102.39 Variants of Carmichael Numbers and Cunningham chains

A composite positive integer n that has the property $a^n \equiv a$ modulo n for *all* a, is known as a Carmichael number. There are infinitely many Carmichael numbers; this is a highly non-trivial fact that has been proved combining techniques ranging from group algebras to sieve methods in analytic number theory. (See [1] where it is shown that asymptotically more than $x^{2/7}$ numbers less than or equal to x are Carmichael numbers.) Let us look at the slightly different congruence $a^{n+1} \equiv a$ modulo n. Which positive integers $n > 1$ have the property $a^{n+1} \equiv a$ modulo n, for every a? We will show that this is rather restrictive and produces *exactly four* such $n > 1$, viz. 2, 6, 42, 1806. Thus, these are very different from Carmichael numbers. On the other hand, another variant is to consider those $n > 1$ having the property that $a^{n-1} \equiv a$ modulo n for all a. In this case, we do find that there are infinitely many such n. Although it is unclear if the infinitude holds for n with more than three prime factors, interestingly, the set of such n with exactly three prime factors is an infinite set if, and only if, there are infinitely many primes p for which $2p - 1$ is prime. This question is analogous to the question of infinitude of Sophie Germain primes and is open as well. We make further remarks on this at the end of this Note.

Variant I

Let us start with the problem of finding all $n > 1$ such that $a^{n+1} \equiv a$ modulo n for every positive integer a. Evidently, $n = 2$ has this property. Now, if $n > 1$ is odd, the integer $a = n - 1$ does not satisfy the congruence since $(n-1)^{n+1} \equiv 1 \not\equiv n - 1$ modulo n. Further, if n is not square-free, say $p^2 | n$, then $a = p$ does not satisfy the congruence because $p^{n+1} - p = p(p^n - 1) \not\equiv 0$ modulo p^2. Therefore, we need to consider numbers of the form

$$n = 2p_1p_2\ldots p_r$$

where $p_1 < p_2 < \ldots < p_r$ are odd primes.

We claim that $r \leqslant 3$ and we determine all the possibilities. Suppose $a^{n+1} \equiv a$ modulo p_i for $i \leqslant r$. For each $1 \leqslant i \leqslant r$, we have $a^n \equiv 1$ modulo p_i for all $(a, p_i) = 1$. By the Chinese remainder theorem, we may choose a which is a primitive root modulo p_i and is congruent to 1 modulo p_j for all $j \neq i$. Then, $p_i - 1$ divides n for each $i \geqslant 1$. As $n = 2p_1p_2\ldots p_r$ with $p_1 < p_2 < \ldots < p_r$, it follows that the even number $p_i - 1$ is a product of some of the p_j for which $j < i$. In particular, $p_1 = 1 + 2 = 3$. Therefore, $r = 1$ gives the unique solution $n = 2p_1 = 6$. Let $r > 1$. Now $p_2 - 1 = 2p_1 = 6$ implies $p_2 = 7$. Therefore, $r = 2$ gives the unique solution $n = 2p_1p_2 = 42$. If $r = 3$, then $p_3 - 1 = 2p_2$ or $2p_1p_2$; this gives $p_3 = 2p_1p_2 + 1 = 43$ because $2p_2 + 1 = 15$ is not a prime. Therefore $r = 3$ gives the unique solution $n = 2p_1p_2p_3 = 1806$. We claim that $r > 3$ is impossible; that is, we claim there is no p_4. Indeed, if it exists, then $p_4 - 1 = 2p_1p_2p_3$ or $2p_1p_3$ or $2p_2p_3$ or $2p_3$. But, these four cases

give $p_4 = 1807, 259, 603$ or 87 none of which are primes. Therefore, $n > 1$ has the property $a^{n+1} \equiv a$ modulo n for all a if, and only if, $n = 2$, 6, 42 or 1806.

Variant II

Consider now the problem of finding all $n > 1$ such that $a^{n-1} \equiv a$ modulo n for all positive integers a. Once again, $n = 2$ evidently has this property. Arguing as above, it is clear that when $n > 1$, it must be odd and square-free. Therefore, we consider $n = 2p_1p_2\ldots p_r$ with odd primes $p_1 < p_2 < \ldots < p_r$ such that $a^{n-1} \equiv a$ modulo n for all a. This reduces to the conditions $a^{n-2} \equiv 1$ modulo p_i for each i and each a not divisible by p_i. Once again, the Chinese remainder theorem allows us to select, for each i, a primitive root a modulo p_i which is congruent to 1 modulo p_j for each $j \neq i$. Thus, $p_i - 1$ must divide $n - 2 = 2(p_1p_2\ldots p_r - 1)$ for each $i \leqslant r$.

If $r = 1$, clearly *any* odd prime p_1 has this property; that is, $n = 2p_1$ is a positive integer such that $a^{n-1} \equiv a$ modulo n for every integer a. Thus, there are infinitely many n with exactly two prime factors with the said property.

Let $r = 2$. Then, the condition that $p_2 - 1$ divides $2(p_1 - 1)$ is satisfied if, and only if, $p_2 - 1 = 2(p_1 - 1)$ since $p_2 > p_1$. But then $p_2 = 2p_1 - 1$ is a prime. Note that in this case $p_1 - 1$ does divide $2(p_2 - 1) = 4(p_1 - 1)$. Therefore, the positive integers n with exactly three prime factors that satisfy the condition $a^{n-1} \equiv a$ modulo n for all a are precisely the numbers $n = 2p_1(2p_1 - 1)$ where $2p_1 - 1$ is prime. Hence, the infinitude of n with exactly three prime factors is equivalent to the infinitude of primes p for which $2p - 1$ is also prime. We presently discuss what this question entails. Before that, we mention in passing that the case $r = 3$ is much more complicated. One example is $n = 2 \times 3 \times 11 \times 17$. It is not clear if there are infinitely many solutions.

Sophie Germain primes and Cunningham chains

We make some comments on questions about the infinitude of certain types of primes. A *Sophie Germain prime* is a prime p such that $2p + 1$ is also prime. Sophie Germain proved that the first case of Fermat's Last Theorem holds for such p. They also play a role in cryptography. However, the question of their infinitude is open. Similarly, the question of infinitude of primes p for which $2p - 1$ is prime is also open and is expected to be of the same level of difficulty − both are addressed by a conjecture of L. E. Dickson. In fact, the more general so-called Cauchy-Bunyakovsky conjecture asserts that if $f_1, \ldots, f_n$ are non-constant integer polynomials such that for every prime p and each $i \leqslant n$, there is an integer a_i such that p does not divide $f(a_i)$, then there are infinitely many integers a for which all the n integers $f_i(a)$ are simultaneously primes. Dickson's conjecture is the case when the f_i have degree 1. In our context, look at the two polynomials x and $2x + 1$ or the two polynomials x and $2x - 1$. The divisibility

condition is evidently necessary; otherwise, there are examples like x and $x + 1$. Though these conjectures predict infinitude, the set of primes produced is rather thin. In particular, Barry Powell showed [2] that for coprime positive integers a, b the set of primes p for which $ap + b$ is also prime has zero primitive density (meaning that the proportion of $p \leqslant x$ for which $ap + b$ is prime, tends to 0 as $x \to \infty$). The set of primes p for which $2p - 1$ is also prime has no special name and there does not seem to be much literature on these excepting what we recall below. Named after A. J. C. Cunningham, there are the so-called Cunningham chains of the first and second kinds [3, p. 333]. A Cunningham chain of length k of the first kind is a chain of primes of the form

$$p_1, p_2, \ldots, p_k$$

where $p_{i+1} = 2p_i + 1$. Thus, the first $k - 1$ primes in the chain are Sophie Germain primes. Similarly, the Cunningham chains of the second kind are defined as chains of the form

$$p_1, p_2, \ldots, p_k$$

where $p_{i+1} = 2p_i - 1$. It is an open question as to whether there are Cunningham chains (of either kind) of any arbitrary length. Let us make some observations about the second kind. Apart from the chain

$$2, 3, 5$$

the other Cunningham chains of the second kind start with an odd prime p_1 and must evidently satisfy $p_i = 2^i a + 1$ where $a = \frac{1}{2}(p_1 - 1)$. In particular, we observe:

> *A Cunningham chain of the second kind starting with an odd prime p_1 can have length at most $p_1 - 1$.*

Indeed, $p_i = 2^{i-1}(p_1 - 1) + 1 \equiv 1 - 2^{i-1}$ modulo p_1. This gives, by Fermat's little theorem, that p_1 divides p_{p_1} which cannot therefore be prime. Furthermore, the following restrictions are also easy to see by looking at the residues modulo 5:

> *For the respective congruence classes $p_1 \equiv 2, 4$ modulo 5, a chain of the second kind must have respective length at most 2 and 3. The only chain starting with a prime $p_1 \equiv 3$ modulo 5 is 3, 5. Thus, the only possibilities for arbitrarily long chains are when $p_1 \equiv 1$ modulo 5.*

Acknowledgement

Thanks are due to the referee who suggested that the connections with primes which arose in our study could merit more discussion. This resulted in the long-ish remark at the end of the Note.

References

1. W. R. Alford, A. Granville and C. Pomerance, There are infinitely

many Carmichael numbers, *Ann. Math.* **140** (1994) pp. 703-722.

2. Barry J. Powell, Primitive densities of certain sets of primes, *J. Number Theory* **12** (1980) pp. 210-217.
3. Paulo Ribenboim, *The new book of prime number records*, Springer-Verlag (1996).

B. SURY

Statistics & Mathematics Unit, Indian Statistical Institute,
8th Mile Mysore Road, Bangalore 560059, India

e-mail: *surybang@gmail.com*