i}}$ must be found.
(4) Each composite integer of the form $n = q_1^{e_1} q_2^{e_2} \cdots q_s^{e_s}$, where e_i is an integer with $0 \leq e_i \leq k_i$, for $i = 1, 2, \ldots, s$, must be generated and checked to see if it satisfies the Fermat's congruence $a^{n-1} \equiv 1 \pmod{n^m}$.

If all primes p satisfying $a^{p-1} \equiv 1 \pmod{p^2}$ are known, up to a given bound B, then this method can be used to generate all pseudoprimes n satisfying $a^{n-1} \equiv 1 \pmod{n^m}$ up to $p_1 B$, where p_1 is the smallest of these prime numbers. If no such prime p_1 exists, then there will be no such pseudoprimes that are less than B^2.

Because prime numbers p that satisfy $a^{p-1} \equiv 1 \pmod{p^2}$ are rare, and prime numbers p that satisfy a Fermat's congruence of higher power are progressively rarer still, the pseudoprimes n that satisfy $a^{n-1} \equiv 1 \pmod{n^2}$ must also be rare (however, there do exist bases for which the number of pseudoprimes n satisfying $a^{n-1} \equiv 1 \pmod{n^2}$ exceeds the number of prime numbers p that satisfy $a^{p-1} \equiv 1 \pmod{p^2}$, up to a given bound). Thus, once the pseudoprimes n that satisfy $a^{n-1} \equiv 1 \pmod{n^2}$ are generated, it is a simple task to merely check to see if they also satisfy a Fermat's congruence of higher power. In this way, we can generate all pseudoprimes that satisfy $a^{n-1} \equiv 1 \pmod{n^m}$ for integers $m \geq 2$, having prime divisors up to a given bound. In Table 1, we list all such pseudoprimes having base $2 \leq a \leq 100$ and having prime divisors less than 2^{32}. A table of primes p that satisfy $a^{p-1} \equiv 1 \pmod{p^2}$, up to 2^{32}, corresponding to these bases (except for the cases in which a is a perfect kth power for an integer $k \geq 2$), can be found in [5] (the prime number 2 must be added to any listing that corresponds to a base a with $a \equiv 1 \pmod 4$).

a	n	m	a	n	m	a	n	m
17	4	2	65	4	3	82	9	2
26	15	2	65	8	2	82	45	2
26	1065	2	68	133	2	97	4	2
33	4	2	73	6	2	99	35	2
37	6	2	80	9	2	99	65	2
49	4	2	81	4	2	99	1729	2

TABLE 1. Pseudoprimes n satisfying $a^{n-1} \equiv 1 \pmod{n^m}$, where $2 \leq a \leq 100$, $m \geq 2$, and with n having prime factors $p < 2^{32}$.

References

[1] W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Annals of Math., **139** (1994), 703–722.
[2] R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp., **66** (1977), no. 217, 433–449.
[3] F.G. Dorais and D. Klyve, *A Wieferich Prime Search up to* 6.7×10^{15}, J. Integer Seq., **14** (2011), no. 9, Art. 11.9.2, 1-14.
[4] C. F. Gauss, *Disquisitiones Arithmeticae. Translated into English by Arthur A. Clarke, S. J.*, Yale Univ. Press, New Haven, Conn.-London, 1966.
[5] P. Montgomery, *New solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp., **61** (1991), 361–363.
[6] A. Rotkiewicz, *Sur les nombres de Mersenne dépourvus de diviseurs carrés et sur les nombres naturels n tels que* $n^2 | 2^n - 2$, Matematički Većnik, **2** (1965), no. 17, 78–80.
[7] A. Wieferich, *Zum letzten Fermat'schen Theorem*, J. Reine Angew. Math., **136** (1909), 293–302.

INTEGERS THAT SATISFY A FERMAT'S CONGRUENCE OF HIGHER POWER

MSC2020: Primary 11A07; Secondary 11D61, 11-04.

Department of Mathematics and Physical Sciences, Rogers State University, 1701 W. Will Rogers Blvd., Claremore, OK 74017-3252
Email address: gfox@rsu.edu