The Resolved and Unresolved Conjectures of R. D. Carmichael

Brian D. Beasley (Presbyterian College)

Brian Beasley (B.S., Emory University; M.S., University of North Carolina; Ph.D., University of South Carolina) has taught at Presbyterian College since 1988. He became a member of the Mathematical Association of America in 1989 and joined ACMS in 2007. Outside the classroom, Brian enjoys family time with his wife and two sons. A big fan of the various writings of C. S. Lewis, he is also an enthusiastic Scrabble player, a somewhat less than enthusiastic jogger, and a very shaky unicyclist.

Abstract

Even before heading to Princeton University to work on his doctoral degree, Robert Carmichael started influencing the path of number theory in the 20th century. From his study of Euler's totient function to his discovery of the first absolute pseudoprime, he set the stage for years of productive research. We present a brief overview of Carmichael's life, including his breadth of mathematical interests and his service on behalf of the Mathematical Association of America. The main focus is upon his two most famous conjectures - which one has been settled, and which one remains open to this day?

1 Early Years

Robert Daniel Carmichael was born in Goodwater, Alabama in 1879. Carmichael spent the first thirty years of his life in Alabama, never too far away from Goodwater. He graduated from nearby Lineville College in 1898, and three years later he married Eula Smith Narramore from Randolph (south of Birmingham). Robert and Eula settled in Hartselle with their four children, Eunice, Erdys, Gershom, and Robert Leslie. Carmichael began training to become a Presbyterian pastor, presumably with the intention of keeping his home and family and ministry in Alabama [30].

Yet starting in 1905, the situation began to change for Carmichael. Between 1905 and 1915, he submitted dozens of problems to *The American Mathematical Monthly*. For example, in 1908 Carmichael contributed the following problem [7] to the "Number Theory and Diophantine Analysis" section:

If p and q are primes and m and n are any integers, find the cases in which the equation $p^m - q^n = 1$ may be satisfied.

Meanwhile, in October of 1906, Carmichael became professor of mathematics at Presbyterian College in Anniston, Alabama. The school was in just its second year when he arrived, and it continued as a college until 1918. As noted in [2], during its brief history, it offered both a Classical Course (B.A.) and a Scientific Course (B.S.), awarding a total of 37 degrees. Presbyterian College also somehow managed to field a football team, playing local high schools and colleges and even taking on the University of Georgia squad in 1909 and in 1911. The team's nickname? The Predestinarians.

In 1909, Carmichael moved his family to Princeton, where he started graduate work in mathematics. Under the direction of George Birkhoff, he wrote his thesis (Linear Difference Equations and their Analytic Solutions) and received his doctorate in 1911. Carmichael then accepted a professorship at Indiana University, teaching there from 1911 to 1915 [30]. Of his eventual 35 doctoral students, only the first earned the degree at Indiana, but this represented a significant milestone: In 1912, Cora B. Hennel became the first person, male or female, to receive a doctorate in mathematics at Indiana [20].

Even before heading to Princeton, Carmichael published 13 papers in various mathematical journals between 1905 and 1909. These articles ranged from shorter pieces involving *Monthly* journal problems (see [5]) to longer works on topics such as multiply perfect numbers (see [4]). The most famous of these papers, entitled "On Euler's ϕ-Function," appeared in the *Bulletin of the American Mathematical Society* in 1907 [6]. In this article, Carmichael remarked, "The object of the present note is the demonstration of certain very elementary propositions concerning Euler's ϕ-function of a number." Yet what Carmichael viewed as a basic proposition has turned out to be much more difficult to establish than he originally believed.

2 The First Conjecture

In his 1907 paper, Carmichael examined the question of whether a number could occur exactly once in the range of the Euler ϕ-function. Recall that given a positive integer n, its Euler phi-function (or totient) value is the number $\phi(n)$ of integers x with $1 \leq x \leq n$ such that $\gcd(x, n) = 1$. For example, $\phi(1) = 1 = \phi(2)$, while $\phi(n)$ is even for all values of $n > 2$. However, not every positive even integer appears in the range of ϕ; the smallest such exception is 14. The two key properties of this function are:

(i) If p is prime and k is a positive integer, then $\phi(p^k) = p^k - p^{k-1}$.

(ii) Given positive integers a and b, if $\gcd(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$.

Using these properties, Carmichael offered a proof of the following claim.

Proposition. The relation $\phi(m) = n$, a given number, is never uniquely satisfied for any given value of n. That is, there is always more than one value of m for every possible value of n.

We present a brief summary of Carmichael's argument [6]. For contradiction, assume there is a positive integer n such that the equation $\phi(m) = n$ has exactly one solution m. If m is odd, then $\phi(2m) = \phi(m) = n$; similarly, if $m/2$ is odd, then $\phi(m/2) = \phi(m) = n$. Thus 4 divides m, so n is even. Writing $m = 4a$ and $n = 2b$ for positive integers a and b yields $\phi(4a) = 2b$, which in turn implies $\phi(2a) = b$. Then both a and b must be even. Continuing this process, we eventually reduce to the case in which both of these integers must be powers of 2. But the equation $\phi(x) = 2^c$ has more than one solution for $c \geq 3$, since we may take $x = 2^{c+1}$ and $x = 2^{c-2} \cdot 3 \cdot 5$.

Unfortunately, there is a gap in Carmichael's proof. The argument that both a and b must be even

depends on the fact that otherwise, there would not be a unique solution for the equation $\phi(2a) = b$; however, that does not necessarily lead to a contradiction with the original assumption of a unique solution for the equation $\phi(m) = n$. At first Carmichael did not recognize the error, and he included the result as a homework problem in his 1914 book *The Theory of Numbers* [10]:

(Chapter 2, Exercise 8) Show that if the equation $\phi(x) = n$ has one solution it always has a second solution, n being given and x being the unknown.

Readers of his book pointed out the gap in the proof, prompting Carmichael to publish another paper, "Note on Euler's ϕ-Function," in 1922 [11]. He noted, "Two correspondents have recently called my attention to the fact that the supposed proof of the following theorem, which I gave some years ago, is not adequate. So far I have been unable to supply a proof of the theorem, though it seems probable that it is correct. I am therefore compelled to allow it to stand in the status of a conjectured or empirical theorem."

Undaunted, in the same 1922 paper Carmichael determined a lower bound on any counterexample to the conjecture. He showed that if there is a positive integer n such that $\phi(m) = n$ is uniquely satisfied by m, then $m > 10^{37}$. This has inspired mathematicians ever since to establish improved lower bounds for such a counterexample. We present several of these results to note their progress over the years:

$m > 10^{400}$	1947 - Klee [21]
$m > 10^{10,000}$	1982 - Masai and Vallette [24]
$m > 10^{10,000,000}$	1994 - Schlafly and Wagon [34]
$m > 10^{10,000,000,000}$	1998 - Ford [17]

Such an immense lower bound is quite remarkable; in comparison, the current lower bound on the possible existence of an odd perfect number is a mere 10^{1500}, as shown by Ochem and Rao [29]. As Schlafly and Wagon [34] remarked, "We do not know of another unsolved problem in mathematics for which a lower bound on a counterexample is so high ... There can be little doubt that Carmichael's conjecture is true."

Work on Carmichael's conjecture and related topics has continued over the years. One approach has been to define the function $A(n)$ for a positive integer n to be the number of solutions of $\phi(m) = n$. For example, $A(1) = 2$ and $A(2) = 3$, while $A(24) = 10$. Also, given any odd integer $n > 1$, we have $A(n) = 0$. Erdős proved that if $A(n) = k$ for some integer n, then there exist infinitely many such n [16]. In addition, Sierpiński conjectured and Ford proved that for each integer $k \geq 2$, there is an integer n such that $A(n) = k$ [18]. This function allows us to restate Carmichael's conjecture: $A(n)$ never equals 1.

To date, Carmichael's first conjecture has not been resolved. We leave the final word in this section to Erdős [16]:

"This conjecture is still unproved and seems very deep."

3 The Second Conjecture

In order to introduce another famous conjecture by Carmichael, we recall an important result from number theory. Fermat's Little Theorem states that if p is prime, then for every integer a with $\gcd(a, p) = 1$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Euler would later generalize this result, showing that given any positive integer n, if a is an integer with $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Fermat's Little Theorem prompts two questions:
(i) Can we find a composite n with $a^{n-1} \equiv 1 \pmod{n}$ and $\gcd(a, n) = 1$ for at least

To answer the first question, Sarrus [33] noted in 1819 that since $2^{10} \equiv 1 \pmod{341}$, we have $2^{340} \equiv 1 \pmod{341}$, even though $341 = 11 \cdot 31$ is not prime. Such composite numbers are called *pseudoprimes* (or pseudoprimes to base 2); they are also often referred to as *Sarrus numbers*.

In tackling the second question, Korselt [22] established the following result in 1899.

Korselt's Criterion. Given a composite integer $n > 1$, $a^{n-1} \equiv 1 \pmod{n}$ for every integer a with $\gcd(a, n) = 1$ if and only if n is squarefree and $p - 1$ divides $n - 1$ for every prime p that divides n.

Such composite numbers n are called *absolute pseudoprimes*. Do they exist?

In 1910, Carmichael [8] found the first example, proving that $561 = 3{\cdot}11{\cdot}17$ is an absolute pseudoprime; he also showed that every absolute pseudoprime is odd and has at least three distinct odd prime factors. Two years later, Carmichael [9] provided a list of 15 additional absolute pseudoprimes. In this paper, he offered a tantalizing footnote as well: "This list might be indefinitely extended." Carmichael's footnote has since been restated in the following form.

Conjecture. There are infinitely many absolute pseudoprimes.

To extend Carmichael's list, Chernick [13] proved in 1939 that every absolute pseudoprime with three prime factors has the form

$$(2r_1h + 1)(2r_2h + 1)(2r_3h + 1),$$

where r_1, r_2, and r_3 are pairwise relatively prime. Taking $r_1 = 1$, $r_2 = 2$, $r_3 = 3$, and $h = 3k$, Chernick also showed that $(6k + 1)(12k + 1)(18k + 1)$ is an absolute pseudoprime if each of its three factors is prime. His list of absolute pseudoprimes included $5 \cdot 17 \cdot 29$, $5 \cdot 17 \cdot 29 \cdot 113$, and $5 \cdot 17 \cdot 29 \cdot 113 \cdot 337$.

In the spirit of Carmichael's original footnote, Chernick added, "The process may be continued to the limits of present-day factor tables."

Meanwhile, the situation for pseudoprimes had been resolved. In 1936, Lehmer [23] proved that there are infinitely many pseudoprimes. In particular, he showed that if p and q are distinct odd primes, then pq divides $2^{pq-1}-1$ if and only if the order of 2 modulo p divides $q-1$ and the order of 2 modulo q divides $p-1$; here, the order of 2 modulo r is defined as the smallest positive integer k such that $2^k \equiv 1 \pmod{r}$. Sierpiński [35] followed this in 1947 with the result that if n is a pseudoprime, then 2^n-1 is also a pseudoprime. And in 1949, Erdős [14] established that for every $k \geq 2$, there are infinitely many pseudoprimes with exactly k different prime factors.

As for absolute pseudoprimes, or *Carmichael numbers* as they had come to be known, we offer two observations from Erdős. In 1949, he commented in [14], "It seems very difficult to determine whether there are infinitely many absolute pseudoprimes." Yet by 1956, Erdős had provided a heuristic argument for the existence of infinitely many absolute pseudoprimes [15]; in particular, he conjectured that for x sufficiently large, there should be $x^{1-o(1)}$ Carmichael numbers up to x (a function $f(x)$ is said to be $o(1)$ if $\lim_{x\to\infty} f(x) = 0$). Pomerance later conjectured in [32] that the exponent in this bound could be improved to $1-\{1+o(1)\}\log\log\log x/\log\log x$.

In 1994, Carmichael's second conjecture was resolved in the affirmative. That year, Alford, Granville, and Pomerance [1] proved that there are indeed infinitely many Carmichael numbers. In their proof, they used Korselt's Criterion and modified Erdős' heuristic argument. In fact, they dedicated their paper to Erdős on the occasion of his 80th birthday. They were able to show that if $C(x)$ is the number of Carmichael numbers up to x, then for sufficiently large x.

$$C(x) > x^{2/7}.$$

In 2008, Harman [19] was able to increase this exponent from 2/7 to 1/3.

Carmichael's work on this topic continues to inspire mathematicians to this day. The search for more Carmichael numbers is ongoing, with particular interest in finding the largest known k-Carmichael (a Carmichael number with exactly k prime factors). For example, the largest known 3-Carmichael has 60,351 digits [3], and the largest known 4-Carmichael (with 30,366 digits) was just recently discovered [28]. In addition, current calculations summarized in [31] feature results such as $C(10^{16}) = 246,683$ and $C(10^{21}) = 20,138,200$. Remaining questions include:

(i) Are there infinitely many 3-Carmichaels?

(ii) Are there infinitely many k-Carmichaels for each $k > 3$?

Research also continues on the question of the existence of special types of Carmichael numbers, such as those found in arithmetic progressions. In 2012, Matomäki [27] showed that if $\gcd(a, M) = 1$ and a is a quadratic residue modulo M, then there are infinitely many Carmichael numbers m with $m \equiv a \pmod{M}$. The next year, Wright [36] proved unconditionally that if $\gcd(a, M) = 1$, then there are infinitely many Carmichael numbers m with $m \equiv a \pmod{M}$.

4 Later Years

Over the next several decades, Carmichael continued his research and service on behalf of the mathematical community. In 1915, he moved to the University of Illinois, working there as a professor of mathematics for 32 years. Carmichael served as the head of the mathematics department at Illinois from 1929 to 1934, and in his last year in that role, he also became the acting dean of the graduate school. The next year, he was elected dean, continuing in that position until his retirement in 1947 [25]. During his tenure at Illinois, he supervised 34 additional doctoral students, with nine of them completing their work after he became the dean [26].

To convey a sense of the impressive range of Carmichael's mathematical interests, we list just a few of his many publications. Having already written books on both relativity and number theory while at Indiana, Carmichael also co-authored texts on calculus and on plane and spherical trigonometry during his time at Illinois. He wrote *Diophantine Analysis* in 1915 and *Introduction to the Theory of Groups of Finite Order* in 1937. In between, he published one of his most interesting works, *The Logic of Discovery*, in 1930. This book summarized Carmichael's views on the philosophy of mathematics and received very positive reviews. In particular, the last chapter on "The Larger Human Worth of Mathematics" gave a glimpse into his theological background. Toward the end of this chapter [12], Carmichael paraphrased Isaiah 52:7, writing

> "How beautiful upon the highway are the feet of him who comes bringing
> in his hands the gift of a new truth to mankind."

While teaching students, leading his department and graduate school, and writing books on a variety of topics, Carmichael still managed to find time to serve the Mathematical Association of America in a number of roles [25]. A charter member of the MAA, he became editor-in-chief of the *Monthly* in 1918. Carmichael held the position of Vice President from 1921 to 1922 and was selected as the organization's eighth President in 1923. He also served on the MAA Board of Governors on three separate occasions, in 1920, 1924-1929, and 1939-1941.

In conclusion, when one considers the many accomplishments of Carmichael's career, along with his obvious love of mathematics and philosophy, it is no wonder that he was held in such high regard by those who knew him best. In tribute [30], his friend Harrison E. Cunningham said of Carmichael:

> "Of unyielding integrity, he loved the truth and hated sham
> and pretense. His appreciation of the beautiful,
> the true, and the good is exceptional.
> His friendship is firm, his loyalty unbreakable.
> Those who know him are fortunate beyond words."

Acknowledgment. The author would like to thank the referees, whose constructive feedback helped to improve the paper.

References

[1] W. Alford, A. Granville, C. Pomerance. There are infinitely many Carmichael numbers, *Annals of Mathematics* **139** (1994), 703-722.

[2] America's Lost Colleges web site. "Alabama Presbyterian College for Men," http://www.lostcolleges.com/alabama-presbyterian-college

[3] D. Broadhurst. 60351-digit 3-Carmichael number, NMBRTHY Archives, 2 Dec 2002. http://listserv.nodak.edu

[4] R. D. Carmichael. Multiply perfect numbers of four different primes, *Annals of Mathematics* **8** (1907), 149-158.

[5] R. D. Carmichael. Note on a recent problem in *The American Mathematical Monthly*, *The American Mathematical Monthly* **14** (1907), 8-9.

[6] R. D. Carmichael. On Euler's ϕ-function, *Bulletin of the American Mathematical Society* **13** (1907), 241-243.

[7] R. D. Carmichael. Problem 155, *The American Mathematical Monthly* **15** (1908), 170.

[8] R. D. Carmichael. Note on a new number theory function, *Bulletin of the American Mathematical Society* **16** (1910), 232-238.

[9] R. D. Carmichael. On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$, *The American Mathematical Monthly* **19** (1912), 22-27.

[10] R. D. Carmichael. *The Theory of Numbers*, John Wiley & Sons (1914).

[11] R. D. Carmichael. Note on Euler's ϕ-function, *Bulletin of the American Mathematical Society* **28** (1922), 109-110.

[12] R. D. Carmichael. *The Logic of Discovery*, Open Court Publishing Co. (1930).

[13] J. Chernick. On Fermat's simple theorem, *Bulletin of the American Mathematical Society* **45** (1939), 269-274.

[14] P. Erdős. On the converse of Fermat's theorem, *The American Mathematical Monthly* **56** (1949), 623-624.

[15] P. Erdős. On pseudoprimes and Carmichael numbers, *Publ. Math. Debrecen* **4** (1956), 201-206.

[16] P. Erdős. Some remarks on Euler's ϕ-function, *Acta Arithmetica* **4** (1958), 10-19.

[17] K. Ford. The distribution of totients, *The Ramanujan Journal* **2** (1998), 67-151.

[18] K. Ford. The number of solutions of $\phi(x) = m$, *Annals of Mathematics* **150** (1999), 283-311.

[19] G. Harman. Watt's mean value theorem and Carmichael numbers, *International Journal of Number Theory* **4** (2008), 242-243.

[20] Indiana University Department of Mathematics web site. "Early History," https://math.indiana.edu/about/history/index.html

[21] V. Klee. On a conjecture of Carmichael, *Bulletin of the American Mathematical Society* **53** (1947), 1183-1186.

[22] A. Korselt. Problème chinois, *L'Intermédiaire des Mathématiciens* **6** (1899), 142-143.

[23] D. H. Lehmer. On the converse of Fermat's theorem, *The American Mathematical Monthly* **43** (1936), 347-354.

[24] P. Masai and A. Vallette. A lower bound for a counterexample to Carmichael's conjecture, *Boll. Un. Mat. Ital.* **1** (1982), 313-316.

[25] Mathematical Association of America web site. "Robert Daniel Carmichael, 1923 MAA President," https://www.maa.org/about-maa/governance/maa-presidents/robert-daniel-carmichael-1923-maa-president

[26] Mathematics Genealogy Project web site. "Robert Daniel Carmichael," https://www.genealogy.math.ndsu.nodak.edu

[27] K. Matomäki. Carmichael numbers in arithmetic progressions, *Journal of the Australian Mathematical Society* **94** (2013), 268-275.

[28] J. Muñoz. New record 4-Carmichael number with 30366 digits, NMBRTHY Archives, 15 May 2017. http://listserv.nodak.edu

[29] P. Ochem and M. Rao. Odd perfect numbers are greater than 10^{1500}, *Mathematics of Computation*, **81** (2012), 1869-1877.

[30] J. O'Connor, E. Robertson. "Robert Daniel Carmichael," MacTutor history of mathematics web, http://www-groups.dcs.st-and.ac.uk/history/Biographies/Carmichael.html

[31] R. Pinch. The Carmichael numbers up to 10^{21}, *TUCS Proceedings of Conference on Algorithmic Number Theory* **46** (2007), 129-131.

[32] C. Pomerance. On the distribution of pseudoprimes, *Mathematics of Computation* **37** (1981), 587-593.

[33] F. Sarrus. Questions résolues, *Annales de Gergonne* **10** (1819-1820), 184-187.

[34] A. Schlafly, S. Wagon. Carmichael's conjecture on the Euler function is valid below $10^{10,000,000}$, *Mathematics of Computation* **63** (1994), 415-419.

[35] W. Sierpiński. Remarque sur une hypothèse des Chinois concernant les nombres $(2^n - 2)/n$, *Colloq. Math.* **1** (1947), 9.

[36] T. Wright. Infinitely many Carmichael numbers in arithmetic progressions, *Bulletin of the London Mathematical Society* **45** (2013), 943-952.