Pseudoprimes and Carmichael Numbers

Emily Riemer

MATH0420

May 3, 2016

Fermat's Little Theorem and Primality

Fermat's Little Theorem is foundational to the study of Carmichael numbers and many classes of pseudoprimes. The theorem states that if p is a prime number, then $a^{p-1} \equiv 1 (\text{mod } p)$, so long as $p \nmid a$. Because $\gcd(p, a) = 1$, we can multiply this congruence by a to arrive at the equivalent result of $a^p \equiv a (\text{mod } p)$. Both of these forms are used throughout the paper, as dictated by context. Though Fermat's Little Theorem is true for prime numbers, its converse is not true. That is, while every prime number satisfies Fermat's Little Theorem, not every number that satisfies Fermat's Little Theorem is prime. So, if $a^n \not\equiv a \pmod{n}$, we can conclude definitively that n is composite. However, finding that $a^n \equiv a \pmod{n}$ for some a does not prove that n is prime.

For example, we are able to determine that 63 is composite by examining $2^{63} (\text{mod } 63)$ and reducing using Euler's formula $[a^{\varphi(63)} = a^{24} \equiv 1 (\text{mod } 63)]$:

$$2^{63} = (2^{24})^2 \cdot 2^{15} \equiv 1 \cdot 2^{15} \equiv (2^6)^2 \cdot 2^3 \equiv (64)^2 \cdot 8 \equiv 1 \cdot 8 \not\equiv 2 (\text{mod } 63)$$

However, we can see that the converse of Fermat's Little Theorem does not hold true by observing the case of $n = 341$, which we know factors as $11 \cdot 31$:

$$2^{10} \equiv 1 (\text{mod } 11) \implies 2^{340} = (2^{10})^{34} \equiv 1 (\text{mod } 11)$$

$$2^{30} \equiv 1 (\text{mod } 31) \implies 2^{340} = (2^{30})^{11} \cdot 2^{10} \equiv 1^{11} \cdot (2^5)^2 \equiv (32)^2 \equiv 1 (\text{mod } 31)$$

$$2^{340} \equiv 1 (\text{mod } 11 \cdot 31) \equiv 1 (\text{mod } 341) \text{ [by the Chinese Remainder Theorem]}$$

Thus, 341 satisfies Fermat's Little Theorem to the base 2, even though we know that it is composite, and actually used its prime factorization to arrive at our result.

Bases a for which $a^n \not\equiv a (\text{mod } n)$ are referred to as witnesses for n. These values provide evidence that n is composite. While most composite numbers have

many witnesses, pseudoprimes have relatively fewer witnesses, and certain kinds of pseudoprimes, such as Carmichael numbers, have no witnesses at all. Prime numbers also have no witnesses, since there is no value of a for which $a^p \not\equiv a \pmod{p}$; such a result would violate Fermat's Little Theorem.

Primality Tests

Primality tests are used to determine whether a given number is prime or composite. A variety of such tests exist, most of which are beyond the scope of this paper. Some primality tests are probabilistic, meaning that they can verify that a number is composite, but can only provide insight into the likelihood that a number is prime. Other primality tests are deterministic, meaning that they can conclusively determine whether numbers are prime or composite. Fermat's Little Theorem functions as a probabilistic primality test, since it cannot do more than suggest that a number is prime. Moreover, there are still composite numbers n for which $a^n \equiv a \pmod{n}$ for some bases a.

The existence of these numbers necessitates more rigorous primality tests. One such test is the Rabin-Miller Test for Composite Numbers. The following definition is excerpted from Joseph Silverman's *Friendly Introduction to Number Theory*:

Let n be an odd integer and write $n - 1 = 2^k \cdot q$ with q odd. If both of the following conditions are true for some a not divisible by n, then n is a composite number:

(a) $a^q \not\equiv 1 \pmod{n}$

(b) $a^{2^i \cdot q} \not\equiv -1 \pmod{n}$ for all $i = 0, 1, 2, ..., k - 1$

The Rabin-Miller test is stronger than Fermat's Little Theorem because 75 percent of bases a between 1 and $n-1$ satisfy the above conditions for each odd composite n. This means that there are many witnesses for every composite number, and by extension

that no Carmichael-like numbers arise when applying this primality test.

Pseudoprimes

Broadly speaking, pseudoprimes are composite numbers that exhibit some properties of prime numbers. Various classes of pseudoprimes exist, and are described by the prime conditions they satisfy. This paper focuses on Fermat pseudoprimes, named as such because they satisfy Fermat's Little Theorem. Formally, a number n is a Fermat pseudoprime to base a if $a^n \equiv a \pmod{n}$, with n a composite positive integer. In this paper, any subsequent reference to pseudoprimes refers specifically to Fermat pseudoprimes.

It is interesting to note that such numbers are more rare than primes to any base a. In Chapter 5 of his *Elementary Number Theory*, Kenneth Rosen calculates that there are $455,052,512$ primes, but only $14,884$ pseudoprimes, less than 10^{10} to the base 2. Despite occurring much less frequently than primes, there are still infinitely pseudoprimes to the base 2. In fact, there are infinitely many pseudoprimes to every base. The proof of infinitely many pseudoprimes is of particular interest because it relies on the same underlying idea that we encountered in our study of Mersenne primes, namely using the Geometric Series formula to draw conclusions about divisibility. [It is also worth mentioning that Rosen's proof of infinitely many pseudoprimes to the base 2 is very similar to Silverman's derivation of the form of Mersenne primes from the general form $a^n - 1$]. The process of the proof itself therefore reinforces the connections between pseudoprimes and primes.

The following proof draws on the approaches used in papers by Bernd Kreussler and Graham Jameson. The goal is to show that $n = \dfrac{(a^{2p}-1)}{(a^2-1)}$ is a pseudoprime to base a, so long as $p \nmid a^2 - 1$. Because there are infinitely many inputs for p and a, the above formula will generate infinitely many pseudoprimes.

If n is a pseudoprime, it must be the case that it is both composite and odd. To prove this for n as defined above, notice that both the numerator and denominator are differences of squares, so the expression can be factored as:

$$n = \frac{(a^{2p} - 1)}{(a^2 - 1)} = \frac{(a^p - 1) \cdot (a^p + 1)}{(a - 1) \cdot (a + 1)}$$

The Geometric Series formula shows that:

$$a^p - 1 = (a - 1)(a^{p-1} + a^{p-2} + ... + a^p + a + 1)$$

We can see from the above equation that $(a - 1) \mid (a^p - 1)$. Similar reasoning leads to the conclusion that $(a + 1) \mid (a^p + 1)$. Because $\frac{(a^p - 1)}{(a - 1)}$ and $\frac{(a^p + 1)}{(a + 1)}$ are both integers, n is composite.

The Geometric Series formula is also helpful in showing that n is odd. In the general case, the Geometric Series formula says the following:

$$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + ... + x^2 + x + 1)$$

Taking $x = a^2$ and $m = p$ gives:

$$(a^2)^p - 1 = (a^2 - 1)((a^2)^{p-1} + (a^2)^{p-2} + ... + (a^2)^2 + a^2 + 1)$$
$$a^{2p} - 1 = (a^2 - 1)(a^{2p-2} + a^{2p-4} + ... + a^4 + a^2 + 1)$$
$$\frac{(a^{2p} - 1)}{(a^2 - 1)} = (a^{2p-2} + a^{2p-4} + ... + a^4 + a^2 + 1)$$
$$n = (a^{2p-2} + a^{2p-4} + ... + a^4 + a^2 + 1)$$

Using parity conditions, if a is even, then $a^{2p-2} + a^{2p-4} + ... + a^4 + a^2$ is even (since each term is even, and even + even = even), and $a^{2p-2} + a^{2p-4} + ... + a^4 + a^2 + 1$ is odd. If a is odd, then $a^{2p-2} + a^{2p-4} + ... + a^4 + a^2$ is even (since each term is odd, and odd + odd = even), and $a^{2p-2} + a^{2p-4} + ... + a^4 + a^2 + 1$ is again odd. Thus, n is always odd.

Finally, we must show that $a^{n-1} \equiv 1 (\text{mod } n)$. Rearranging the given equation for n shows that $n \cdot (a^2 - 1) = a^{2p} - 1$. We can then see that $n \mid a^{2p} - 1 \implies a^{2p} - 1 \equiv 0 \pmod{n} \implies a^{2p} \equiv 1 (\text{mod } n)$. This suggests that finding a relationship between $2p$ and $n - 1$ is critical to proving that $a^{n-1} \equiv 1 (\text{mod } n)$.

Expanding $n - 1$ yields:

$$\begin{aligned} n - 1 = \frac{(a^{2p} - 1)}{(a^2 - 1)} - 1 = \frac{(a^{2p} - 1)}{(a^2 - 1)} - \frac{(a^2 - 1)}{(a^2 - 1)} \\ = \frac{(a^{2p} - 1 - a^2 + 1)}{(a^2 - 1)} \\ = \frac{(a^{2p} - a^2)}{(a^2 - 1)} \end{aligned}$$

Our numerator is now a variation of Fermat's Little Theorem; multiplying both sides of $a^{p-1} \equiv 1 (\text{mod } p)$ by a gives $a^p \equiv a (\text{mod } p)$, and squaring this yields $a^{2p} \equiv a^2 (\text{mod } p)$. So with a little manipulation, Fermat's Little Theorem implies that $p \mid (a^{2p} - a^2)$.

Recall that if $p \mid ab$, $p \mid a$ or $p \mid b$. In this instance, because $p \mid (a^{2p} - a^2)$, and $(a^{2p} - a^2) = (n - 1)(a^2 - 1)$, p must divide $(n - 1)$ or $(a^2 - 1)$. However, by definition $p \nmid (a^2 - 1)$. Thus, p must divide $(n - 1)$. We demonstrated previously that n is odd, which means that $n - 1$ is even, so $2 \mid (n - 1)$. If 2 and p both divide $(n - 1)$, then $2p$ must also divide $(n - 1)$, and there must be some k such that $2p \cdot k = (n - 1)$. We also know from our work two paragraphs prior that $a^{2p} \equiv 1 (\text{mod } n)$. Putting all of this together yields:

$$a^{n-1} \equiv a^{2p \cdot k} \equiv (a^{2p})^k \equiv 1^k \equiv 1 \pmod{n}.$$

Thus, $a^{n-1} \equiv 1 (\text{mod } n)$. This completes our proof of infinitely many pseudoprimes.

Carmichael Numbers and Korselt's Criterion

As mentioned previously, Fermat's Little Theorem does not always identify composite numbers as such. Numbers for which $a^n \equiv a \pmod{n}$ for *every* integer

$1 \leq a \leq n$ are known as Carmichael numbers. The smallest Carmichael number is 561, the product of $3 \cdot 11 \cdot 17$. It is straightforward to verify that $a^{561} \equiv a \pmod{561}$ for all values of a. One can use Fermat's Little Theorem to show that $a^{561} \equiv a \pmod{p_i}$ for $p_i = 3$, 11, and 17, then use the Chinese Remainder Theorem to confirm that $a^{561} \equiv a \pmod{3 \cdot 11 \cdot 17} \implies a^{561} \equiv a \pmod{561}$.

Carmichael numbers are are further defined by Korselt's Criterion, which states that n is a Carmichael number if and only if:

a) n is odd

b) For every prime p dividing n, $p^2 \nmid n$ (in other words, n is the product of distinct primes)

c) For every p dividing n, $(p-1) \mid (n-1)$

All numbers satisfying Korselt's Criterion are Carmichael numbers, and all Carmichael numbers satisfy Korselt's Criterion. Not presented in this paper, the proof of Korselt's Criterion can be approached using a heuristic similar to one used in our proof of Gaussian primes and integer primes that can be written as sums of squares. Each component can be connected to the next in a kind of triangle, in which (a) $\implies$ (b), (b) $\implies$ (c), and (c) $\implies$ (a). One could easily check that our first Carmichael number 561 satisfies Korselt's Criterion.

Korselt's Criterion states that every Carmichael number is the product of distinct primes. In fact, Carmichael numbers are always the products of at least three distinct primes. To understand why, consider n, the product of primes p and q. If n is a Carmichael number, then by Korselt's Criterion it must be that case that $(p-1) \mid (n-1)$ and $(q-1) \mid (n-1)$, and neither p^2 nor q^2 divides n. The latter requirement tells us that $p \neq q$, so one must be larger than the other, say $q > p$. Then $q - 1 > p - 1$, and $(q-1)$ cannot divide $(p-1)$. We know that $(q-1) \mid (n-1) - (p-1)$, since

$(n-1)-(p-1) = n-p = pq-p = p(q-1)$. And if $q-1$ divides the linear combination $(n-1)-(p-1)$ and also divides $n-1$, then it must divide $p-1$. But we have shown that $q-1 \nmid p-1$. Therefore, we have a contradiction, and n cannot be a Carmichael number.

It was not proven until 1994 that there are infinitely many Carmichael numbers, despite the fact that mathematicians have been discovering new Carmichael numbers since the late 19th century. One method for generating Carmichael numbers relies on the following claim: If k is chosen such that $6k+1, 12k+1$, and $18k+1$ are all prime, then their product n is a Carmichael number. Recall that in order for n to be a Carmichael number, it must satisfy Korselt's Criterion. That is, n must be odd, and for every prime p dividing n, it must be the case that $p^2 \nmid n$ and $p-1 \mid n-1$.

The first step in the proof is to show that n is odd. If $6k+1, 12k+1$, and $18k+1$ are all prime, then they must all be odd. This means that n is the product of three odd numbers, and is itself odd.

Second, we must show that $p_i^2 \nmid n$. This is true since the prime factorization of n is $(6k+1)\cdot(12k+1)\cdot(18k+1)$, or $p_1 \cdot p_2 \cdot p_3$. Because of unique prime factorization, n can only be factored as $p_1 \cdot p_2 \cdot p_3$, so p_i^2 cannot be a factor of n.

The third component of the proof is to show that $(p_i - 1) \mid (n-1)$. To do so, start by expanding n:

$$n = (6k+1)\cdot(12k+1)\cdot(18k+1)$$

$$n = 1296k^3 + 396k^2 + 36k + 1$$

$$n - 1 = 1296k^3 + 396k^2 + 36k$$

$$n - 1 = 36k(36k^2 + 11k + 1)$$

Next, consider each p_i in turn:

a) $(p_1 - 1) = 6k + 1 - 1 = 6k$

$36k = 6 \cdot 6k \implies 6k \mid 36k(36k^2 + 11k + 1) \implies (p_1 - 1) \mid (n - 1)$

b) $(p_2 - 1) = 12k + 1 - 1 = 12k$

$36k = 3 \cdot 12k \implies 12kd \mid 36k(36k^2 + 11k + 1) \implies (p_2 - 1) \mid (n - 1)$

c) $(p_3 - 1) = 18k + 1 - 1 = 18k$

$36k = 2 \cdot 18k \implies 18k \mid 36k(36k^2 + 11k + 1) \implies (p_3 - 1) \mid (n - 1)$

Finally, if n is a Carmichael number, it must also satisfy $a^{n-1} \equiv 1 \pmod{n}$. Because we have defined $(6k + 1), (12k + 1)$, and $(18k + 1)$ to be prime, we know by Fermat's Little Theorem that $a^{p_i - 1} \equiv 1 \pmod{p_i}$.

We want to show that $a^{n-1} \equiv 1 \pmod{p_i}$, and then use the Chinese Remainder Theorem to show $a^{n-1} \equiv 1 \pmod{n}$. Because we know that $a^{p_i - 1} \equiv 1 \pmod{p_i}$, our task is to find a way to relate $a^{p_i - 1}$ and a^{n-1}. In fact, we have already shown that $(p_i - 1) \mid (n - 1)$, so we know that $v \cdot (p_i - 1) = (n - 1)$ for some v. Then $a^{n-1} = a^{v \cdot (p_i - 1)} = (a^{p_i - 1})^v \equiv 1^v \pmod{p_i}$. Thus, we have shown that $a^{n-1} \equiv 1 \pmod{p_i}$. Using the Chinese Remainder Theorem and the fact that $n = p_1 \cdot p_2 \cdot p_3$, we can show that $a^{n-1} \equiv 1 \pmod{p_1 \cdot p_2 \cdot p_3} \equiv 1 \pmod{n}$. This completes the proof that n is a Carmichael number.

Using the above method, the smallest value of k for which n is a Carmichael number is 1. When $k = 1, p_1 = 7, p_2 = 13$, and $p_3 = 19$. This gives $n = 1729$.

Applications of Pseudoprimes and Carmichael Numbers

Though there are no obvious direct applications of pseudoprimes or Carmichael numbers, such concepts are relevant in the realm of cryptography. Public keys necessitate the generation or discovery of large prime numbers (what we have been referring to as p and q in our discussion of RSA cryptography). Finding and verifying large prime numbers is therefore an essential prerequisite for RSA. Primality tests can be used to

locate large primes, and understanding which composite numbers appear prime when applying certain primality tests (i.e. when pseudoprimes might appear) is critical to ensuring that one has correctly chosen primes for encryption. Unknowingly selecting a pseudoprime as p or q would lead to an incorrect calculation of $\varphi(m)$, which would then derail the rest of the encryption computations. Despite an ostensible lack of direct applications, mathematicians remain interested in finding and further examining Carmichael numbers.

Works Consulted

Baker, Matthew. Korselt's Criterion for Carmichael Numbers. Notes for MATH4150, Spring 2011, Georgia Institute of Technology. http://people.math.gatech.edu/∼mbaker/pdf/korselt.pdf

Kreussler, Bernd. Pseudoprimes. Notes for MA6011, Mary Immaculate College, University of Limerick. http://www.maths.mic.ul.ie/kreussler/MA6011/week05.pdf

Jameson, Graham. Finding pseudoprimes. March 2010, Lancaster University. http://www.maths.lancs.ac.uk/ jameson/carfind.pdf

Jameson, Graham. Carmichael numbers and pseudoprimes. May 2010, Lancaster University. http://www.maths.lancs.ac.uk/ jameson/carpsp.pdf

Rosen, Kenneth. Elementary Number Theory and Its Applications. 6th ed. New Jersey: Pearson Education, Inc., 2010.

Silverman, Joseph H. A Friendly Introduction to Number Theory. 4th ed. New Jersey: Pearson Education, Inc., 2013.