K-LEHMER AND *K*-CARMICHAEL NUMBERS

Max Lewis
Dept. of Mathematics, University of Queensland, St Lucia, QLD 4072, Australia

Victor Scharaschkin
Dept. of Mathematics, University of Queensland, St Lucia, QLD 4072, Australia
v.scharaschkin@gmail.com

Received: 10/13/15, Accepted: 11/13/16, Published: 11/22/16

Abstract

Grau and Oller-Marcén have defined k-Lehmer and k-Carmichael numbers as generalizations of Lehmer and Carmichael numbers, respectively. We partially resolve some of their conjectures by proving that for infinitely many k there are Carmichael numbers that are k-Lehmer but not $(k-1)$-Lehmer. We also prove an analogous result for k-Carmichael numbers.

1. Introduction

Let φ denote Euler's totient function. If n is prime then $\varphi(n) = n - 1$. A *Lehmer number* [11] is a composite integer n such that $\varphi(n) \mid (n-1)$. It is an open question whether any such n exist [9, B37]. Clearly, if n is a Lehmer number then

$$\text{for all } a \in \mathbb{N}, \text{ if } \gcd(a, n) = 1 \text{ then } a^{\varphi(n)} \equiv 1 \pmod{n}. \tag{1}$$

Let $\mathcal{C}$ be the set of composite numbers satisfying (1). Elements of $\mathcal{C}$ are called *Carmichael numbers* [19, A002997]. In contrast to Lehmer numbers, it was shown in Alford, Granville and Pomerance's seminal paper [1] that $\mathcal{C}$ is infinite.

Generalizing Lehmer's definition, Grau and Oller-Marcén [7] define sets $\mathcal{L}_1 \subseteq \mathcal{L}_2 \subseteq \cdots \subseteq \mathcal{L}_\infty$ by

$$\mathcal{L}_k = \{n \in \mathbb{N} \colon \varphi(n) \mid (n-1)^k\}, \qquad \mathcal{L}_\infty = \bigcup_{k=1}^{\infty} \mathcal{L}_k$$

and show that $\mathcal{C} \subset \mathcal{L}_\infty$. (The containment is strict. For example $15 \in \mathcal{L}_3 \setminus \mathcal{C}$.)

For $k \leq \infty$ let $\mathcal{L}'_k$ be the subset of $\mathcal{L}_k$ consisting of composite numbers, so $\mathcal{L}'_1$ is the (possibly empty) set of Lehmer numbers. An element of $\mathcal{L}'_k$ is called a *k-Lehmer number* [19, A238574]. McNew has shown [13, Theorem 4] that for $k \geq 2$ $\left| \mathcal{L}'_k \cap [1, x] \right| \ll_k x^{1-\frac{1}{4k-1}}$.

Note that we have $\mathcal{L}'_1 \subseteq \mathcal{C} \subseteq \mathcal{L}'_\infty$. In this notation Lehmer's original problem is whether the "lower bound" $\mathcal{L}'_1$ for $\mathcal{C}$ is non-empty. More generally we can ask how $\mathcal{C}$ is distributed among the $\mathcal{L}_k$.

If $n \in \mathcal{L}_\infty$, we define the *level* of n, $\ell(n)$, to be the smallest k such that $n \in \mathcal{L}_k$. McNew and Wright [14] have recently shown that for every $k \geq 3$ there are infinitely many integers of level k, but none of the numbers they construct are Carmichael. Grau and Oller-Marcén conjecture that for every $k \geq 2$ there are infinitely many Carmichael numbers of level k. Thus, conjecturally, the set $\ell(\mathcal{C})$ contains every integer greater than one. In §2 we prove a weaker result by showing that $\ell(\mathcal{C})$ is infinite.

Theorem 1. *For infinitely many $k \in \mathbb{N}$ there exists a Carmichael number of level k. That is, $\mathcal{C} \cap \left(\mathcal{L}'_k \setminus \mathcal{L}'_{k-1}\right)$ is non-empty infinitely often.*

Lehmer's condition $\varphi(n) \mid (n-1)$ for composite n is so stringent that it may be impossible to satisfy. Another weakening of this condition is to replace the order $\varphi(n)$ of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ by the exponent of this group, $\lambda(n)$. As Carmichael showed [4], the resulting analogue of Lehmer's condition is satisfied precisely by the Carmichael numbers: for n composite, $\lambda(n) \mid (n-1)$ if and only if $n \in \mathcal{C}$.

In another paper, Grau and Oller-Marcén [8] weaken this condition further. Given $k \in \mathbb{N}$, they define a composite number n to be a *k-Carmichael number* if $\lambda(n) \mid k(n-1)$. Thus a 1-Carmichael number is precisely a Carmichael number in the usual sense.

In analogy to ℓ, we define $\mathsf{k}(n)$ to be the smallest integer k such that n is a k-Carmichael number. We believe it is natural to ask which integers occur in the image of k. If k were surjective it would mean that there are natural numbers, n, that are arbitrarily far away from being Carmichael in the sense that $\lambda(n)$ only divides $k(n-1)$ for large k. In §4 we prove the following:

Theorem 2. *For every finite non-empty set S of primes, there exists n such that the prime factors of $\mathsf{k}(n)$ are exactly the primes in S. That is, the function $\operatorname{rad} \circ \mathsf{k} \colon \mathbb{N} \to \{n \in \mathbb{N} \colon n \text{ is square-free}\}$ is surjective.*

We record some results and notation for future reference. If m is a positive integer, let $\omega(m)$ be the number of distinct prime factors of m. If G is a finite group, let $\lambda(G)$ denote its exponent. In the special case $G = (\mathbb{Z}/n\mathbb{Z})^\times$, write $\lambda(n)$ for $\lambda(G)$, and call λ the *Carmichael λ function.* As $n \to \infty$ we have $\lambda(n) \to \infty$. Indeed, from Erdős, Pomerance and Schmutz [6, Theorem 1], for sufficiently large n

$$\lambda(n) > \log(n)^{\log\log\log n}. \tag{2}$$

It is easy to see that any Carmichael number n must be odd and square-free. *Korselt's criterion* [10] states that a square-free integer $n > 1$ is Carmichael if and only if for each prime p with $p \mid n$ it follows that $(p-1) \mid (n-1)$. Finally we have a simple lemma.

Lemma 1. *Let a and b be positive integers, and let c be the least positive integer such that $a \mid bc$. Then $c = a/\gcd(a,b) = \operatorname{lcm}(a,b)/b$.*

2. Carmichael Numbers of Level k

Lemma 2. *Let $n \in \mathcal{C}$, $n = \prod_{j=1}^{k} p_j$. Then*

$$\ell(n) = \max_{q \mid (n-1)} \left\{ \left\lceil \sum_{j=1}^{k} \frac{\operatorname{ord}_q(p_j - 1)}{\operatorname{ord}_q(n-1)} \right\rceil \right\}. \tag{3}$$

Each fraction in the sum lies in the interval $[0,1]$.

Proof. By Korselt's criterion $(p_j - 1) \mid (n-1)$ for each $j = 1, \ldots, k$, so $\operatorname{ord}_q(p_j - 1) \leq \operatorname{ord}_q(n-1)$ and each fraction is in $[0,1]$.

By definition, $\ell = \ell(n)$ is the smallest positive integer such that $\varphi(n) = \prod_{j=1}^{k}(p_j - 1) \mid (n-1)^{\ell}$. Equivalently, ℓ is minimal such that for all primes $q \mid (n-1)$ we have $\operatorname{ord}_q \prod_{j=1}^{k}(p_j - 1) \leq \operatorname{ord}_q(n-1)^{\ell}$. That is, $\sum_{j=1}^{k} \operatorname{ord}_q(p_j - 1) \leq \ell \operatorname{ord}_q(n-1)$. So ℓ is the smallest integer greater than or equal to $\sum_{j=1}^{k} \frac{\operatorname{ord}_q(p_j-1)}{\operatorname{ord}_q(n-1)}$ for every q, as claimed. $\square$

Example. The smallest Carmichael number is $n = 3 \cdot 11 \cdot 17 = 561$ with $n - 1 = 2^4 \cdot 5 \cdot 7$, and

$$\begin{aligned} \ell(n) &= \max_{q \in \{2,5,7\}} \left\{ \left\lceil \frac{\operatorname{ord}_q(2) + \operatorname{ord}_q(10) + \operatorname{ord}_q(16)}{\operatorname{ord}_q(2^4 \cdot 5 \cdot 7)} \right\rceil \right\} \\ &= \max \left\{ \left\lceil \frac{1+1+4}{4} \right\rceil, \left\lceil \frac{0+1+0}{1} \right\rceil, \left\lceil \frac{0+0+0}{1} \right\rceil \right\} \\ &= 2. \end{aligned}$$

Indeed $\varphi(n) = 2^6 \cdot 5$, so $\varphi(n) \mid (n-1)^2$ but $\varphi(n) \nmid (n-1)$, and so $\ell(n) = 2$.

Since each fraction in (3) is bounded above by 1 we have a simple bound for $\ell(n)$. Recall that $\omega(n)$ is the number of distinct prime factors of n.

Corollary 1. *If $n \in \mathcal{C}$ then $\ell(n) \leq \omega(n)$.*

This inequality is not tight in general, as the example $n = 561 = 3 \cdot 11 \cdot 17$ shows. However, under some additional hypotheses the inequality is actually an equality.

Corollary 2. *Let q be any prime. Suppose $n \in \mathcal{C}$, $n = \prod_{j=1}^{k} p_j$ and $n \not\equiv 1 \pmod{q^2}$ is such that $p_j \equiv 1 \pmod{q}$ but $p_j \not\equiv 1 \pmod{q^2}$ for $j = 1, 2, \cdots, k$. Then $\ell(n) = k$.*

Proof. By Korselt's criterion $q \mid (p_j - 1) \mid (n-1)$, so q is one of the primes indexing the set in (3). The hypotheses of the corollary imply that each of the k fractions in the corresponding sum is equal to 1, so the sum is k, which is the maximum possible (so no other $q' \mid (n-1)$ can produce a larger value). $\square$

This result takes a particularly simple form if $q = 2$, since the condition $p_j \equiv 1 \pmod 2$ is automatically satisfied.

Corollary 3. *If $n \in \mathcal{C}$ and $n \equiv 3 \pmod 4$, then $\ell(n) = \omega(n)$. Moreover, in this situation $\ell(n)$ must be odd.*

Proof. Let $n = \prod_{j=1}^{k} p_j$. If some $p_j \equiv 1 \pmod 4$ then $4 \mid (p_j - 1) \mid (n-1)$ by Korselt's criterion, but this is impossible since $n - 1 \equiv 2 \pmod 4$. So $\mathrm{ord}_2(p_j - 1) = 1$ for each j. Putting $q = 2$ in Corollary 2 shows $\ell(n) = k$. Furthermore, each $p_j \equiv -1 \pmod 4$ so $n \equiv (-1)^k \pmod 4$ and so k must be odd. $\square$

In a recent advance, Wright [20] proved "Dirichlet's theorem for Carmichael numbers." That is, for all positive integers a and m with $\gcd(a, m) = 1$ there exist infinitely many Carmichael numbers n with $n \equiv a \pmod m$. It is implicit in Wright's proof that n may be chosen with many prime factors. For clarity, we make this explicit.

Theorem 3 ([20]). *Let $a, m \in \mathbb{N}$ with $\gcd(a, m) = 1$ and let $k \in \mathbb{N}$. Then there exist infinitely many Carmichael numbers n with $n \equiv a \pmod m$ and $\omega(n) \geq k$.*

Proof. This is implicit in Wright, but requires close reading. It is difficult to summarize the arguments without reproducing much of the exposition there.

Fix a and m. (In the notation of [20], also fix θ.) It suffices to show the existence of one such n, since if $n_1 \in \mathcal{C}$, $n_1 \equiv a \pmod m$ and $\omega(n_1) = k_1 > k$, then there exists $n_2 \in \mathcal{C}$ with $n_2 \equiv a \pmod m$ and $\omega(n_2) = k_2 \geq k_1 + 1$. In particular, $n_2 \neq n_1$ and the result follows by repeating this argument.

We sketch Wright's proof. Let y be an integer parameter that we ultimately let become very large. Construct an integer $L = L(y)$ with many divisors d such that $dk_0 + 1$ is prime for some k_0. Collect a certain subset of these primes into a set $\mathcal{P}$ whose cardinality may be estimated. From [20, Lemma 4.3] the construction yields

$$\log L \gg y. \tag{4}$$

The desired n is obtained from the following:

Theorem 4. *Let G be a finite multiplicative abelian group of exponent $\lambda(G)$, and let $\mathcal{P}$ be a length p sequence of elements of $G \setminus \{1_G\}$. Then there exist integers $n(G)$ and $s(G) \gg \lambda(G)^2$ and a subgroup $\{1_G\} \neq H \subseteq G$ such that each of the following hold.*

1. *If $p \geq s(G)$ then $\mathcal{P} \cap H$ is non-empty.*

2. *If $p \geq s(G)$ and $h \in H$ then there exists a subsequence of $\mathcal{P}$ whose product is h.*

3. *Let t be an integer with $s(G) < t < p - n(G)$ and let*

$$N_t = \binom{p - n(G)}{t - n(G)} \cdot \binom{p}{n(G)}^{-1}.$$

Then for each $h \in H$ there are at least N_t subsequences of $\mathcal{P}$ of length at least $t - n(G)$ whose product is h.

Proof. Parts (1) and (2) follow from Baker and Schmidt [3, Proposition 1] (see discussion after (1.14) in that paper), and part (3) follows from Matomäki [12, Lemma 6]. Explicit bounds for $s(G)$ and $n(G)$ are given in these references but we shall not need them in this sketch. □

Now apply Theorem 4 in (at least) two different ways. Let $G = (\mathbb{Z}/mL\mathbb{Z})^{\times}$, so $\lambda(G) = \lambda(mL)$. One shows $p > s(G)$, so by Theorem 4(1) H exists with $\mathcal{P} \cap H \neq \emptyset$. Let $p_H \in \mathcal{P} \cap H$. It is not difficult to find r such that $h := p_H^r$ satisfies $h \equiv 1 \pmod{L}$ and $h \equiv a \pmod{m}$. Then Theorem 4(2) implies there exists a product, n, of primes from $\mathcal{P}$ whose image in G satisfies $n = h$. Finally this n is shown to be Carmichael using Korselt's criterion.

Furthermore, Wright gives an explicit positive integer $t = t(M, L)$ to use in Theorem 4(3), such that:

$$s(G) < t < p - n(G), \qquad t - n(G) \geq \frac{2}{3}t, \qquad \log N_t \gg ty.$$

Thus, for y large enough, $N_t \geq 1$ certainly holds and hence there exists $n \in \mathcal{C}$ with $n \equiv a \pmod{m}$ and $\omega(n) \geq 2t/3$. In particular, as $y \to \infty$, $L \to \infty$ by (4), and hence $\lambda(mL) \to \infty$ by (2). Since $\omega(n) \geq \frac{2}{3}t > \frac{2}{3}s(G) \gg \lambda(mL)^2$ it follows that if y is chosen large enough then $\omega(n) \geq k$. □

Combining Wright's result with Corollary 3 we can now prove Theorem 1.

Theorem 5. *For infinitely many odd integers k there is a Carmichael number of level k.*

Proof. Let $m \in \mathbb{N}$. By Theorem 3 there exists a Carmichael number $n \equiv 3 \pmod{4}$ with $\omega(n) \geq m$. By Lemma 3 $\ell(n) = \omega(n) \geq m$, and $\ell(n)$ is odd. So for every m there exists odd $k \geq m$ and a Carmichael number of level k. The result follows. □

The limitation that k is odd comes from using $q = 2$ in Corollary 2. Below we construct many Carmichael numbers of large known level, both even and odd.

3. Examples of Carmichael Numbers of Level k

Alford, Grantham, Hayman and Shallue [2] give a probabilistic algorithm for producing Carmichael numbers with a large number of prime factors. They find examples with almost 20 million factors. By implementing a modified version of their algorithm we were able to find Carmichael numbers of known level exceeding 10^5, including examples of even level. We give details in Table 1. Calculations were carried out in Pari [15].

The algorithm uses the following variant of Corollary 2.

Lemma 3. *Let q be prime and M be any positive integer not divisible by q. Let*

$$\mathcal{P} = \{p = qd + 1 \ : \ d \mid M, \ \ p \nmid M, \ \ \text{and } p \text{ is prime}\}.$$

Suppose there exist distinct elements $p_1, \ldots, p_k \in \mathcal{P}$ with $k \geq 3$ such that the product $n = p_1 \cdots p_k$ satisfies $n \equiv 1 \pmod{qM}$ and $n \not\equiv 1 \pmod{q^2}$. Then n is a Carmichael number of level k.

Proof. Observe that $(p-1) = qd \mid qM \mid (n-1)$ for all $p \in \mathcal{P}$, and thus n satisfies Korselt's criterion, so $n \in \mathcal{C}$. We have $p = qd + 1 \equiv 1 \pmod{q}$ for all $p \in \mathcal{P}$, and each $d \mid M$, so $q \nmid d$ and thus $p \not\equiv 1 \pmod{q^2}$. So n satisfies the conditions of Corollary 2 and hence has level k. $\square$

Let $L = qM$. The algorithm works by choosing M with many small prime factors, generating the set $\mathcal{P}$, and then searching for long products n that are 1 modulo L but not $1 \pmod{q^2}$. In the case $q = 2$ this is equivalent to choosing a product of odd length.

$q = 2$
$M_2 = 3^8 \cdot 5^4 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47$
$\quad = 841317949047219840239793 75$
$k = 101015$, $\lvert\mathcal{P}\rvert = 101208$
$n = 4459278357 \ldots 1375428751 \equiv 3 \pmod{4}$
$q = 3$
$M_3 = 2^9 \cdot 5^4 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47$
$\quad = 6565383171958185615040000$
$k = 109544$, $\lvert\mathcal{P}\rvert = 109691$
$n = 1712274852 \ldots 4645120001 \equiv 7 \pmod{9}$

Table 1: Carmichael numbers with level $k > 10^5$

Although this works well in practice, we cannot prove that such products n must exist. Let $\delta(n)$ denote the number of divisors of n of the form $p - 1$ where p is prime, and, for a specific example, let M_2 be as in Table 1 and consider $L = 2M_2$.

For this L one finds that $\delta(L) = 101217$. It is shown in [1, Theorem 2] that there exists a product that is congruent to 1 modulo L, provided

$$\delta(L) \geq \lambda(L)\left(1 + \log\frac{\varphi(L)}{\lambda(L)}\right). \tag{5}$$

But $\lambda(L)\left(1+\log\frac{\varphi(L)}{\lambda(L)}\right) \approx 3.4 \times 10^{12}$ is much larger than $\delta(L)$, and yet we still easily found many subsequences with product 1. It appears that inequality (5) is stronger than what is really needed to guarantee such subsequences exist. Similarly, Prachar's lower bound for $\delta(n)$ in [16] seems much smaller than our computed value of $\delta(L)$. An improvement of these bounds might lead to a proof that there are Carmichael numbers of every possible level.

We note here a method of producing natural numbers that are the product of only two primes (and hence not Carmichael) that have large known level. It follows from Grau and Oller-Marcén [7, Proposition 5] that the product of any two primes of the form $p = 2^a d+1$, $q = 2^b d+1$ for some odd d and $a < b$, is of level $k = \left\lceil \frac{b}{a} \right\rceil + 1$. Primes of the form $p = 2^n d + 1$ for odd k and $2^n > k$ are called *Proth primes* [19, A080076]. If we take $p = 2^1 \cdot 3 + 1$ and let q be the large Proth prime $q = 2^b \cdot 3 + 1$ where $b = 10829346$, then pq has level $b + 1$, which exceeds 10^7.

4. *k*-Carmichael Numbers

Recall that a composite number n is a *k-Carmichael number* if $\lambda(n)$ divides $k(n-1)$, where $\lambda(n)$ is Carmichael's lambda function, which can be calculated as follows:

$$\begin{aligned}
\lambda(2^h) &= \varphi(2^h) && \text{for } h = 0, 1, 2,\\
\lambda(2^h) &= \frac{1}{2}\varphi(2^h) && \text{for } h > 2,\\
\lambda(p^h) &= \varphi(p^h) && \text{for odd primes } p,\\
\lambda(p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}) &= \operatorname{lcm}\left(\lambda(p_1^{h_1}),\, \lambda(p_2^{h_2}), \ldots,\, \lambda(p_s^{h_s})\right) && \text{for distinct primes } p_j.
\end{aligned}$$

(This may be remembered as follows. Let $a * b$ denote $\operatorname{lcm}(a, b)$. Then except for the prime 2, λ is calculated in the semigroup $(\mathbb{N}, *)$ in the same way as φ in the semigroup $(\mathbb{N}, \cdot)$.)

Of course $\lambda(n)$ always divides $k(n-1)$ for some k (such as $k = \lambda(n)$), so we are led to the following definition.

Definition 1. Let $\mathsf{k}(1) = 1$, let $\mathsf{k}(p) = 1$ for any prime p and for composite n define $\mathsf{k}(n)$ to be the smallest integer k such that n is a k-Carmichael number.

Thus for n composite, $\mathsf{k}(n) = 1$ if and only if n is Carmichael in the usual sense.

Putting $a = \lambda(n)$ and $b = (n-1)$ in Lemma 1 gives a formula found in [8, page 7]:

$$\mathsf{k}(n) = \frac{\lambda(n)}{\gcd(\lambda(n),\, n-1)} = \frac{\operatorname{lcm}(\lambda(n),\, n-1)}{n-1}. \tag{6}$$

(This also holds for n prime, but not for $n = 1$.) For example, if p is an odd prime then $\mathsf{k}(2p) = p-1$ and so $\limsup \mathsf{k}(n) = \infty$, while $\liminf \mathsf{k}(n) = 1$. In analogy with ℓ, we make the following conjecture.

Conjecture 1. *The function* k *is surjective.*

Since $\lambda(p^{m+1})$ or $\lambda(p^{m+2}) = p^m$, it is clear that the image of k contains every prime power. Unfortunately, k is not multiplicative: $\mathsf{k}(15) = 2$, $\mathsf{k}(28) = 2$, but $\mathsf{k}(15 \cdot 28) = 12$.

Lemma 4. *Let p be an odd prime and $k \geq 2$ an integer. If $q = k(p-1)+1$ is prime then $\mathsf{k}(pq) = k$.*

Proof. Applying (6)

$$\begin{aligned}
\mathsf{k}(pq) &= \frac{\operatorname{lcm}(p-1, q-1)}{\gcd\big(\operatorname{lcm}(p-1, q-1),\ pq-1\big)} &(7)\\
&= \frac{k(p-1)}{\gcd(k(p-1),\, (kp+1)(p-1))} &(8)\\
&= \frac{k(p-1)}{p-1} = k. &\square
\end{aligned}$$

In practice this result gives us an easy way of finding an $n \in \mathbb{N}$ such that $\mathsf{k}(n) = k$ for a given $k \in \mathbb{N}$. We have used it to show that there exists an $n \in \mathbb{N}$ such that $\mathsf{k}(n) = k$ for every $k \leq 10^6$. For example, taking $k = 10^6$, we find that $q = 10^6 \cdot (23-1) + 1 = 22000001$ is prime and so $\mathsf{k}(23 \cdot 22000001) = 10^6$.

Unfortunately Lemma 4 does not lead to a proof that k is surjective. Let $f_k(x) = k(x-1)+1$, and let $g(x) = x$. If there exists an integer x such that $f_k(x)$ and $g(x)$ are simultaneously prime then $\mathsf{k}(xf_k(x)) = k$ so k is in the image of k. The existence of an integer x where r linear polynomials simultaneously take prime values is *Dickson's prime r-tuple conjecture* [5]. It is well known (see [17, p. 372]) that if there exists such an x and Dickson's conjecture is true, then there must be infinitely many such x. Hence:

Corollary 4. *If Dickson's prime r-tuple conjecture holds then* k *is surjective, and indeed for each positive integer k there exist infinitely many n with $\mathsf{k}(n) = k$.*

Dickson's conjecture with $r = 1$ is Dirichlet's theorem on primes in arithmetic progressions, and is open for all cases when $r > 1$. Its difficulty is clear since it also implies the existence of infinitely many twin primes, infinitely many Sophie

Germain primes and so on. Dickson's conjecture is itself a special case of Schinzel's *Hypothesis H* [18] concerning prime values of arbitrary polynomials.

If k is also prime then the converse of Lemma 4 holds.

Lemma 5. *If $p < q$ are odd primes and $\mathsf{k}(pq) = k$ where k is prime, then $q = k(p-1)+1$.*

Proof. Let $L = \operatorname{lcm}(p-1,\, q-1)$, $g = \gcd(p-1, q-1)$, $(p-1) = ga$ and $(q-1) = gb$ where $\gcd(a,\, b) = 1$ and $a < b$. Assume $\mathsf{k}(pq) = k$. From (7) $L = k \cdot \gcd(L,\, pq-1)$, so $L \mid k(pq-1) = k\big[(ag+1)(bg+1)-1\big] = kg(abg+a+b)$. Multiplying through by g, $abg^2 = (p-1)(q-1) = Lg \mid kg^2(abg+a+b)$. Hence $ab \mid k(a+b)$. So $a \mid kb$, and since $\gcd(a,\, b) = 1$ we have $a \mid k$ and similarly $b \mid k$. Since $a < b$ and k is prime, $a = 1$ and $b = k$ is the only possibility. Hence $g = p-1$ and $q = bg+1 = k(p-1)+1$. □

For products of more than two primes, analogous formulas exist but are more involved. (One reason for this is that the analogue of the formula $\gcd(a_1, a_2)\operatorname{lcm}(a_1, a_2) = a_1a_2$ becomes more complicated.) For example, we have a sort of "Chernick formula" in the case $n = pqr$.

Lemma 6. *Let p be a prime and m a positive integer satisfying $m \mid (kp+1)$ for some integer $k \geq 2$. If $q = km(p-1)+1$ and $r = k(pq-1)+1$ are both prime then $\mathsf{k}(pqr) = k$.*

Proof. Suppose p, $q = km(p-1)+1$ and $r = k(pq-1)+1$ are prime, where the integer $k \geq 2$ and $m \mid (kp+1)$. Then

$$\begin{aligned}\lambda(pqr) &= \operatorname{lcm}\big(p-1,\, km(p-1),\, k(kmp+1)(p-1)\big)\\ &= km(p-1)(kmp+1).\end{aligned}$$

So

$$\begin{aligned}\mathsf{k}(pqr) &= \frac{\lambda(pqr)}{\gcd(\lambda(pqr),\, pqr-1)}\\ &= \frac{km(p-1)(kmp+1)}{\gcd\big(km(p-1)(kmp+1),\, (p-1)(kmp+1)(k^2mp(p-1)+kp+1)\big)}\\ &= \frac{km(p-1)(kmp+1)}{m(p-1)(kmp+1)} = k,\end{aligned}$$

since $m \mid (k^2mp(p-1)+kp+1)$ but $k \nmid (k^2mp(p-1)+kp+1)$. □

It seems difficult to make further progress in this direction. Instead we observe that if $\mathcal{S} = \{p_1,\, \ldots,\, p_s\}$ is a set of odd primes and $M = \prod_{j=1}^{s} p_j^{m_j}$, we may have

$$\mathsf{k}(M) = \mathsf{k}(p_1^{m_1}\cdots p_s^{m_s}) \stackrel{?}{=} p_1^{m_1-1}\cdots\, p_s^{m_s-1} = \frac{M}{\operatorname{rad}(M)}. \tag{9}$$

(This equation should be slightly modified if one of the primes is 2.) Obviously if (9) always held then k would be surjective. Unfortunately, an extra factor, $F(M)$, may also occur on the right hand side. For example, $\mathsf{k}(3^4 \cdot 5^3) = 3^3 \cdot 5^2$, but $\mathsf{k}(3^3 \cdot 5^3) = 2 \cdot 3^2 \cdot 5^2$. Nonetheless, for any M with $\{p : p \mid M\} = \mathcal{S}$ we can show that only finitely many different $F(M)$ occur, and that their occurrence is periodic in the m_j. This gives a more precise version of Theorem 2.

We need some notation. Let $\mathcal{S} = \{p_1, \ldots, p_s\}$ be a non-empty set of (distinct) primes. Let $L = L_{\mathcal{S}} = \operatorname{lcm}\{p_j - 1 \mid 1 \leq j \leq s\}$. Let $N = N_{\mathcal{S}}$ be a positive integer such that for every prime q with $\operatorname{ord}_q(L) = v > 0$:

1. If $q \notin \mathcal{S}$ then $\lambda(q^v) \mid N$, and
2. If $q \in \mathcal{S}$ then $N \geq v + 2$.

Suppose M is an integer with $\{p : p \mid M\} = \mathcal{S}$. Say $M = \prod_j p_j^{m_j}$ where all the $m_j > 0$. Define

$$F(M) := \frac{\mathsf{k}(M)}{M'} \quad \text{where} \quad M' = \begin{cases} \frac{M}{2\operatorname{rad}(M)} & \text{if } M \neq 4 \text{ and } \operatorname{ord}_2(M) \geq \operatorname{ord}_2(4L), \\ \frac{M}{\operatorname{rad}(M)} & \text{otherwise.} \end{cases}$$

We now show (condition (2) below) that $F(M)$ depends only on the $m_j \pmod{N_{\mathcal{S}}}$.

Theorem 6. *With $M = \prod_j p_j^{m_j}$ and notation as above:*

1. *If each $m_j \equiv 0 \pmod{N_{\mathcal{S}}}$ then $F(M) = 1$.*
2. *Suppose for $1 \leq j \leq s$ there exists an integer $t_j \geq 0$ such that $m_j = r_j + t_j N_{\mathcal{S}}$ with $r_j \geq N_{\mathcal{S}}$. Let $R = \prod_j p_j^{r_j}$. Then $F(M) = F(R)$.*

Proof. We drop the subscript $\mathcal{S}$. If all the p_j are odd, a small calculation shows $\lambda(M) = \operatorname{lcm}\{L, M'\}$. The definition of M' is made to ensure this holds in the case $p_j = 2$ also. Thus from (6) we obtain

$$F(M) = \frac{\mathsf{k}(M)}{M'} = \frac{L}{\gcd\big(L,\, (M-1)M'\big)}.$$

Let q be any prime dividing L. Let

$$\operatorname{ord}_q(L) = v, \qquad \operatorname{ord}_q(R'(R-1)) = r, \qquad \operatorname{ord}_q(M'(M-1)) = m.$$

If $q \notin \mathcal{S}$ then for $1 \leq j \leq s$ we have $p_j \neq q$, so p_j is invertible modulo q^v and $p_j^{\lambda(q^v)} \equiv 1 \pmod{q^v}$. Then $\lambda(q^v) \mid N$ by definition of N, so $p_j^N \equiv 1 \pmod{q^v}$ for all j, and so

$$\text{if } q \notin \mathcal{S} \text{ then } \prod p_j^N \equiv 1 \pmod{q^v}. \tag{10}$$

We now prove statement (1) of the theorem. Suppose that $m_j \equiv 0 \pmod{N}$ for all j. If $q \in \mathcal{S}$ then $m \geq N \geq v + 2$ so $\operatorname{ord}_q(M') \geq \operatorname{ord}_q(M) - 2 \geq v$. If $q \notin \mathcal{S}$

then $M \equiv 1 \pmod{q^v}$ from (10) so $m \geq \mathrm{ord}_q(M-1) \geq v$. Thus, in all cases $\mathrm{ord}_q(L) \leq \mathrm{ord}_q(M'(M-1))$. Thus $L \mid M'(M-1)$, so $F(M) = 1$.

To prove statement (2), we shall show

$$\min\{v, m\} = \min\{v, r\}. \tag{11}$$

Thus $\mathrm{ord}_q(F(M)) = v - \min\{v, m\} = v - \min\{v, r\} = \mathrm{ord}_q(F(R))$ for every $q \mid L$, and since $F(m)$ and $F(R)$ are positive integers dividing L, it follows that $F(M) = F(R)$.

Finally, we prove that equation (11) holds. Suppose $q \in \mathcal{S}$. Thus $q = p_i$ for some i. By definition of N we have $m_i, r_i \geq N \geq 2 + v > v$, so both sides in (11) are equal to v.

Now suppose $q \notin \mathcal{S}$. If m, $r \geq v$ we are done, so we assume $v > r$ or $v > m$. We show that $m = r$, so both sides in (11) are equal to m $(= r)$. Since $q \notin \mathcal{S}$ we have $m = \mathrm{ord}_q(M-1)$ and $r = \mathrm{ord}_q(R-1)$. Thus it suffices to show that $M \equiv R \pmod{q^v}$, since then $M - 1 \equiv R - 1 \pmod{q^v}$. Then, as one of $M-1$, $R-1$ is non-zero mod q^v, both are, and $m = \mathrm{ord}_q(M-1) = \mathrm{ord}_q(R-1) = r$. But $p_j^{m_j} = p_j^{r_j} \cdot (p_j^N)^{r_j} \equiv p_j^{r_j} \pmod{q^v}$ for each j by (10), so $M \equiv R \pmod{q^v}$. □

Note: the definition of $N_{\mathcal{S}}$ used in the proof is not necessarily minimal. For example if $q \in \mathcal{S} \setminus \{2\}$ then we only need $N \geq v + 1$.

Corollary 5. *The function*

$$\mathrm{rad} \circ \mathsf{k} \colon \mathbb{N} \to \{n \in \mathbb{N} \colon n \text{ is square-free}\}$$

is surjective.

Theorem 6 implies that in principle, for each set $\mathcal{S}$, only finitely many cases are needed to furnish a proof that every M with $\{p : p \mid M\} = \mathcal{S}$ is in the image of k. But for each $\mathcal{S}$ an *ad hoc* argument is needed to deal with each of the finitely many $F(M) \neq 1$ that may occur. We give two examples.

Example. Every number of the form $k = 3^a \cdot 5^b$ with a, $b \in \mathbb{N}$ is in the image of k. Indeed $\mathsf{k}(M) = k$ if

$$M = \begin{cases} 3^{a+1} \cdot 5^{b+1} & \text{if } a \equiv 1 \pmod 2, \\ 3^{a+1} \cdot 5^{b+1} \cdot 7 & \text{if } a \equiv 0 \pmod 2. \end{cases}$$

To see this, first consider $M_1 = 3^{a+1} \cdot 5^{b+1}$. Then $M_1' = k$, so if $F(M_1) = 1$ then $\mathsf{k}(M_1) = k$. In this case we can take $N_{\mathcal{S}_1} = 2$. Indeed, $\mathcal{S}_1 = \{3, 5\}$ and $L = 4$, so $F(M_1) = 4/\gcd(4, 3^{a+1} \cdot 5^{b+1} - 1)$. But $M_1 \equiv (-1)^{a+1} \pmod 4$, so $F(M_1) = 1$ (and we are done) if and only if a is odd.

This leaves the case a even. We deal with this by putting $M_2 = 3^{a+1} \cdot 5^{b+1} \cdot z$ where z is some auxiliary factor to be chosen. This will work well if z is square-free,

$\gcd(z, 3 \cdot 5) = 1$ and $F(M_2) = 1$. This leads to the choice $z = 7$. Then $L_2 = 12$ and M_2' is still equal to k so $(M_2 - 1)M_2' = 3^a \cdot 5^b(3^{a+1} \cdot 5^{b+1} \cdot 7 - 1)$ is divisible by L_2. Hence $F(M_2) = 1$, which is to say, $\mathsf{k}(M_2) = M_2' = k$.

In the previous example if $F(M) \neq 1$ we could proceed by replacing M by Mz for some z. This is not always possible.

Example. Let $k = 3^a \cdot 19^b$ and $M = 3^{a+1} \cdot 19^{b+1}$. Then $M'(M-1) = 3^a \cdot 19^b(3^a \cdot 19^b - 1)$ and $L = 18$, so $F(M_1) = 1$ if and only if $a \geq 2$. The difficult case is $k = 3 \cdot 19^b$. (Instead of a congruence condition on a we have an inequality.) If $b = 1$ we could try introducing a factor z as in the previous example. Thus consider $M = 3^2 \cdot 19^2 \cdot z$ where z is square-free, and $\gcd(z, 3 \cdot 19) = 1$. If $F(M) = 1$ then $3^2 \mid L \mid M'(M-1)$ which implies $3^2 \mid M' = 3 \cdot 19 \cdot z'$, a contradiction. So in this case no such z will work.

Instead, let $M = 7 \cdot 19^{b+1}$. Then $M' = 3 \cdot 19^b$, $L = 18$ and $M'(M-1) = 19^b(7 \cdot 19^{b+1} - 1) \equiv 6 \pmod{18}$, so $\gcd(L, M'(M-1)) = 6$. Thus $\mathsf{k}(M) = 3M' = 3 \cdot 19^b = k$. Hence

$$M = \begin{cases} 7 \cdot 19^{b+1} & \text{if } a = 1 \\ 3^{a+1} \cdot 19^{b+1} & \text{if } a \geq 2 \end{cases} \qquad \text{implies} \qquad \mathsf{k}(M) = 3^a \cdot 19^b.$$

Acknowledgments. The authors wish to thank the referee for his/her useful comments that have helped us to improve this paper.

References

[1] W. R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math.* **139** (1994), 703–722.

[2] W. R. Alford, J. Grantham, Hayman and A. Shallue, Constructing Carmichael numbers through improved subset-product algorithms, *Math. Comp.* **83** (2014), 899–915.

[3] R. C. Baker and W. M. Schmidt, Diophantine problems in variables restricted to the values 0 and 1, *J. Number Theory* **12** (1980), 460–486.

[4] R. D. Carmichael, Note on a new number theory function, *Bull. Amer. Math. Soc.* **16** (1910), 232–238.

[5] L. E. Dickson, A new extension of Dirichlet's theorem on prime numbers, *Messenger of Mathematics* **33** (1904), 155–161. Available at `https://oeis.org/wiki/File:A_new_extension_of_Dirichlet%27s_theorem_on_prime_numbers. pdf`.

[6] P. Erdős, C. Pomerance and E. Schmutz, Carmichael's lambda function, *Acta Arith.* **58** (1991), 363–385.

[7] J. M. Grau and A. M. Oller-Marcén, On k-Lehmer numbers, *Integers* **12** (2012), 1081–1089.

[8] J. M. Grau and A. M. Oller-Marcén, On the congruence $\sum_{j=1}^{n-1} j^{k(n-1)} \equiv -1 \mod n$, k-strong Giuga and k-Carmichael numbers. (2013). Available at `arXiv:1311.3522v1`.

[9] R. Guy, *Unsolved Problems in Number Theory*, 2nd edition, Springer, 1994.

[10] A. R. Korselt, Problème chinois, *L'Intermédiaire des Mathématiciens* **6** (1899), 142–143. Available at `http://gdz.sub.uni-goettingen.de/dms/load/img/?PID=PPN599473517_0006|LOG_0018&physid=PHYS_0151`.

[11] D. H. Lehmer, On Euler's totient function, *Bull. Amer. Math. Soc.* **38** (1932), 745–751.

[12] K. Matomäki, Carmichael numbers in arithmetic progressions, *J. Aust. Math. Soc.* **94** (2013), 268–275.

[13] N. McNew, Radically weakening the Lehmer and Carmichael conditions, *Int. J. Number Theory* **09** (2013), 1215–1224.

[14] N. McNew and T. Wright, Infinitude of k-Lehmer numbers which are not Carmichael, to appear in *Int. J. Number Theory.* Available at `http://www.worldscientific.com/doi/abs/10.1142/S1793042116501153`.

[15] PARI, Bordeaux, Available at `http://pari.math.u-bordeaux.fr/`.

[16] K. Prachar, Über die Anzahl der Teiler einer natürlichen Zahl, welche die Form $p-1$ haben, *Monatsh. Math.* **59** (1955) 91–97. Available at `https://eudml.org/doc/176962`.

[17] P. Ribenboim, *The new Book of Prime Number Records*, Springer, 1988.

[18] A. Schinzel and W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958), 185–208.

[19] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences. Available at `http://oeis.org`.

[20] T. Wright, Infinitely many Carmichael numbers in arithmetic progressions, *Bull. Lond. Math. Soc.* **45** (2013), 943–952.