CARMICHAEL NUMBERS AND KORSELT'S CRITERION

KEITH CONRAD

Fermat's little theorem says for a prime p and all integers $a \not\equiv 0 \bmod p$ that $a^{p-1} \equiv 1 \bmod p$. Conversely, if $n > 1$ and $a^{n-1} \equiv 1 \bmod n$ for all $a \not\equiv 0 \bmod n$ then n must be prime: from $a^{n-1} \equiv 1 \bmod n$ we get $(a, n) = 1$, so n is relatively prime to all integers from 1 to $n-1$, and thus n is a prime number.

While $a \not\equiv 0 \bmod p$ is the same as $(a, p) = 1$ when p is prime and a is any integer, the conditions $a \not\equiv 0 \bmod n$ and $(a, n) = 1$ are *not* the same when n is composite: $(a, n) = 1 \Rightarrow a \not\equiv 0 \bmod n$ but the converse is usually false (depending on a). If we write $a \not\equiv 0 \bmod p$ with $(a, p) = 1$ in Fermat's little theorem, making it "$(a, p) = 1 \Longrightarrow a^{p-1} \equiv 1 \bmod p$," we have an implication that is sometimes true if we replace prime p by composite n.

Definition 1. An integer $n > 1$ is called a *Carmichael number* if n is composite and $(a, n) = 1 \Longrightarrow a^{n-1} \equiv 1 \bmod n$ for all $a \in \mathbf{Z}$.

Initially it is not at all clear that there should be any Carmichael numbers, but the first few were found by Robert Carmichael [1], [2] in the early 20th century and they are

$$561, \ \ 1105, \ \ 1729, \ \ 2465, \ \ 2821.$$

It is possible to verify that an integer n is a Carmichael number without using the definition, so not having to check $a^{n-1} \equiv 1 \bmod n$ for all a that are relatively prime to n. Instead we can check a property of the prime factorization of n known as Korselt's criterion.

Theorem 2 (Korselt)**.** *A composite integer $n > 2$ is a Carmichael number if and only if (i) n is squarefree and (ii) for every prime p dividing n, also $(p-1) \mid (n-1)$.*

Proof. Assume n is a Carmichael number. First we will show n is squarefree. If a prime p divides n more than once, write $n = p^k n'$ where $k \geq 1$ and $(p, n') = 1$. We want to show $k = 1$, and will do this by contradiction using the Chinese remainder theorem.

Assume $k \geq 2$, so n is divisible by p^2. By the Chinese remainder theorem there is an $a \in \mathbf{Z}$ such that $a \equiv 1 + p \bmod p^k$ and $a \equiv 1 \bmod n'$. Then $(a, n) = 1$, so

$$a^{n-1} \equiv 1 \bmod n$$

by the definition of Carmichael numbers. Reduce the above congruence modulo p^2, getting $(1+p)^{n-1} \equiv 1 \bmod p^2$. By the binomial theorem, $(1+p)^{n-1} \equiv 1 + (n-1)p \bmod p^2$. Since n is divisible by p, $1 + (n-1)p \equiv 1 - p \bmod p^2$. Thus $1 - p \equiv 1 \bmod p^2$. This is a contradiction, so $k = 1$.

Next we show $(p-1) \mid (n-1)$ for each prime p dividing n. Since n is squarefree, p and n/p are relatively prime. Pick any $b \in \mathbf{Z}$ such that $b \bmod p$ has order $p-1$ (there is a primitive root modulo any prime). By the Chinese remainder theorem there's an $a \in \mathbf{Z}$ such that $a \equiv b \bmod p$ and $a \equiv 1 \bmod n/p$, so $(a, n) = 1$. Then $a^{n-1} \equiv 1 \bmod n$. Reducing both sides modulo p, $b^{n-1} \equiv 1 \bmod p$. This implies, by the choice of b, that $(p-1) \mid (n-1)$.

Now assume n is squarefree and $(p-1) \mid (n-1)$ for every prime p that divides n. We want to show n is Carmichael. If $a \in \mathbf{Z}$ satisfies $(a, n) = 1$ then for each prime p dividing n we have $(a, p) = 1$, so $a^{p-1} \equiv 1 \bmod p$. Since $p-1$ is a factor of $n-1$ we get $a^{n-1} \equiv 1 \bmod p$.

As this holds for all primes p dividing n, and n is squarefree, we get $a^{n-1} \equiv 1 \bmod n$. Also n is composite (hypothesis), so n is Carmichael. □

Korselt [4] proved this theorem about 10 years before Carmichael essentially rediscovered it [1], [2], but Korselt was unable to find examples of such numbers and that is why they are called Carmichael numbers. On that basis, however, these numbers should be called Šimerka numbers since V. Šimerka found the first 7 examples 25 years before Carmichael. Below is an excerpt from Šimerka's article [5], which appeared in a Czech math journal that was not widely read.

bývá. Tak na př. při $561 = 3 \,.\, 11 \,.\, 17$, $b = 2$ nalezneme

$$2_{10} = -98,\ 2_{20} = 67,\ 2_{40} = 1,\ (2_{40})^{14} = 2_{560} = 1.$$

Tolikéž u čísel

$$1105 = 5 \,.\, 13 \,.\, 17,\ 1729 = 7 \,.\, 13 \,.\, 19,\ 2465 = 5 \,.\, 17 \,.\, 29,$$
$$2821 = 7 \,.\, 13 \,.\, 31,\ 6601 = 7 \,.\, 23 \,.\, 41,\ 8911 = 7 \,.\, 19 \,.\, 67 \text{ a j. v.},$$

kdykoli b s modulem nesoudělné jest.

FIGURE 1. Carmichael numbers found by Šimerka before Carmichael.

Example 3. We use Korselt's criterion to verify a construction of Carmichael numbers due to Chernick [3]: if k is a positive integer such that $6k+1$, $12k+1$, and $18k+1$ are all prime then the product $n = (6k+1)(12k+1)(18k+1)$ is a Carmichael number. For instance, $7 \cdot 13 \cdot 19 = 1729$ is a Carmichael number.

The first condition of Korselt's criterion, that n be squarefree, obviously holds. To check the second criterion we want to show $n-1$ is divisible by $6k$, $12k$, and $18k$. Since $6 \mid 12$ it suffices to look at n mod $12k$ and n mod $18k$. Modulo $12k$ we have $n \equiv (6k+1)(6k+1) \equiv 1 \bmod 12k$, and modulo $18k$ we have $n \equiv (6k+1)(12k+1) \equiv 1 \bmod 18k$. Thus $n-1$ is divisible by the desired factors, so it is a Carmichael number when its three factors are all prime.

This method of Chernick is very convenient if you want to construct an example of a large Carmichael number, such as if you are giving a lecture on Carmichael numbers and want to give an example other than the same examples that are in all the books. Run a computer algebra package to find big k where $6k+1$, $12k+1$, and $18k+1$ are all prime (it's believed this should happen infinitely often, and in any case it usually doesn't take long to find such a choice of k), take their product, and you're done.

As an exercise, verify with Korselt's criterion that if $6k+1$, $12k+1$, $18k+1$, and $36k+1$ are all prime then their product is a Carmichael number.

Corollary 4. *A composite integer n is a Carmichael number if and only if $a^n \equiv a \bmod n$ for all $a \in \mathbf{Z}$.*

Proof. If $a^n \equiv a \bmod n$ for all $a \in \mathbf{Z}$, then when $(a, n) = 1$ we can cancel a from both sides and get $a^{n-1} \equiv 1 \bmod n$, so n is a Carmichael number since it is composite.

Conversely, assume n is Carmichael. To prove, for each $a \in \mathbf{Z}$, that $a^n \equiv a \bmod n$ it suffices since n is squarefree to prove $a^n \equiv a \bmod p$ for each prime p dividing n. This congruence is obvious if $a \equiv 0 \bmod p$. If $a \not\equiv 0 \bmod p$ then $a^{p-1} \equiv 1 \bmod p$ by Fermat's little theorem, and $p-1$ is a factor of $n-1$, so $a^{n-1} \equiv 1 \bmod p$, and thus $a^n \equiv a \bmod p$. □

Here are some further properties (but not characterizations) of Carmichael numbers.

Theorem 5. *Every Carmichael number n is odd, has at least three different prime factors, and every prime factor of n is less than $\sqrt{n}$.*

Proof. Since $n-1$ is relatively prime to n, we have $(n-1)^{n-1} \equiv 1 \bmod n$, so $(-1)^{n-1} \equiv 1 \bmod n$ and we know $(-1)^{n-1} = \pm 1$. Since $n > 2$ we have $-1 \not\equiv 1 \bmod n$, so $(-1)^{n-1} = 1$. Thus $n-1$ is even, so n is odd.

Suppose $n = pq$ for primes p and q. Since n is squarefree, $p \neq q$. We may assume without loss of generality that $p > q$. By Korselt's criterion, $(p-1) \mid (n-1)$. Since

$$\frac{n-1}{p-1} = \frac{pq-1}{p-1} = \frac{(p-1)q+q-1}{p-1} = q + \frac{q-1}{p-1},$$

we must have $(p-1) \mid (q-1)$. But this is impossible since $q-1 < p-1$. Thus n has at least three different prime factors.

If p is a prime factor of n, then

$$\frac{n-1}{p-1} = \frac{p(n/p)-1}{p-1} = \frac{(p-1)(n/p)+n/p-1}{p-1} = \frac{n}{p} + \frac{n/p-1}{p-1},$$

so $(p-1) \mid (n/p-1)$. Thus $p \leq n/p$, and the inequality must be strict (otherwise $n = p^2$, which is impossible), so $p < \sqrt{n}$. Incidentally, this gives another proof that n has at least three prime factors: if $n = pq$ with $p < \sqrt{n}$ and $q < \sqrt{n}$ then $n = pq < \sqrt{n}\sqrt{n} = n$, which is a contradiction. □

References

[1] R. D. Carmichael, *Note on a New Number Theory Function*, Bulletin Amer. Math. Soc. **16** (1910), 232–238.

[2] R. D. Carmichael, *On composite P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \bmod P$*, Amer. Math. Monthly **19** (1912), 22–27.

[3] J. Chernick, *On Fermat's simple theorem*, Bull. Amer. Math. Soc. **45** (1939), 269–274.

[4] A. R. Korselt, *Problème chinois*, L'intermédiaire des mathématiciens **6** (1899), 142–143.

[5] V. Šimerka *Zbytky z arithemetické posloupnosti* (*On the remainders of an arithmetic progression*), Časopis pro pěstování matematiky a fysiky **14** (1885), 221–225. Online at https://gdz.sub.uni-goettingen.de/id/PPN31311028X_0014.