When does each prime dividing $\varphi(n)$ also divide $n-1$

Nathan McNew
Dartmouth College
Hanover, New Hampshire

Québec/Maine Number Theory Conference
September 29th, 2012

Lehmer's Condition

In 1932, Lehmer asked whether there exist composite integers n for which $\varphi(n) | n - 1$.
Lehmer showed that such n must be:

- odd
- squarefree
- $\omega(n) \geq 7$

Lehmer's Condition

In 1932, Lehmer asked whether there exist composite integers n for which $\varphi(n)|n-1$.

Lehmer showed that such n must be:

- odd
- squarefree
- $\omega(n) \geq 7$

We know now that for such "Lehmer Numbers"

- $\omega(n) \geq 14$ (Cohen and Hagis, 1980)
- $n > 10^{30}$ (Pinch, 2006)
- If $3|n$ then $n > 5.5 \times 10^{570}$ and $\omega(n) \geq 212$. (Lieuwens, 1970)

Lehmer's Condition

In 1932, Lehmer asked whether there exist composite integers n for which $\varphi(n) | n-1$.

Lehmer showed that such n must be:

- odd
- squarefree
- $\omega(n) \geq 7$

We know now that for such "Lehmer Numbers"

- $\omega(n) \geq 14$ (Cohen and Hagis, 1980)
- $n > 10^{30}$ (Pinch, 2006)
- If $3|n$ then $n > 5.5 \times 10^{570}$ and $\omega(n) \geq 212$. (Lieuwens, 1970)
- If $\mathcal{L}(x)$ counts the Lehmer Numbers up to x then as $x \to \infty$

$$\mathcal{L}(x) \leq \frac{x^{1/2}}{(\log x)^{1/2+o(1)}} \quad \text{(Luca and Pomerance, 2009)}$$

Carmichael's Condition

A Carmichael number is a composite integer n which satisfies the congruence

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

for all integers a relatively prime to n.

Carmichael's Condition

A Carmichael number is a composite integer n which satisfies the congruence

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

for all integers a relatively prime to n.

Korselt's Criterion (1899)

A composite integer n is a Carmichael number if and only if n is square-free, and for each prime divisor p of n, $p - 1 | n - 1$.

Carmichael's Condition

In 1910 Robert Carmichael found the smallest example, 561, and gave a new characterization of these numbers:

Let $\lambda(n)$ be the size of the largest cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. This function satisfies

- $\lambda(p^k) = \varphi(p^k)$ if p is an odd prime or if $p = 2$ and $k < 3$
- $\lambda(2^k) = \frac{1}{2}\varphi(2^k)$ if $k \geq 3$
- $\lambda(p_1^{k_1} \cdots p_i^{k_i}) = \mathrm{lcm}[\lambda(p_1^{k_1}), \cdots, \lambda(p_i^{k_i})]$

Theorem

A composite number n is a Carmichael number if and only if $\lambda(n) | n - 1$.

Carmichael's Condition

Note that $\lambda(n)|\varphi(n)$, so Carmichael's condition is a weakening of Lehmer's.

Carmichael's Condition

Note that $\lambda(n)|\varphi(n)$, so Carmichael's condition is a weakening of Lehmer's.

What we know about Carmichael numbers:

Carmichael's Condition

Note that $\lambda(n)|\varphi(n)$, so Carmichael's condition is a weakening of Lehmer's.

What we know about Carmichael numbers:

- They have at least 3 prime factors.

Carmichael's Condition

Note that $\lambda(n)|\varphi(n)$, so Carmichael's condition is a weakening of Lehmer's.

What we know about Carmichael numbers:

- They have at least 3 prime factors.
- There are infinitely many. (Alford, Granville and Pomerance, 1994) In fact if $C(x)$ is the count of Carmichael numbers up to x then for sufficiently large x, $C(x) > x^{0.33}$. (Harman, 2005)

Carmichael's Condition

Note that $\lambda(n) | \varphi(n)$, so Carmichael's condition is a weakening of Lehmer's.

What we know about Carmichael numbers:

- They have at least 3 prime factors.
- There are infinitely many. (Alford, Granville and Pomerance, 1994) In fact if $C(x)$ is the count of Carmichael numbers up to x then for sufficiently large x, $C(x) > x^{0.33}$. (Harman, 2005)
- As $x \to \infty$,

$$C(x) \leq x^{1-\{1+o(1)\} \log\log\log x / \log\log x}$$

Carmichael's Condition

Note that $\lambda(n)|\varphi(n)$, so Carmichael's condition is a weakening of Lehmer's.

What we know about Carmichael numbers:

- They have at least 3 prime factors.
- There are infinitely many. (Alford, Granville and Pomerance, 1994) In fact if $C(x)$ is the count of Carmichael numbers up to x then for sufficiently large x, $C(x) > x^{0.33}$. (Harman, 2005)
- As $x \to \infty$,

$$C(x) \leq x^{1-\{1+o(1)\}\log\log\log x/\log\log x}$$

- Heuristically, this is believed to be the actual asymptotic value of $C(x)$. (Pomerance, 1988)

New Condition

In a recent paper, Grau and Oller-Marcén define a k-**Lehmer number** to be a composite integer n satisfying $\varphi(n)|(n-1)^k$ for a fixed k.

New Condition

In a recent paper, Grau and Oller-Marcén define a k-**Lehmer number** to be a composite integer n satisfying $\varphi(n)|(n-1)^k$ for a fixed k.

They also look at those composite n which satisfy $\varphi(n)|(n-1)^k$ for some k. Such n satisfy

$$\mathrm{rad}(\varphi(n))|n-1$$

Where $\mathrm{rad}(m)$ denotes the product of the primes dividing m.

New Condition

Notation:
Let $\kappa(n) = \text{rad}(\varphi(n))$. (Note that $\kappa(n) = \text{rad}(\lambda(n))$.)
Let $K(x)$ be the number of composite n up to x for which $\kappa(n) | n - 1$.

New Condition

Notation:
Let $\kappa(n) = \text{rad}(\varphi(n))$. (Note that $\kappa(n) = \text{rad}(\lambda(n))$.)
Let $K(x)$ be the number of composite n up to x for which $\kappa(n)|n-1$.

What do we know about composite n which satisfy this condition?

- They are odd. (if $n > 2$ then $\kappa(n)$ is even)

Notation:
Let $\kappa(n) = \text{rad}(\varphi(n))$. (Note that $\kappa(n) = \text{rad}(\lambda(n))$.)
Let $K(x)$ be the number of composite n up to x for which $\kappa(n)|n-1$.

What do we know about composite n which satisfy this condition?

- They are odd. (if $n > 2$ then $\kappa(n)$ is even)
- They are squarefree. (if $p^2|n$, then $p|\varphi(n)$ and $p \nmid n-1$)

New Condition

Notation:
Let $\kappa(n) = \text{rad}(\varphi(n))$. (Note that $\kappa(n) = \text{rad}(\lambda(n))$.)
Let $K(x)$ be the number of composite n up to x for which $\kappa(n)|n-1$.

What do we know about composite n which satisfy this condition?

- They are odd. (if $n > 2$ then $\kappa(n)$ is even)
- They are squarefree. (if $p^2|n$, then $p|\varphi(n)$ and $p\nmid n-1$)
- All Carmichael (Lehmer) numbers satisfy the condition.

Computations

n	$C(10^n)$	$K(10^n)$
2	0	4
3	1	19
4	7	103
5	16	422
6	43	1559
7	105	5645
8	255	19329
9	646	64040
10	1547	205355
11	3605	631949

Computations

n	$C(10^n)$	$K(10^n)$
2	0	4
3	1	19
4	7	103
5	16	422
6	43	1559
7	105	5645
8	255	19329
9	646	64040
10	1547	205355
11	3605	631949

Conjecture: $\lim_{x\to\infty} \frac{K(x)}{C(x)} = \infty$

Upper Bound

In light of this data, it is surprising to see that $K(x)$ satisfies the same upper bound as $C(x)$.

Upper Bound

In light of this data, it is surprising to see that $K(x)$ satisfies the same upper bound as $C(x)$.

Theorem

Define $L(x) = \exp(\log x \frac{\log\log\log x}{\log\log x})$*. Then as* $x \to \infty$*,*

$$K(x) \leq \frac{x}{L(x)^{1+o(1)}} = x^{1-(1+o(1)) \log\log\log x / \log\log x}.$$

The proof is similar to the proof for the upper bound of Carmichael numbers.

Proof Idea

Consider two cases to count n satisfying our condition.

Case 1: n has a large prime divisor p.

Proof Idea

Consider two cases to count n satisfying our condition.

Case 1: n has a large prime divisor p.
Write $n = mp$, so $m \leq \frac{x}{p}$.
$\kappa(mp) | mp - 1$, so $mp \equiv 1 \pmod{\mathrm{rad}(p-1)}$.

Proof Idea

Consider two cases to count n satisfying our condition.

Case 1: n has a large prime divisor p.
Write $n = mp$, so $m \leq \frac{x}{p}$.
$\kappa(mp) | mp - 1$, so $mp \equiv 1 \pmod{\text{rad}(p-1)}$.
Now, $p \equiv 1 \pmod{\text{rad}(p-1)}$, so $m \equiv 1 \pmod{\text{rad}(p-1)}$.
Thus there are at most $\frac{x}{p \cdot \text{rad}(p-1)}$ possibilities for $m > 1$.

Proof Idea

Consider two cases to count n satisfying our condition.

Case 1: n has a large prime divisor p.
Write $n = mp$, so $m \leq \frac{x}{p}$.
$\kappa(mp)|mp-1$, so $mp \equiv 1 \pmod{\text{rad}(p-1)}$.
Now, $p \equiv 1 \pmod{\text{rad}(p-1)}$, so $m \equiv 1 \pmod{\text{rad}(p-1)}$.
Thus there are at most $\frac{x}{p \cdot \text{rad}(p-1)}$ possibilities for $m > 1$.
Summing this over p we have

$$\sum_{p > L(x)^2} \frac{x}{p \cdot \text{rad}(p-1)}$$

Proof Idea

Consider two cases to count n satisfying our condition.

Case 1: n has a large prime divisor p.
Write $n = mp$, so $m \le \frac{x}{p}$.
$\kappa(mp) | mp - 1$, so $mp \equiv 1 \pmod{\text{rad}(p-1)}$.
Now, $p \equiv 1 \pmod{\text{rad}(p-1)}$, so $m \equiv 1 \pmod{\text{rad}(p-1)}$.
Thus there are at most $\frac{x}{p \cdot \text{rad}(p-1)}$ possibilities for $m > 1$.
Summing this over p we have

$$\sum_{p > L(x)^2} \frac{x}{p \cdot \text{rad}(p-1)} \le \sum_{c > L(x)^2} \frac{x}{c \cdot \text{rad}(c)}$$

Proof Idea

Consider two cases to count n satisfying our condition.

Case 1: n has a large prime divisor p.
Write $n = mp$, so $m \leq \frac{x}{p}$.
$\kappa(mp) | mp - 1$, so $mp \equiv 1 \pmod{\text{rad}(p-1)}$.
Now, $p \equiv 1 \pmod{\text{rad}(p-1)}$, so $m \equiv 1 \pmod{\text{rad}(p-1)}$.
Thus there are at most $\frac{x}{p \cdot \text{rad}(p-1)}$ possibilities for $m > 1$.
Summing this over p we have

$$\sum_{p > L(x)^2} \frac{x}{p \cdot \text{rad}(p-1)} \leq \sum_{c > L(x)^2} \frac{x}{c \cdot \text{rad}(c)} \leq \sum_{\substack{d > L(x)^2 \\ d \text{ squarefull}}} \frac{x}{d}$$

Proof Idea

Consider two cases to count n satisfying our condition.

Case 1: n has a large prime divisor p.
Write $n = mp$, so $m \leq \frac{x}{p}$.
$\kappa(mp)|mp - 1$, so $mp \equiv 1 \pmod{\mathrm{rad}(p-1)}$.
Now, $p \equiv 1 \pmod{\mathrm{rad}(p-1)}$, so $m \equiv 1 \pmod{\mathrm{rad}(p-1)}$.
Thus there are at most $\frac{x}{p \cdot \mathrm{rad}(p-1)}$ possibilities for $m > 1$.
Summing this over p we have

$$\sum_{p > L(x)^2} \frac{x}{p \cdot \mathrm{rad}(p-1)} \leq \sum_{c > L(x)^2} \frac{x}{c \cdot \mathrm{rad}(c)} \leq \sum_{\substack{d > L(x)^2 \\ d \text{ squarefull}}} \frac{x}{d} \leq \frac{x}{L(x)}$$

Proof Idea

Case 2: n has only small prime divisors.
So n has a divisor d with $\frac{x}{L(X)^3} < d \leq \frac{x}{L(x)}$. Again write $n = md$, so $m \equiv 1 \pmod{\kappa(d)}$.
Now there are at most $1 + \lfloor \frac{x}{d\kappa(d)} \rfloor$ possibilities for m.

Proof Idea

Case 2: n has only small prime divisors.
So n has a divisor d with $\frac{x}{L(X)^3} < d \leq \frac{x}{L(x)}$. Again write $n = md$, so $m \equiv 1 \pmod{\kappa(d)}$.
Now there are at most $1 + \lfloor \frac{x}{d\kappa(d)} \rfloor$ possibilities for m.

$$\sum_{d} \left(1 + \frac{x}{d\kappa(d)}\right) \leq \frac{x}{L(x)} + \sum_{c \leq L(x)^3} \frac{x}{c} \sum_{\kappa(d)=c} \frac{1}{d}$$

Proof Idea

Case 2: n has only small prime divisors.
So n has a divisor d with $\frac{x}{L(X)^3} < d \leq \frac{x}{L(x)}$. Again write $n = md$, so $m \equiv 1 \pmod{\kappa(d)}$.
Now there are at most $1 + \lfloor \frac{x}{d\kappa(d)} \rfloor$ possibilities for m.

$$\sum_{d} \left(1 + \frac{x}{d\kappa(d)}\right) \leq \frac{x}{L(x)} + \sum_{c \leq L(x)^3} \frac{x}{c} \underbrace{\sum_{\kappa(d)=c} \frac{1}{d}}_{\leq L(x)^{-1+o(1)}}$$

Proof Idea

Case 2: n has only small prime divisors.
So n has a divisor d with $\frac{x}{L(X)^3} < d \leq \frac{x}{L(x)}$. Again write $n = md$, so $m \equiv 1 \pmod{\kappa(d)}$.
Now there are at most $1 + \lfloor \frac{x}{d\kappa(d)} \rfloor$ possibilities for m.

$$\sum_d \left(1 + \frac{x}{d\kappa(d)}\right) \leq \frac{x}{L(x)} + \sum_{c \leq L(x)^3} \frac{x}{c} \underbrace{\sum_{\kappa(d)=c} \frac{1}{d}}_{\leq L(x)^{-1+o(1)}} \ll \frac{x}{L(x)^{1+o(1)}}$$

The first 45 n with $\kappa(n)|n-1$

The first 45 n with $\kappa(n) | n - 1$

15	3 * 5		703	19 * 37		1843	19 * 97
51	3 * 17		763	7 * 109		1891	31 * 61
85	5 * 17		771	3 * 257		2047	23 * 89
91	7 * 13		949	13 * 73		2071	19 * 109
133	7 * 19		1105	5 * 13 * 17		2091	3 * 17 * 41
247	13 * 19		1111	11 * 101		2119	13 * 163
255	3 * 5 * 17		1141	7 * 163		2431	11 * 13 * 17
259	7 * 37		1261	13 * 97		2465	5 * 17 * 29
435	3 * 5 * 29		1285	5 * 257		2509	13 * 193
451	11 * 41		1351	7 * 193		2701	37 * 73
481	13 * 37		1387	19 * 73		2761	11 * 251
511	7 * 73		1417	13 * 109		2821	7 * 13 * 31
561	3 * 11 * 17		1615	5 * 17 * 19		2955	3 * 5 * 197
595	5 * 7 * 17		1695	3 * 5 * 113		3031	7 * 433
679	7 * 97		1729	7 * 13 * 19		3097	19 * 163

Two prime factors

Many of these numbers have exactly two prime factors. Carmichael numbers always have at least 3. How big a contribution can these numbers make?

Two prime factors

Many of these numbers have exactly two prime factors. Carmichael numbers always have at least 3. How big a contribution can these numbers make?

Let $K_d(x) = \#\{x < n | n \text{ composite}, \kappa(n) | n-1, \omega(n) = d\}$.

Two prime factors

Many of these numbers have exactly two prime factors. Carmichael numbers always have at least 3. How big a contribution can these numbers make?

Let $K_d(x) = \#\{x < n | n \text{ composite}, \kappa(n) | n - 1, \omega(n) = d\}$.

Theorem

As $x \to \infty$, $K_2(x) \ll x^{1/2+o(1)}$.

To prove this we observe that $\kappa(pq) | pq - 1$ if and only if $\text{rad}(p-1) = \text{rad}(q-1)$ and count pairs of primes which have this property.

Two prime factors

Many of these numbers have exactly two prime factors. Carmichael numbers always have at least 3. How big a contribution can these numbers make?

Let $K_d(x) = \#\{x < n | n \text{ composite}, \kappa(n) | n-1, \omega(n) = d\}$.

Theorem

As $x \to \infty$, $K_2(x) \ll x^{1/2+o(1)}$.

To prove this we observe that $\kappa(pq) | pq - 1$ if and only if $\text{rad}(p-1) = \text{rad}(q-1)$ and count pairs of primes which have this property.

Assuming a strong form of the prime k-tuples conjecture, we can show that $K_2(x)$ is at least of order $x^{1/2}/(\log x)^2$.

Two prime factors

Many of these numbers have exactly two prime factors. Carmichael numbers always have at least 3. How big a contribution can these numbers make?

Let $K_d(x) = \#\{x < n | n \text{ composite}, \kappa(n) | n-1, \omega(n) = d\}$.

Theorem

As $x \to \infty$, $K_2(x) \ll x^{1/2+o(1)}$.

To prove this we observe that $\kappa(pq) | pq - 1$ if and only if $\text{rad}(p-1) = \text{rad}(q-1)$ and count pairs of primes which have this property.

Assuming a strong form of the prime k-tuples conjecture, we can show that $K_2(x)$ is at least of order $x^{1/2}/(\log x)^2$.

If we could show that there are infinitely many pairs of primes p, q with $\text{rad}(p-1) = \text{rad}(q-1)$, then we could prove $\lim_{x\to\infty} K(x) - C(x) = \infty$.

d prime factors

What about $K_d(x)$ for $d \geq 3$? For Carmichael numbers it is conjectured that $C_d(x) = x^{1/d+o(1)}$ as $x \to \infty$, and known that $C_3(x) \ll x^{7/20+\epsilon}$. (Heath-Brown, 2007) It would make sense to make the same conjectures for $K_d(x)$.

d prime factors

What about $K_d(x)$ for $d \geq 3$? For Carmichael numbers it is conjectured that $C_d(x) = x^{1/d+o(1)}$ as $x \to \infty$, and known that $C_3(x) \ll x^{7/20+\epsilon}$. (Heath-Brown, 2007) It would make sense to make the same conjectures for $K_d(x)$.

What we can prove is:

Theorem

For $d \geq 3$, $K_d(x) \ll x^{1-\frac{1}{2d}}$.

using the same techniques as the first theorem.

k-Lehmer Numbers

The bound in the main theorem resolves several conjectures made by Grau and Oller-Marcén in their paper on k-Lehmer numbers. Our bound shows that these integers remain less numerous than the primes. (i.e. $K(x) = O(\pi(x))$

k-Lehmer Numbers

The bound in the main theorem resolves several conjectures made by Grau and Oller-Marcén in their paper on k-Lehmer numbers. Our bound shows that these integers remain less numerous than the primes. (i.e. $K(x) = O(\pi(x))$

What more can we say about the k-Lehmer numbers? (Composite n such that $\varphi(n)|(n-1)^k$)

k-Lehmer Numbers

The bound in the main theorem resolves several conjectures made by Grau and Oller-Marcén in their paper on k-Lehmer numbers. Our bound shows that these integers remain less numerous than the primes. (i.e. $K(x) = O(\pi(x))$

What more can we say about the k-Lehmer numbers? (Composite n such that $\varphi(n)|(n-1)^k$)

Theorem

Let $L_k(x)$ be the number of k-Lehmer numbers up to x. Then for $k \geq 2$ we have $L_k(x) \ll x^{1-\frac{1}{4k-1}}$.

k-Lehmer Numbers

The bound in the main theorem resolves several conjectures made by Grau and Oller-Marcén in their paper on k-Lehmer numbers. Our bound shows that these integers remain less numerous than the primes. (i.e. $K(x) = O(\pi(x))$

What more can we say about the k-Lehmer numbers? (Composite n such that $\varphi(n)|(n-1)^k$)

Theorem

Let $L_k(x)$ be the number of k-Lehmer numbers up to x. Then for $k \geq 2$ we have $L_k(x) \ll x^{1-\frac{1}{4k-1}}$.

Recall, that for $k = 1$ we know $L_1 \leq \frac{x^{1/2}}{(\log x)^{1/2+o(1)}}$

k-Lehmer Numbers

The bound in the main theorem resolves several conjectures made by Grau and Oller-Marcén in their paper on k-Lehmer numbers. Our bound shows that these integers remain less numerous than the primes. (i.e. $K(x) = O(\pi(x))$

What more can we say about the k-Lehmer numbers? (Composite n such that $\varphi(n)|(n-1)^k$)

Theorem

Let $L_k(x)$ be the number of k-Lehmer numbers up to x. Then for $k \geq 2$ we have $L_k(x) \ll x^{1-\frac{1}{4k-1}}$.

Recall, that for $k = 1$ we know $L_1 \leq \frac{x^{1/2}}{(\log x)^{1/2+o(1)}}$

Strong prime k-tuples gives us $L_3(x) \gg x^{1/2}/(\log x)^2$ just considering pairs of primes.

Thank You!