Elem. Math. 68 (2013) 93 – 95
0013-6018/13/030093-3
DOI 10.4171/EM/227

© Swiss Mathematical Society, 2013

Elemente der Mathematik

On Korselt's criterion for Carmichael numbers

Wolfgang Knapp

Wolfgang Knapp studierte Mathematik und Physik in Tübingen und Chicago. Er promovierte 1971, und 1976 folgte die Habilitation. Nach einem Heisenberg-Stipendium der DFG wurde er 1982 Professor für Mathematik an der Universität Tübingen. Er forscht zur Gruppentheorie, Darstellungstheorie, Codierungstheorie und Zahlentheorie.

An easy but fundamental fact in elementary number theory is Fermat's little theorem:

> Let p be a prime number. Then for all (rational) integers x we have $x^p \equiv x \pmod{p}$ (or equivalently $x^{p-1} \equiv 1 \pmod{p}$ if p does not divide x).

It is clear from the definition of a prime number that an integer $n > 1$ is a prime number if and only if for all integers x not divisible by n the congruence $x^{n-1} \equiv 1 \pmod{n}$ holds. However, if only $x^{n-1} \equiv 1 \pmod{n}$ holds for all integers x which are coprime with n (i.e., $\gcd(x, n) = 1$), equivalently $x^n \equiv x \pmod{n}$ for all integers x coprime with n, then n need not be a prime number.

Composite positive integers n which have this last mentioned property are called *Carmichael numbers* in reference to Carmichael's article [3] of 1912.

In this way Carmichael numbers provide just the examples of composite positive integers n that pass all possible primality tests using Fermat's little theorem requiring $\gcd(x, n) = 1$ for the test input parameter x. All Carmichael numbers are odd, square-free and have at

Der Restklassenring $\mathbb{Z}/m\mathbb{Z}$ für eine natürliche Zahl $m > 1$ ist bekanntlich genau dann ein Körper, wenn m eine Primzahl ist. Hieraus ergibt sich der kleine Satz von Fermat: Wenn p eine Primzahl ist, so gilt die Kongruenz $x^p \equiv x \pmod{p}$ für alle ganzen Zahlen x. Man kann nun die Frage stellen, für welche natürlichen Zahlen m bei festem, gegebenem $n > 1$ die Kongruenzen $x^n \equiv x \pmod{m}$ für alle ganzen Zahlen x gelten. Diese Frage wird hier beantwortet, wobei sich enge Beziehungen zum kleinen Satz von Fermat, zu den sogenannten Carmichael-Zahlen und zum Korselt-Kriterium für Carmichael-Zahlen herausstellen. Entscheidend sind die Teilbarkeitsbeziehungen zwischen $q - 1$ und $n - 1$ für die Primteiler q von n.

least three prime factors, the smallest Carmichael number being $n = 561 = 3 \cdot 11 \cdot 17$. It is a deep and brilliant result of Alford, Granville and Pomerance that there are even infinitely many Carmichael numbers, see [1].

All theorems on Carmichael numbers are based on their characterization by *Korselt's criterion* which (in our terminology) tells that a composite positive integer n is a Carmichael number if and only if n is square-free and $p - 1$ divides $n - 1$ for every prime divisor p of n, see [5]. Note that Carmichael rediscovered Korselts's criterion much later, but apparently he was not aware in his 1912 paper [3] of Korselt's previous result of 1899 given in [5]. Thus Carmichael numbers maybe should rather be called Korselt numbers in order to acknowledge that Korselt was the first author who studied these numbers and obtained their characterization.

Korselt's criterion is well known in the literature. On the other hand it seems to be less known that it admits an easy but interesting generalization. In the present short note the following extension of Korselt's criterion is established. Some facts which might lead to the idea of this generalization can be found in several exercises given in a few textbooks on elementary number theory, e.g., in [4, Übung 7.2 a) and b)] or [7, p. 159].

In the following, as usual, $\mathbb{N}$ denotes the set of natural numbers and $\mathbb{Z}$ denotes the set of (rational) integers.

Theorem. *Suppose n is an integer ≥ 2. Let $\Phi(n)$ denote the set of all prime numbers p such that $p - 1$ divides $n - 1$. Then there exists a unique positive integer $\kappa(n)$ with the following property:*

If for any positive integer m the congruence $x^n \equiv x \pmod{m}$ holds for all $x \in \mathbb{Z}$ then m divides $\kappa(n)$; hence $\kappa(n)$ is the largest integer with this property. Moreover, we have $\kappa(n) = \prod_{p \in \Phi(n)} p$.

$\kappa(n)$ is called the Korselt indicator *of n.*

Proof. As usual, write $x \mid y$ to indicate that x divides y, with corresponding notation for the negation. Set $\kappa(n) := \prod_{p \in \Phi(n)} p$.

(i) If $p \in \Phi(n)$ then $x^n \equiv 0 \equiv x \pmod{p}$ holds if $p \mid x$ and if $p \nmid x$ then by Fermat's little theorem $x^{n-1} = x^{(p-1)t} \equiv 1^t = 1 \pmod{p}$ where $n - 1 = (p - 1)t$. It follows that $x^n \equiv x \pmod{p}$ holds for all $x \in \mathbb{Z}$ and therefore $x^n \equiv x \pmod{\kappa(n)}$ for all $x \in \mathbb{Z}$.

(ii) Conversely suppose that $m \in \mathbb{N} \setminus \{0, 1\}$ has the property that $x^n \equiv x \pmod{m}$ for all $x \in \mathbb{Z}$.

If m were not square-free, i.e., divisible by the square of a prime p, then we would have $x^n \equiv x \pmod{p^2}$ for all $x \in \mathbb{Z}$, hence also $p^n \equiv p \pmod{p^2}$, thus $(p^{n-1} - 1)p \equiv 0 \pmod{p^2}$ and therefore $p^{n-1} \equiv 1 \pmod{p}$, a contradiction. So m is necessarily square-free.

If p is a prime divisor of m then for all $x \in \mathbb{Z}$ we have $x^n \equiv x \pmod{p}$. But there exists a primitive root a modulo p, i.e., the order of $a + p\mathbb{Z}$ in the group of units in $\mathbb{Z}/p\mathbb{Z}$ is $p - 1$. So we have $a^{n-1} \equiv 1 \pmod{p}$, hence $p - 1 \mid n - 1$. It follows $p \in \Phi(n)$ and finally $m \mid \kappa(n)$ since m is square-free. The theorem follows. □

Note that $\kappa(n)$ divides $n!$ by its very definition. There are some easy consequences worth noticing: the following assertion (i) is essentially a restatement of Korselt's criterion whereas assertion (ii) reflects the well known fact that Carmichael numbers are odd.

Corollaries. *Let n be an integer ≥ 2. Let $\mathbb{P}$ denote the set of prime numbers. Then the following hold.*

(i) *n is a prime number or a Carmichael number if and only if n divides $\kappa(n)$.*

(ii) *n is even if and only if $\kappa(n) = 2$. n is odd if and only if 6 divides $\kappa(n)$.*

(iii) *If $n = 2^b + 1$ for $b \in \mathbb{N}$ then $\Phi(n) = \{2\} \cup \{p \in \mathbb{P} \mid p$ is a Fermat prime $\leq n\}$; $\kappa(n)$ is bounded by a constant as a function of b if and only if there exist only finitely many Fermat primes.*

Proof. (i) is an immediate consequence of the theorem and the definition of prime numbers and Carmichael numbers; clearly it implies Korselt's criterion. (ii) and (iii) are easily verified. □

Remark. Computations of the Korselt indicator $\kappa(n)$ suggest that there might be infinitely many (odd composite) natural numbers such that $\kappa(n) = 6$.

Acknowledgement. The author thanks the referee for useful suggestions concerning the presentation.

References

[1] W. ALFORD, A. GRANVILLE, C. POMERANCE: There are infinitely many Carmichael numbers, Ann. of Math. 139, 703–722 (1994).

[2] R. CANDALL, C. POMERANCE: Prime Numbers, a computational perspective. Springer Verlag 2001.

[3] R.D. CARMICHAEL: On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$, American Mathematical Monthly **19** (2) 22–27 (1912).

[4] O. FORSTER: Algorithmische Zahlentheorie, Verlag Vieweg 1996.

[5] A. KORSELT: Problème Chinois, L'intermédiaire des mathématiciens 6, 142–143 (1899).

[6] P. RIBENBOIM: The New Book of Prime Number Records, Springer Verlag 1988–1996.

[7] H. SCHEID, A. FROMMER: Zahlentheorie, Spektrum Akademischer Verlag 2007.

Wolfgang Knapp
Universität Tübingen
Mathematisches Institut
Auf der Morgenstelle 10
D-72076 Tübingen, Germany