ON GENERALIZED CARMICHAEL NUMBERS

BY

Lorenz Halbeisen and Norbert Hungerbühler

ABSTRACT. For arbitrary integers $k \in \mathbb{Z}$ we investigate the set C_k of the generalized Carmichael numbers, i.e. the natural numbers $n > \max\{1, 1-k\}$ such that the equation $a^{n+k} \equiv a \mod n$ holds for all $a \in \mathbb{N}$. We give a characterization of these generalized Carmichael numbers and discuss several special cases. In particular, we prove that C_1 is finite and that C_k is infinite, whenever $1-k > 1$ is square-free. We also discuss generalized Carmichael numbers which have one or two prime factors. Finally, we consider the Jeans numbers, i.e. the set of odd numbers n which satisfy the equation $a^n \equiv a \mod n$ only for $a = 2$, and the corresponding generalizations. We give a stochastic argument which supports the conjecture that infinitely many Jeans numbers exist which are squares.

1 Introduction: Historical Background

On October 18th, 1640, Pierre de Fermat wrote in a letter to Bernard Frenicle de Bessy that if p is a prime number, then p divides $a^{p-1} - 1$ for all integers a not divisible by p, a result now known as "Fermat's Little Theorem". An equivalent formulation is the assertion that p divides $a^p - p$ for all integers a, whenever p is prime. Fermat's remark to Frenicle proved one half of what has been called the Chinese hypothesis which dates from about 2000 years earlier[†], that an integer n is prime if and only if $2^n - 2$ is divisible by n. The other half of this is false, since, for example, $2^{341} - 2$ is divisible by $341 = 11 \times 31$ (and this is the smallest counter example as noted by J. H. Jeans in [Je1898]). The question arose whether all integers n satisfying the stronger requirement of the Fermat congruence, namely

$$a^n \equiv a \mod n \qquad \text{for all integers } a, \tag{1}$$

are prime (this rules out at least the example $n = 341$, since $3^{341} \equiv 168 \mod 341$). However, also this implication turned out to be false. This was noticed by R. D. Carmichael in 1910 who pointed out in [Ca1910] that $561 = 3 \times 11 \times 17$ divides $a^{561} - a$ for all integers a. In 1899 already, Korselt had noted in [Ko1899] that one could easily test for such integers by using (what is now called)

Korselt's Criterion: n divides $a^n - a$ for all numbers $a \in \mathbb{N}$, if and only if n is square-free and $p - 1$ divides $n - 1$ for all primes p dividing n.

In a series of papers around 1910, Carmichael began an in-depth study of composite numbers with this property, which have become known as **Carmichael numbers**. In [Ca1912], Carmichael exhibited an algorithm to construct such numbers and stated, perhaps somewhat wishfully, that "*this list* (of Carmichael numbers) *might be indefinitely extended*". However, this conjecture remained open during almost the whole century until it was positively proved in [AGP1994].

*Received on 04-01-2000

1991 *Mathematics Subject Classification* **11A51** 11A07 11N25

The first author wishes to thank the *Swiss National Science Foundation* for supporting him.

†J. H. Jeans states in [Je1898]: "A paper fond among those of the late Sir Thomas Wade, and dating from the time of Confucius, contains the theorem, that $2^{n-1} - 1 \equiv 0 \mod n$ when n is prime, and also states that it does not hold if n is not a prime." Other sources impute this statement to an erroneous translation and point out that the ancient Chinese did never even formulate the concept of prime numbers (see [Ri1989]).

The other line we want to follow in this exposition is this: For addition, multiplication and exponentiation, we have the well known reduction formulas[‡]:

$$
\begin{aligned}
a+b &\equiv \mathrm{Mod}(a,n)+\mathrm{Mod}(b,n) \mod n &(2)\\
a\cdot b &\equiv \mathrm{Mod}(a,n)\cdot\mathrm{Mod}(b,n) \mod n &(3)\\
a^b &\equiv \mathrm{Mod}(a,n)^b \mod n &(4)
\end{aligned}
$$

It is much more difficult to find reduction formulas which allow to reduce the *exponent.* Of course in general

$$a^b \not\equiv a^{\mathrm{Mod}(b,n)} \mod n. \tag{5}$$

It is easy to see, that the numbers n for which the reduction formula (5) holds generally are precisely the numbers n for which

$$a^{n+1} \equiv a \mod n \qquad \text{for all integers } a. \tag{6}$$

The set of numbers with the property (6) is surprisingly short (compared to the infinite list of the Carmichael numbers) and will be determined below.

Comparing (1) and (6), the following generalization of the Carmichael numbers emerges very naturally:

$$\mathrm{C}_k := \left\{n\in\mathbb{N} : \min\{n,n+k\}>1 \text{ and } a^{n+k}\equiv a \mod n \text{ for all } a\in\mathbb{N}\right\}$$

So, the original Carmichael numbers together with all primes form the set C_0, and the numbers with the reduction property (6) are the numbers in C_1.

It will turn out that it is useful to consider the following function[§] defined for natural numbers $n>1$:

$$g(n) := \begin{cases} \mathrm{lcm}\{p-1 : p \text{ prime and } p\mid n\} & \text{if } n \text{ is square free}\\ \infty & \text{otherwise}\end{cases}$$

For $\ell\in\mathbb{Z}$ we say that $n\in\mathbb{N}$ is an **ℓ-number**, if $g(n)\mid n+\ell$ and $n>\max\{1,-\ell\}$.

The rest of this paper is organized as follows: In Section 2 we give a characterization of the generalized Carmichael numbers and establish contact with the function g. In Section 3 we discuss several special cases and prove in particular, that C_1 is finite and that C_k is infinite whenever $1-k>1$ is square-free. In Section 4 we discuss generalized Carmichael numbers which have one or two prime factors. Finally, in Section 5, we consider the Jeans numbers, i.e. the set of odd numbers n which satisfy the equation $a^n\equiv a \mod n$ only for $a=2$, and the corresponding generalizations. We give a stochastic argument which supports the conjecture that infinitely many Jeans numbers exist which are squares.

[‡]Here, by $\mathrm{Mod}(a,n)$ we mean the uniquely determined number $r\in\{1,\dots,n\}$ such that $a=kn+r$ for some $k\in\mathbb{Z}$.

[§]lcm denotes the **l**east **c**ommon **m**ultiple, and we write $a\mid b$ for $a,b\in\mathbb{Z}$ with $\frac{b}{a}\in\mathbb{Z}$.

2 Korselt's Criterion Generalized

Korselt's original criterion (see Section 1) characterizes the set C_0 of Carmichael and prime numbers. It turns out that a properly generalized version of Korselt's criterion, as stated in Theorem 2.1, characterizes the generalized Carmichael numbers C_k:

Theorem 2.1 *Let $k \in \mathbb{Z}$ be any fixed integer. Then the natural number n belongs to C_k if and only if*
(α) $n > \max\{1, 1-k\}$,
(β) n is square-free and
(γ) $p - 1 \mid n + k - 1$ for all primes p dividing n.

It is sometimes useful to replace condition (γ) by an equivalent condition, namely

Lemma 2.2 *For all fixed $k, n \in \mathbb{Z}$, the following conditions are equivalent:*
(γ) $p - 1 \mid n + k - 1$ for all primes p dividing n.
(γ') $p - 1 \mid \frac{n}{p} + k - 1$ for all primes p dividing n.

Proof. Let p be a prime dividing n and let $m = \frac{n}{p}$. Now we get $p - 1 \mid mp + k - 1 \iff p - 1 \mid \big(pm + p(k-1) - (p-1)(k-1)\big) \iff p - 1 \mid pm + p(k-1)$ and because p is prime, this is equivalent to $p - 1 \mid m + k - 1$. **q.e.d.**

So, our second formulation of the generalized Korselt criterion reads as follows:

Theorem 2.3 *Let $k \in \mathbb{Z}$ be any fixed integer. Then the natural number n belongs to C_k if and only if*
(α) $n > \max\{1, 1-k\}$,
(β) n is square-free and
(γ') $p - 1 \mid \frac{n}{p} + k - 1$ for all primes p dividing n.

The proof of the Theorems 2.1 and 2.3—which are equivalent by Lemma 2.2—is given in the following lemmas. First, we address the implication which assumes $n \in \mathrm{C}_k$. (α) follows directly from the definition of C_k. (β) is proven in the next lemma:

Lemma 2.4 *If $n \in \mathrm{C}_k$, then n is square-free.*

Proof. Assume the contrary, then there exists an $n \in \mathrm{C}_k$ and a prime p such that $p^2 \mid n$ and for all $a \in \mathbb{N}$ we have $a^{n+k} \equiv a \mod n$. Notice that $n \in \mathrm{C}_k$ implies $n + k > 1$. Now, for $a = p$ we get $p^{n+k} - p = p(p^{n+k-1} - 1)$ which implies that $p^2 \nmid p^{n+k} - p$ and therefore, $n \nmid p^{n+k} - p$, which is a contradiction to the requirement that for all $a \in \mathbb{N}$ there holds $n \mid a^{n+k} - a$. **q.e.d.**

To prepare the proof of (γ), we need the following lemma:

Lemma 2.5 *If p is prime and $0 < r < p-1$, then there is an $a \not\equiv 0 \mod p$ such that $a^r \not\equiv 1 \mod p$.*

Proof. Assume not, then the polynomial $x(x^r - 1) = x^{r+1} - x \equiv 0 \mod p$ (for all x) is a non-trivial normed null-polynomial of degree less than p. But this is a contradiction to [HHL1999, Theorem 7], which states that the minimal degree of a non-trivial normed null-polynomial modulo p is equal to p, if p is prime.
q.e.d.

Now, (γ) is proven in the next lemma:

Lemma 2.6 *If $n \in \mathrm{C}_k$, then $p - 1 \mid n + k - 1$ for all primes p dividing n.*

Proof. Assume there exists an $n \in \mathrm{C}_k$ for which we find a prime p dividing n such that $p-1 \nmid n+k-1$. Then it follows that $n \geq 3$ and that for a natural number r with $0 < r < p-1$ we have $n + k - 1 = (p - 1)h + r$ for an $h \in \mathbb{N}$. Let $a \not\equiv 0 \mod p$ be such that $a^r \not\equiv 1 \mod p$ (see Lemma 2.5). So, by Fermat's Little Theorem (since p is prime and (a, p)[¶] $= 1$), we get $a^{n+k} = (a^{p-1})^h \cdot a^r \cdot a \equiv a^{r+1} \not\equiv a \mod p$. Hence, $n \nmid a^{n+k} - a$ which contradicts $n \in \mathrm{C}_k$. **q.e.d.**

Now, we prove the opposite implication in Theorem 2.1. First, we state the following lemma:

Lemma 2.7 *Let $k, n \in \mathbb{Z}$ and p a prime dividing n such that $p - 1 \mid n + k - 1$. Then, for all $a \in \mathbb{N}$ with $(a, p) = 1$, we have $a^{n+k} \equiv a \mod p$.*

Proof. By the premise we have $n + k = (p - 1)h + 1$ for some h and therefore, $a^{n+k} = (a^{p-1})^h \cdot a \equiv a \mod p$ (by Fermat's Little Theorem). **q.e.d.**

Conclusion. Now, assume (α), (β) and (γ). Since n is square-free, in order to conclude $n \in \mathrm{C}_k$, which is equivalent to $a^{n+k} \equiv a \mod n$ (for all $a \in \mathbb{N}$), it suffices to show that for all $a \in \mathbb{N}$ and for all primes p dividing n we have $a^{n+k} \equiv a \mod p$. If $(a, p) = 1$, the congruence follows from Lemma 2.7, and otherwise it is trivial. This completes the proof of the generalized version of Korselt's criterion.

For completeness, let us state the following lemma:

Lemma 2.8 *If $n \in \mathrm{C}_k$ and $(a, n) = 1$, then $a^{n+k-1} \equiv 1 \mod n$.*

Proof. This follows immediately from the fact that the residues which are relatively prime to n are a multiplicative group modulo n. **q.e.d.**

Now, we formulate the connection between the generalized Carmichael numbers and the function g introduced at the end of Section 1.

[¶] (a, b) denotes the greatest common divisor of the natural numbers a and b.

Theorem 2.9 *The number n belongs to $\mathrm{C}_{\ell+1}$ if and only if n is an ℓ-number.*

Proof. Let $n \in \mathbb{N}$ with $n > \max\{1, -\ell\}$ be given. Since the statement of the theorem is trivial if n contains a square, we may assume that n is square-free. So, according to Theorem 2.1, we simply have to check that $g(n) \mid n + \ell$ if and only if $p - 1 \mid n + \ell$ for all prime divisors p of n. But this follows directly from the definition of the function g. **q.e.d.**

Theorem 2.9 answers in particular the question to which C_k a given number n belongs, namely precisely to all C_k with $k = 1 - n + m \cdot g(n)$, where $m = 1, 2, 3, \ldots$. We should also remark explicitly that g can alternatively be defined by

$$g(n) = \min\{m > 1 : a^m = a \mod n \text{ for all } a\} - 1.$$

3 Special Cases

In this section we consider the set C_k for certain k's.

3.1 The case $k = 0$

Since, by Fermat's Little Theorem, for every prime p we have $a^p \equiv a \mod p$ (for all $a \in \mathbb{N}$), every prime belongs to C_0. In [AGP1994] it is shown that the set C_0 contains also infinitely many composite numbers (the Carmichael numbers).

3.2 The case $k = 1$

It is shown in [HHL1999] that $\mathrm{C}_1 = \{2, 6, 42, 1806\}$. Here, we give a new and simpler proof of this result by using the generalized Korselt criterion for C_1.

Theorem 3.1 $\mathrm{C}_1 = \{2, 6, 42, 1806\}$.

Proof. First remember that each member of C_1 is square-free. If a prime p belongs to C_1, then by Theorem 2.1 we have $p - 1 \mid p$, which implies $p = 2$. Hence, 2 is the only prime belonging to C_1. If $p < q$ are two primes and $pq \in \mathrm{C}_1$, then we get by Theorem 2.3 that $p - 1 \mid q$ and $q - 1 \mid p$. By $p - 1 \mid q$ we get $p - 1 = 1$ or $p = q + 1$, but we assumed $p < q$, so $p = 2$; and by $q - 1 \mid 2$ we must have $q = 3$. Hence, 6 is the only member of C_1 which is a product of two primes. Now assume $p < q < r$ are three primes and $pqr \in \mathrm{C}_1$. Because $p - 1 \mid qr$ and both q and r are greater than p we get $p = 2$. By $q - 1 \mid 2r$ we get, since $q < r$, $q = 3$. Finally, by $r - 1 \mid 6$ and because $r > 3$ we get $r = 7$. Hence, 42 is the only member of C_1 which is a product of three primes. Assume now $p < q < r < s$ are four primes such that $pqrs \in \mathrm{C}_1$. By $p - 1 \mid qrs$ we get again $p = 2$, by $q - 1 \mid 2rs$ we get $q = 3$, by $r - 1 \mid 6s$ we get $r = 7$ and by $s - 1 \mid 42$ we get $s = 43$. Hence, 1806 is the only member of C_1 which is a product of four primes. For five (or more) primes $p < q < r < s < t$ we get again $p = 2$, $q = 3$, $r = 7$ and $s = 43$. Thus, $t > 43$ and $t - 1 \mid 2 \cdot 3 \cdot 7 \cdot 43$, which implies

$t \in \{87, 259, 603, 1807\}$, and therefore, t is not prime. This shows that there is no number in C_1 which is a product of five or more distinct primes. **q.e.d.**

Remark: In [AGP1994, page 708] it is claimed that for $b = 0$ and $b = 1$ and for any fixed nonzero integer a, there are infinitely many square-free, composite integers n such that $p - a \mid n - b$ for all primes p dividing n. However, as we have seen in Theorem 3.1, for $a = 1$ and $b = 0$ there are only finitely many such numbers. For b other than 0 or 1 the corresponding statement is open. Below we prove at least for $a = 1$ and several special b that there are infinitely many composite, square-free numbers n having the corresponding property.

3.3 The case $1 - k > 1$ square-free

Theorem 3.2 *If $1 - k > 1$ is square-free, then C_k is an infinite set. In particular*

(a) for each prime number $n \nmid 1 - k$ of the form $n = 1 + s\,g(1 - k)$, or

(b) for each composite number $n \in \mathrm{C}_0$ with $g(1 - k) \mid g(n)$ and $(1 - k, n) = 1$,

the number $n(1 - k)$ belongs to C_k.

Before we start with the proof of Theorem 3.2, we note the following property of the function g which follows immediately from its definition. Namely, we observe that

$$g(mn) = \frac{g(m)g(n)}{(g(m), g(n))} \tag{7}$$

whenever m and n are square-free numbers with $(m, n) = 1$. *Proof.* Let $m = 1 - k > 1$ be a square-free number. Moreover, let $n \nmid m$ be a prime number of the form $n = 1 + s\,g(m)$ (according to Dirichlet's result from 1837[‖], there exist infinitely many such numbers n) or, more generally, let $n \in \mathrm{C}_0$ be such that $g(m) \mid g(n)$ and $(m, n) = 1$. Then we have $(g(m), g(n)) = g(m)$ and hence, because of (7),

$$g(mn) = g(n) \mid m(n - 1).$$

In view of Theorem 2.9 this proves the claim. **q.e.d.**

Remark: We call the numbers $n(1 - k) \in \mathrm{C}_k$ with n prime, which we found in Theorem 3.2, **primitive**. Thus, these infinitely many primitive numbers correspond to case (a) in Theorem 3.2. The question arises, whether besides these primitive numbers, there are other members of C_k, for example if case (b) actually does occur.

From Theorem 3.2(a) we immediately obtain for $k = -1$, that $2p \in \mathrm{C}_{-1}$ (where p is any odd prime). Using Theorem 3.2(b), we can prove that apart from the primitive numbers $2p$ (p prime), there are infinitely many other elements in C_{-1}:

Proposition 3.3 *If $n \in \mathrm{C}_0$ is odd, then $2n \in \mathrm{C}_{-1}$. In particular, there are infinitely many non-primitive elements in C_{-1}.*

[‖]There are infinitely many primes in any arithmetic progression $b, b + d, b + 2d, \ldots$, where $(b, d) = 1$

Proof. If $n > 2$ is prime, then $2n \in \mathrm{C}_{-1}$ by Theorem 3.2(a). If $n \in \mathrm{C}_0$ is a composite number, in other words, if n is one of the infinitely many Carmichael numbers (and hence odd), then $2n \in \mathrm{C}_{-1}$ by Theorem 3.2(b). **q.e.d.**

From Theorem 3.2(a) we obtain for $k = -2$, that $3p \in \mathrm{C}_{-1}$ (for any prime $p > 3$). Again, by Theorem 3.2(b), we get the following slightly stronger result:

Proposition 3.4 *If $3 < n \in \mathrm{C}_0$, n not a multiple of 3, then $3n \in \mathrm{C}_{-2}$.*

Proof. If $n > 3$ is prime, then $3n \in \mathrm{C}_{-2}$ by Theorem 3.2(a). If $3 < n \in \mathrm{C}_0$ is a composite number and not a multiple of 3, then $3n \in \mathrm{C}_{-2}$ by Theorem 3.2(b). **q.e.d.**

Similarly, for $k = -5$, we obtain from Theorem 3.2:

Proposition 3.5 *If $n \in \mathrm{C}_0$ is neither divisible by 2 nor by 3, then $6n \in \mathrm{C}_{-5}$.*

The cases $k = -6, -12, -18, -36$ allow us to make contact to a construction for Carmichael numbers which goes back to Chernick: He observed in [Ch1939] that if the numbers $p = 1 + 6m$, $q = 1 + 12m$ and $r = 1 + 18m$ are all prime, then $n = pqr$ is a Carmichael number**. The first values for m such that the corresponding triplet consists of primes are $m = 1, 6, 35, 45, 51, 55, 56, 100, \ldots$. It is widely believed that there exist infinitely many values of m with this property (usually it is accredited to an extended Hardy-Littlewood prime k-tuple conjecture). For these special Carmichael numbers, we have the following

Proposition 3.6 *If $p = 1 + 6m$, $q = 1 + 12m$ and $r = 1 + 18m$ are prime numbers, and hence $n = pqr \in \mathrm{C}_0$, then $7n \in \mathrm{C}_{-6}$ if $m > 1$, $13n \in \mathrm{C}_{-12}$ if $m > 2$, $19n \in \mathrm{C}_{-18}$ if $m > 3$, and $37n \in \mathrm{C}_{-36}$ if $m > 6$.*

Proof. Again, the claims follow easily from Theorem 3.2(a). Observe, that $g(n) = 36m$. **q.e.d.**

Remark: If, in Proposition 3.6, $m > 5$ is a multiple of 5, then $31n \in \mathrm{C}_{-30}$.

The condition (b) in Theorem 3.2 is certainly not optimal. For illustration, consider the case $k = -9$: Here we have the following

Proposition 3.7 *If $n \in \mathrm{C}_0$ is neither divisible by 2 nor by 5, then $10n \in \mathrm{C}_{-9}$.*

Proof. We have, according to (7), that $g(10n) \mid 2g(n)$ and since $g(n) \mid n-1$, $2g(n) \mid 10(n-1)$. **q.e.d.**

A similar example is the case $k = -20$: Here we have the following

Proposition 3.8 *If $n \in \mathrm{C}_0$ is neither divisible by 2, nor by 3, nor by 7, then $21n \in \mathrm{C}_{-20}$.*

Proof. We have $g(21n) \mid 3g(n)$ and since $g(n) \mid n - 1$, $3g(n) \mid 21(n - 1)$. **q.e.d.**

**Actually, Chernick's theorem is more general and the special case that we mention here follows immediately from Korselt's criterion.

4 Short products in C_k

In this section, we investigate numbers $n \in \mathrm{C}_k$ which are the product of few (distinct) primes. To warm up, we consider the case of one prime factor $n = p \in \mathrm{C}_k$. A necessary condition is that $p-1 \mid p+k-1$. Hence, $\alpha(p-1) = p+k-1$ for some $\alpha = 1, 2, 3, \ldots$. In case $\alpha = 1$, we conclude $k = 0$, and we know, that C_0 contains all prime numbers. If $\alpha \neq 1$, we can solve for p and obtain $p = 1 + \frac{k}{\alpha-1}$. If $k \geq 1$, this is maximal for $\alpha = 2$ and hence, we have

Proposition 4.1 *If $k \geq 1$ and $p \in \mathrm{C}_k$ is prime, then $p \leq 1 + k$. In particular, C_k contains only finitely many prime numbers.*

For $k \leq -1$ we obtain

Proposition 4.2 *C_k does not contain prime numbers for $k \leq -1$.*

No we consider $n \in \mathrm{C}_k$ which are the product of two (distinct) primes, say $2 \leq p < q$. From the generalized Korselt criterion (Theorem 2.3) we infer that

$$\begin{array}{rcl} p-1 & \mid & q+k-1 \\ q-1 & \mid & p+k-1, \end{array}$$

and hence,

$$\alpha(p-1) = q+k-1 \tag{8}$$
$$\beta(q-1) = p+k-1 \tag{9}$$

for some $\alpha, \beta \in \mathbb{N}$. Let us first discuss the case $\alpha\beta = 1$:

First case $\alpha = \beta = 1$: By adding (8) and (9), it follows that $k = 0$ and subsequently we get $p = q$. In other words, this case does not occur.

Second case $\alpha = \beta = -1$: Here, (8) and (9) are equivalent and we have the condition $p + q = 2 - k$, and in particular, $k \leq -3$. Therefore, we get

Proposition 4.3 *If $p < q$ are both prime, then $pq \in \mathrm{C}_{2-p-q}$.*

Of course, this follows also immediately from Theorem 2.3.

From now on, we assume $\alpha\beta \neq 1$. Solving (8) and (9) for p and q, we obtain

$$\begin{aligned} p &= 1 + k\frac{\beta+1}{\alpha\beta-1} \\ q &= 1 + k\frac{\alpha+1}{\alpha\beta-1}. \end{aligned}$$

Thus, we have the conditions

$$\begin{aligned} k\frac{\beta+1}{\alpha\beta-1} &= 1 + r \\ k\frac{\alpha+1}{\alpha\beta-1} &= k\frac{\beta+1}{\alpha\beta-1} + 1 + s \end{aligned}$$

for some real numbers $r, s \geq 0$. Now, for given k we ask what values of α and β (and subsequently for p and q) are still possible. Obviously, for $k = 0$ the set of possible α and β is empty. Hence (together with the case $\alpha\beta = 1$), an immediate conclusion is that no number in C_0 can have precisely two prime factors. Expressing everything in r and s, we have

$$\begin{aligned} \alpha &= 1 + \frac{1+k+s}{1+r} \\ \beta &= \frac{1+k+r}{2+r+s} \\ p &= 2+r \\ q &= 3+r+s\,. \end{aligned}$$

If we consider first the case $k \geq 1$, we see, that p is maximal, if r is maximal, which happens (since $\alpha \in \mathbb{N}$) for $\alpha = 2$, i.e., for $k + s = r$. Then, $\beta = \frac{1+2k+s}{2+k+2s} \geq 1$, or $s = k\frac{2-b}{2b-1} - 1$, and hence $r = k\frac{\beta+1}{2\beta-1} - 1$. This is maximal for $\beta = 1$ and we obtain $p \leq 2k+1$. A similar reasoning gives $q \leq 3k+1$. Hence, we obtain

Proposition 4.4 *If $k \geq 1$ and $p < q$ prime such that $pq \in \mathrm{C}_k$, then $p \leq 2k+1$ and $q \leq 3k+1$. In particular, only finitely many members of C_k consist of precisely two prime factors.*

For $k \leq -1$ we first observe, that $\beta \leq 0$. Now, if $\beta = 0$, then $r = -1-k$, $\alpha = -\frac{s+1}{k}$ and hence $p = 1-k$ and $q = 1-k(\alpha+1) = 1+(p-1)\alpha'$ for $\alpha' = 2, 3, \ldots$. This is precisely what we also have from Theorem 3.2(a) in case $1-k$ prime.

Finally, we consider the case $\beta < 0$: Similar arguments as above in the discussion of $k \geq 1$ lead to the following result: $p \leq 1 - \frac{k}{5}$ and $q \leq \frac{1-k}{2}$. Summarizing, we have:

Proposition 4.5 *Let $k \leq -1$ and $p < q$ both prime such that $pq \in \mathrm{C}_k$. Then*

(a) $p = 1-k$ and $q = 1 + h(p-1)$ for some $h = 2, 3, \ldots$, or

(b) $p \leq 1 - \frac{k}{5}$ and $q \leq \frac{1-k}{2}$.

In particular, if $1-k$ is not prime, then only finitely many elements of C_k have exactly two prime factors.

5 When $a = 2$

In this section we come back to the Chinese hypothesis and the observation of Jeans (see Section 1). We consider the set of odd numbers n for which the equation $2^n \equiv 2 \mod n$ holds. First we note the following

Fact 5.1 *For an odd number n we have $2^n \equiv 2 \mod n$ if and only if $2^{n-1} \equiv 1 \mod n$.*

Proof. This follows immediately from the fact that the residues which are relatively prime to n are a multiplicative group modulo n. **q.e.d.**

At the end of the 19th century, Jeans investigated the set of composite odd numbers n, such that $2^{n-1} \equiv 1 \mod n$ (see [Je1898]). Let us denote the set of all these numbers by J_0 and if $n \in J_0$, then we call n a $\boldsymbol{J_0}$**-number**, or just a $\boldsymbol{J}$**-number**. In general,

$$J_k := \left\{n \in \mathbb{N} : \min\{n, n+k\} > 1 \text{ and } n+k \text{ is odd and } 2^{n+k} \equiv 2 \mod n\right\}.$$

5.1 On the set of J-numbers

To investigate the set J, let us recall first some notations and basic facts.

The Euler ϕ function: For $n \in \mathbb{N}$, $\phi(n)$ is defined to be the number of integers between 1 and n relatively prime to n. For example, $\phi(1) = 1$, $\phi(6) = 2$, and if p is a prime, then $\phi(p) = p - 1$.

Primitive roots and orders: Let $a, n \in \mathbb{N}$ and $(a, n) = 1$, then we say a has **order** h mod n, if h is the smallest positive integer such that $a^h \equiv 1 \mod n$. This h is denoted by $\text{ord}_a(n)$. If $h = \phi(n)$, where a and n are as above, then a is called a **primitive root mod** $\boldsymbol{n}$. It is well-known that for every prime number there is a primitive root. Moreover, for p prime there are $\phi(p-1)$ primitive roots for p. But on the other hand, there is no simple way of finding primitive roots for some p, even if p is prime, and for small primes trial and error is probably as good a method as any. Hence, there is no simple function which calculates $\text{ord}_2(p)$, for any odd prime p. At this point we like to mention Artin's conjecture which states that if $a > 1$ is not a square, then there are infinitely many primes for which a is a primitive root.

For odd numbers n we get by Euler's Theorem that $2^{\phi(n)} \equiv 1 \mod n$, and therefore, $\text{ord}_2(n) \mid \phi(n)$. Thus, for odd primes p we have $\text{ord}_2(p) \mid p - 1$.

Pseudoprimes: A composite integer n is called a **pseudoprime to the base** $\boldsymbol{a}$ if $a^{n-1} \equiv 1 \mod n$. So, a composite n is a J-number if and only if n is odd and a pseudoprime to the base 2. One can show that for each integer $a > 1$, there are infinitely many pseudoprimes n to the base a, namely

$$n = \frac{a^p - 1}{a - 1}\frac{a^p + 1}{a + 1},$$

where p is an odd prime not dividing $a(a^2 - 1)$ (see e.g. [Re1996, p. 125]).

Thus, there are infinitely many composite J-numbers.

Lemma 5.2 *If n is odd and square-free, then $2^{n-1} \equiv 1 \mod n$ if and only if for each prime p dividing n, $\text{ord}_2(p) \mid n - 1$.*

Proof. Let p be a prime dividing n. If $\text{ord}_2(p) \mid n - 1$, then, for some $h \in \mathbb{N}$, $2^{n-1} = 2^{h \cdot \text{ord}_2(p)} = \left(2^{\text{ord}_2(p)}\right)^h \equiv 1 \mod p$. On the other hand, if $2^{n-1} \equiv 1 \mod n$, then $2^{n-1} \equiv 1 \mod p$ for each p dividing n, and hence, $\text{ord}_2(p) \mid n - 1$. **q.e.d.**

In the case of J-numbers it is not true that J-numbers are square-free. Moreover, there are J-numbers which *are* squares, like 1093^2 or 3511^2. Furthermore, there are many

J-numbers which are the product of exactly two different primes. To find such composite J-numbers, the following fact is a useful tool.

Fact 5.3 *If p and q are odd primes such that $p < q$, $q \mid 2^{p-1} - 1$ and $\text{ord}_2(p) \mid q-1$ (or $p-1 \mid q-1$), then pq is a J-number.*

Proof. $q \mid 2^{p-1} - 1$ implies $2^{p-1} \equiv 1 \mod q$ and thus, $\text{ord}_2(q) \mid p-1$, which implies $\text{ord}_2(q) \mid q(p-1) + (q-1)$, since $\text{ord}_2(q) \mid q-1$. Further, since $\text{ord}_2(p) \mid q-1$ we get $\text{ord}_2(p) \mid p(q-1) + (p-1)$, because $\text{ord}_2(p) \mid p-1$. **q.e.d.**

Some Examples: $p = 11$ and $q = 31$ (check that $31 \mid 2^{11-1} - 1$); $p = 17$ and $q = 257$; $p = 19$ and $q = 73$; $p = 23$ and $q = 89$; ...

As a matter of fact we like to mention that if p is an odd prime, then $3p \mid 2^{p-1} - 1$.

Now we turn back to J-numbers n of the form $n = p^2$, with p prime. It is an open question whether there are infinitely many J-numbers which are square numbers. Here, we give a heuristic argument which lends some support to the conjecture that there are in fact infinitely many such numbers, but they are very likely to be extremely rare.

Lemma 5.4 *Let $n = p^2$ for some odd prime p, then n is a J-number if and only if $2^{p-1} \equiv 1 \mod p^2$.*

Proof. First notice that $\phi(p^2) = p(p-1)$ and therefore $2^{p^2-p} - 1 \equiv 0 \mod p^2$, which implies that $\text{ord}_2(p^2) \mid p^2 - p$.

If p^2 is a J-number, then $2^{p^2-1} - 1 \equiv 0 \mod p^2$, which implies that $\text{ord}_2(p^2) \mid p^2 - 1$, and together with $\text{ord}_2(p^2) \mid p^2 - p$ we get $\text{ord}_2(p^2) \mid p-1$. So, $2^{p-1} \equiv 1 \mod p^2$.

If $2^{p-1} \equiv 1 \mod p^2$, then $\text{ord}_2(p^2) \mid p-1$, and therefore, $\text{ord}_2(p^2) \mid \phi(p^2)$ (since $\phi(p^2) = p(p-1)$). Further, this implies that $\text{ord}_2(p^2) \mid p^2 - 1$, (since $p^2 - 1 = p^2 - p + (p-1)$), and hence, $2^{p^2-1} \equiv 1 \mod p^2$. **q.e.d.**

If p is prime and p^2 is a J-number, then we say that p is a **germ**.

Since $2^{p-1} \equiv 1 \mod p$ for every odd prime p, we get $2^{p-1} \equiv bp+1 \mod p^2$ for some $0 \leq b \leq p-1$. Let $\mathbb{P}$ be the set of all odd prime numbers and consider the function $\xi : \mathbb{P} \to [0,1)$ defined as follows: For $p \in \mathbb{P}$ let $\xi(p) \in [0,1)$ be such that $2^{p-1} \equiv \xi(p)p^2 + 1 \mod p^2$, in other words, $\xi(p) := \frac{b}{p}$, where b is as above and p is odd. It is very likely that the distribution of $\xi(p)$ is uniform. To illustrate this, let p_i (for $i \in \mathbb{N}$) be an enumeration of $\mathbb{P}$ such that $p_i < p_{i+1}$. First we tested the first $60,000$ odd primes and found that $\sum_{i \leq 60,000} \xi(p_i) \cong 29,934$. Further, $\sum_{60,000 \leq i < 100,000} \xi(p_i) \cong 19,928$ and $\sum\{\xi(p_i) : \xi(p_i) < \frac{1}{10} \text{ and } 60,000 \leq i < 100,000\} \cong 204$. Another test (up to over 2 Million) gave us $\sum_{100,000 \leq i < 160,000} \xi(p_i) \cong 29880$ and $\sum\{\xi(p_i) : \frac{1}{10} < \xi(p_i) < \frac{3}{10} \text{ and } 100,000 \leq i \leq 160,000\} \cong 2426$.

The idea is now to replace the mapping $p \mapsto b$ by equidistributed independent random variables X_p which take values in $\{0, 1, \ldots, p-1\}$, i.e., the probability that $X_p = i$ is $\frac{1}{p}$ for each $i \in \{0, 1, \ldots, p-1\}$. From X_p we construct a new random variable Y_p which takes, for each prime number p, the value 1 if $X_p = 0$ and zero otherwise. In other words, instead of looking whether $b = 0$ (and hence p is a germ), we throw a dice with p faces $\{0, 1, \ldots, p-1\}$. Therefore, a value p for which $Y_p = 1$ is now called a **random germ**. The idea is that random germs should have approximately the same distribution as the effective germs. The probability that p is not a random germ is

$$P(p \text{ is not a random germ}) = 1 - \frac{1}{p}.$$

Thus, we have

$$\begin{aligned} P(p_1, \ldots, p_k \text{ are all not random germs}) &= \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \\ &= \exp \sum_{i=1}^{k} \log \left(1 - \frac{1}{p_i}\right). \end{aligned}$$

Observe that $\log(1-x) \leq -x$ for $x \geq 0$ (and $|\log(1-x) + x| = O(x^2)$ for $x \to 0$). Thus, we can estimate

$$P(p_1, \ldots, p_k \text{ are all not random germs}) \lesssim \exp \left(- \sum_{i=1}^{k} \frac{1}{p_i} \right).$$

Now, the sum of inverse primes is divergent, and hence,

$$P(p_n, \ldots, p_k \text{ are all not random germs}) \to 0 \quad \text{for } k \to \infty.$$

In other words, the probability that after a certain odd prime number p_n no other random germ occurs is zero. So, we should expect that infinitely many J-numbers exist which are the square of a prime.

On the other hand, what can we say about the frequency of occurrence of (random) germs? In order to answer this question, we close this discussion by calculating the distribution function of random germs. In other words we ask: How many random germs may we expect in the set $\{p_1, p_2, \ldots, p_k\}$. This is simply

$$E\left[\sum_{i=1}^{k} Y_{p_i}\right] = \sum_{i=1}^{k} E[Y_{p_i}] = \sum_{i=1}^{k} \frac{1}{p_i}.$$

Example. The expected number of random germs $p \in \{3, 4, \ldots, 2000\}$ is 1.792448 (the actual number of germs in this interval is 1, namely $p = 1093$). In the interval $\{3, 4, \ldots, 10^6\}$ the expected number of random germs is 2.38733, the actual number of germs is 2, namely $p = 1093$ and $p = 3511$. ○

We can now state the following conjecture:

Conjecture 5.5 *There exist infinitely many J-numbers which are the square of a prime. Furthermore, the distribution function of the germs is asymptotically*

$$\big|\{p \leq n : p \textit{ is a germ}\}\big| \sim \sum_{\substack{p \leq n \\ p \text{ prime}}} \frac{1}{p} \sim \log \log n.$$

Remark: If we consider the random variable Z which takes the value p where p is the smallest random germ, then a similar calculation as above shows that the expected value of Z is $E[Z] = \infty$.

5.2 On the set of J_k-numbers

In the following we give a characterization of the set J_k. For this we first define $\operatorname{ord}_2(2) := 1$.

Theorem 5.6 *Let $k \in \mathbb{Z}$, then $n \in J_k$ if and only if $4 \nmid n$ and $\operatorname{ord}_2(p^l) \mid p^{l-1}m + k - 1$, where $n = p^l m$ and $p \nmid m$.*

The proof is given in the following two lemmas:

Lemma 5.7 *If k is even, then $n \in J_k$ if and only if $\operatorname{ord}_2(p^l) \mid p^{l-1}m + k - 1$, where $n = p^l m$ and $p \nmid m$.*

Proof. Assume $p^l m = n$ and $p \nmid m$, then

$$2^{n+k} = 2^{p^l m+k} = 2^{p^{l-1}(p-1)m+p^{l-1}m+k} = \left(2^{p^{l-1}(p-1)}\right)^m \cdot 2^{p^{l-1}m+k},$$

and because $2^{p^{l-1}(p-1)} \equiv 1 \mod p^l$ we get

$$2^{n+k} \equiv 2^{p^{l-1}m+k} \mod p^l .$$

Thus, $n \in J_k$ if and only if $2^{p^{l-1}m+k} \equiv 2 \mod p^l$, which is equivalent to $\operatorname{ord}_2(p)^l \mid p^{l-1}m + k - 1$. **q.e.d.**

Notice that if n is square-free, Lemma 5.7 is equivalent to $\operatorname{ord}_2(p) \mid m + k - 1$ and remember that $\operatorname{ord}_2(p) \mid p - 1$.

Lemma 5.8 *If k is odd, then $n \in J_k$ if and only if $4 \nmid n$ and for all odd primes p, where $n = p^l m$ and $p \nmid m$, we have $\operatorname{ord}_2(p^l) \mid p^{l-1}m + k - 1$.*

Proof. The proof is similar to the proof of Lemma 5.7. We only have to show that $n \in J_k$ implies n is even and $4 \nmid n$. Let $n \in J_k$, then by definition we have $n + k > 1$ and $n + k$ is odd, and hence n is even. Because $n + k > 1$ we have $2^{n+k} \geq 4$ and therefore $4 \mid 2^{n+k}$, which implies $4 \nmid 2^{n+k} - 2$. Thus, $2^{n+k} \not\equiv 2 \mod 4$ and we get $4 \nmid n$. **q.e.d.**

Notice that if n is square-free, Lemma 5.8 is equivalent to $\operatorname{ord}_2(p) \mid m + k - 1$ and $n = 2m$ for some m.

5.3 Some square-free elements of J_k

We have seen that there are only four numbers in the set C_1. These numbers also appear in the set J_1. However, the set J_1 is much bigger than C_1, even if we restrict our attention to square-free numbers.

Let $p \in J_1$ be a prime, then because each number belonging to J_1 is even, $p = 2$. Assume now $2q \in J_1$ for an odd prime q. By Lemma 5.8 we get $\mathrm{ord}_2(q) \mid 2$, which implies $q = 3$. Now assume $2qr \in J_1$ where $2 < q < r$ are primes. Again by Lemma 5.8 we get $\mathrm{ord}_2(q) \mid 2r$, which implies again, because r is prime and greater than q, that $q = 3$. Further, because $\mathrm{ord}_2(r) \mid 6$, $r > 3$ and r is a prime we get $r = 7$. If we assume $2qrs \in J_1$, where $2 < q < r < s$ are primes, then we get again $q = 3$ and $r = 7$, but s is not uniquely determined by $q = 3$ and $r = 7$. For example, $s = 127$ and $s = 43$ are possible values for s. It is very likely that—in contrast to C_1—the set J_1 contains infinitely many square-free elements.

Acknowledgement: We like to thank Stephanie Halbeisen who wrote all the JAVA programs we used in this paper.

References

[AGP1994] W. R. Alford, A. Granville and C. Pomerance: There are infinitely many Carmichael numbers. *Annals of Mathematics* **140** (1994), 703–722.

[Ca1910] R. D. Carmichael: Note on a new number theoretic function. *Bulletin of the American Mathematical Society* **16** (1910), 232–238.

[Ca1912] 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.

[Ch1939] J. Chernick: On Fermat's simple theorem. *Bulletin of the American Mathematical Society* **45** (1939), 269–274.

[HHL1999] L. Halbeisen, N. Hungerbühler and H. Läuchli: Powers and polynomials in $\mathbb{Z}_m$. *Elemente der Mathematik* **54** (1999), 118–129.

[Je1898] J. H. Jeans: The converse of Fermat's theorem. *Messenger of Mathematics* **XXVII** (1898), 174.

[Ko1899] A. Korselt: Problème chinois. *L'intermédiaire des mathématiciens* **6** (1899), 143.

[Re1996] D. Redmond: "Number Theory, an Introduction." Marcel Dekker, Inc., New York (1996).

[Ri1989] P. Ribenboim: "The book of prime number records." Springer-Verlag, Berlin, New York (1989).

Address of the Authors:

Prof. L. Halbeisen
Department of Mathematics,
University of California at Berkeley,
Evans Hall 938,
Berkeley CA 94720, U.S.A.

E-mail:- L. Halbeisen: halbeis@math.berkeley.edu

Prof. N. Hungerbühler
Department of Mathematics,
University of Alabama at Birmingham,
452 Campbell Hall,
Birmingham AL 35294-1170. U.S.A.

E-mail:- N. Hungerbühler: buhler@math.uab.edu