Article 9 INTEGERS 11A (2011)

Proceedings of Integers Conference 2009

THE NUMBER OF SOLUTIONS OF $\lambda(X) = N$

Kevin Ford
Dept. of Mathematics, University of Illinois at Urbana-Champaign, Urbana, Illinois
ford@math.uiuc.edu

Florian Luca
Instituto de Matemáticas, Universidad Nacional Autonoma de México, Morelia, Michoacán, México
fluca@matmor.unam.mx

Received: 11/16/09, Accepted: 3/24/10, Published: 3/9/11

Abstract

We study the question of whether for each n there is an $m \neq n$ with $\lambda(m) = \lambda(n)$, where λ is Carmichael's function. We give a "near" proof of the fact that this is the case unconditionally, and a complete conditional proof under the Extended Riemann Hypothesis.

–To Professor Carl Pomerance on his 65th birthday

1. Introduction

Let $\lambda(n)$ be the Carmichael function, that is, $\lambda(n)$ is the largest order of any number modulo n. Recently, Banks et al [1] made the following conjecture:

Conjecture 1. *For every positive integer n, there is an integer $m \neq n$ with $\lambda(m) = \lambda(n)$.*

The analogous question for the Euler function $\phi(n)$ is known as Carmichael's conjecture and remains unsolved. If there are counterexamples to Conjecture 1, the authors of [1] proved that all such counterexamples n are multiples of the smallest counterexample n_0. Further, they showed that if n_0 exists, then n_0 is divisible by every prime less than 30000. In this note, we prove that Conjecture 1 follows from the Extended Riemann Hypothesis (ERH) for Dirichlet L-functions, and also we come very close to proving the conjecture unconditionally.

If n has prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$, then $\lambda(n) = [\lambda(p_1^{e_1}), \ldots, \lambda(p_k^{e_k})]$, where $[a_1, \ldots, a_k]$ denotes the least common multiple of $a_1, \ldots, a_k$, $\lambda(p^e) = p^{e-1}(p-$

1) when p is odd or $e \le 2$, and $\lambda(2^e) = 2^{e-2}$ when $e \ge 3$. The following is proved in Section 7 of [1].

Lemma 2. *Suppose n_0 exists, that is, Conjecture 1 is false. Then (i) $2^4|n_0$ and (ii) if $(p-1)|\lambda(n_0)$ for a prime p, then $p^2|n_0$.*

Proof. Since $\lambda(1) = \lambda(2)$ and $\lambda(4) = \lambda(8)$, part (i) follows. If $(p-1)|\lambda(n_0)$ and $p \nmid n_0$, then $\lambda(n_0) = \lambda(pn_0)$, which proves that $p|n_0$. Assume that $p^2 \nmid n_0$. By the minimality of n_0, $\lambda(n_0/p) = \lambda(m)$ for some $m \ne n_0/p$. We have $p \nmid m$, else $(p-1)|\lambda(n_0/p)$ and $\lambda(n_0) = \lambda(n_0/p)$. Thus,

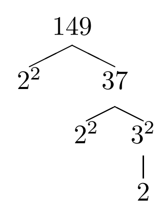
$$\lambda(n_0) = [p-1, \lambda(n_0/p)] = [p-1, \lambda(m)] = \lambda(pm),$$

a contradiction. Therefore, $p^2|n_0$, proving (ii). □

With Lemma 2, it is easy to show that many primes must divide n_0. For example, by (i) and (ii) with $p = 3$ and $p = 5$, we immediately obtain $3^2|n_0$ and $5^2|n_0$. Thus, $2^2 \cdot 3 \cdot 5|\lambda(n_0)$, and by (ii) again, n_0 is divisible by 7^2, 11^2, 13^2, 31^2 and 61^2. Subject to certain hypotheses, we may continue this process and deduce that every prime must divide n_0, which would prove Conjecture 1.

Notation. Throughout, the letters p, q, r, s, with or without subscripts, will always denote primes. By *prime power* we mean a number of the form p^a where p is prime and $a \ge 1$, and a *proper prime power* is a prime power with $a \ge 2$.

For a prime q, we construct a tree $T(q)$ with q as the root node as follows. Below q form links to each prime power p^e with $p^e \| (q-1)$. Now continue the process, linking each p^e to the prime powers r^b with $r^b \| (p-1)$, etc. The end result will be a tree with leaves which are powers of 2. For example, here is the tree corresponding to $q = 149$.



Let $f(q)$ denote the largest proper prime power occurring in the tree. Set $f(q) = 1$ if there are no proper prime powers in the tree; this only happens when $q \in \{2, 3, 7, 43\}$ (If $q > 43$ is the smallest prime with $f(q) = 1$, then $q-1$ is squarefree and $q > 2\cdot3\cdot7\cdot43+1$ by explicit calculation, so $q-1$ has a prime divisor r other than $2, 3, 7, 43$. By the minimality of q, $f(r) > 1$ and therefore $f(q) > 1$, a contradiction). Alternatively, we may define $f(q)$ inductively by the formulas $f(2) = 1$ and if $q \ge 3$ and $q - 1 = p_1^{e_1} \cdots p_k^{e_k}$ with $e_1 = \cdots = e_h = 1 < e_{h+1} \le e_{h+2} \le \cdots \le e_k$, then

$$f(q) = \max(f(p_1), \ldots, f(p_h), p_{h+1}^{e_{h+1}}, \ldots, p_k^{e_k}).$$

For example, $f(149) = 9$. The tree $T(q)$ is similar to the tree constructed for the Pratt primality certificate [6].

Conjecture 3. For every prime power p^a, there is a prime q with $p^a|(q-1)$ and $f(q) < p^{a+1}$.

Note that we must have $p^a \| (q-1)$.

Theorem 4. *Conjecture 3 implies Conjecture 1.*

Proof. Suppose Conjecture 3 is true and Conjecture 1 is false. Let p^{a+1} be the smallest prime power not dividing $\lambda(n_0)$ (here $a \ge 0$). Each prime power divisor of $p-1$ is $< p^{a+1}$ and hence $(p-1)|\lambda(n_0)$. Lemma 2 implies that $p^2|n_0$, thus $p|\lambda(n_0)$ and $a \ge 1$. Let $b = a+1$ if $p > 2$ and $b = a+2$ if $p = 2$, so that $\lambda(p^b) = p^a(p-1)$. We have $p^b \| n_0$, since $p^{b+1}|n_0$ implies $p^{a+1}|\lambda(n_0)$ and $p^b \nmid n_0$ implies $\lambda(n_0) = \lambda(pn_0)$. We next claim that every prime r with $f(r) < p^{a+1}$ satisfies $r^2|n_0$. Proceed by induction on r, noting that the case $r = 2$ is taken care of by Lemma 2 (i). Suppose $s > 2$, $f(s) < p^{a+1}$ and every prime $r < s$ with $f(r) < p^{a+1}$ satisfies $r^2|n_0$. If $r \| (s-1)$, then $f(r) < p^{a+1}$ and hence $r|\lambda(n_0)$, and if $r^c \| (s-1)$ with $c \ge 2$ then $r^c < p^{a+1}$ and hence $r^c|\lambda(n_0)$. Consequently, $(s-1)|\lambda(n_0)$, and applying Lemma 2 once again we see that $s^2|n_0$. By hypothesis, there is a prime q with $p^a|(q-1)$ and $f(q) < p^{a+1}$. In particular, $q^2|n_0$ and $q|\lambda(n_0)$. This means $p^a|\lambda(n_0/p^b)$ and

$$\lambda(n_0) = [\lambda(p^b), \lambda(n_0/p^b)] = [\lambda(p^{b-1}), \lambda(n_0/p^b)] = \lambda(n_0/p),$$

a contradiction. ∎

We pose the following questions. (1) For each proper prime power p^a, is there a prime q with $f(q) = p^a$? (2) Is there a prime power p^a so that there are infinitely many primes q with $f(q) = p^a$? (3) Does $f(q) \to \infty$ as $q \to \infty$? Computations suggest that there are infinitely many primes q with $f(q) = 4$, but this will be very difficult to prove.

It is clear that $f(q)$ is at most the largest prime power dividing $q-1$, thus

$$p^a \| (q-1) \text{ and } q < p^{2a+1} \implies f(q) < p^{a+1}. \tag{1}$$

Hence, it is almost sufficient to find a prime $q \equiv 1 \pmod{p^a}$ with $q < (p^a)^{2+1/a}$. Let $P(b,m)$ denote the least prime which is $\equiv b \pmod m$. Linnik proved that there is a constant L such that $P(b,m) \ll m^L$ for all coprime b, m. The best constant known today is $L = 5.5$ and due to Heath-Brown. However, the Extended Riemann Hypothesis (ERH) for Dirichlet L-functions implies that

$$\left| \pi(x,m,b) - \frac{\mathrm{li}(x)}{\phi(m)} \right| \le x^{1/2} \log(xm^2) \tag{2}$$

uniformly in x, m, b [5], where $\pi(x, m, b)$ is the number of primes $r \le x$ with $r \equiv b \pmod{m}$ and $\mathrm{li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$. Consequently, we may take $L = 2 + \varepsilon$ for any fixed ε. Using (2) and a finer analysis of $f(q)$, we prove the following.

Theorem 5. *ERH implies Conjecture 3.*

The main result of this paper is the following "near" proof of Conjecture 3.

Theorem 6. *For an effective constant K, if $p^a > K$ then there is a prime q with $p^a|(q-1)$ and $f(q) < p^{a+1}$.*

Theorem 6 is proved in the next section. Next, the proof of Theorem 5 will be given in Section 3.

2. Proof of Theorem 6

We need first an effective lower bound for the number of primes in an arithmetic progression with prime power modulus.

Lemma 7. *There are positive, effective constants K_1, K_2, K_3 so that if $p^a \ge K_1$ and $x \ge p^{aK_2}$, then*

$$\pi(x; p^a, 1) - \pi(x; p^{a+1}, 1) \ge K_3 \frac{x/\log x}{p^{a+1/2}\log p}.$$

Proof. This basically follows from an effective version of Linnik's Theorem. For a modulus $q \ge 3$, let $\beta = \beta(q)$ the largest real zero of an L-function (primitive or not) of a real character of modulus q. If no such zero exists, set $\beta = \frac{1}{2}$. By Prop. 18.5 of [4], there are effective constants c_1, c_2, c_3 so that if $x \ge q^{c_1}$ then

$$\Psi(x; q, 1) = \frac{x}{\phi(q)}\left[1 - \frac{x^{\beta-1}}{\beta} + \theta\left(x^{-\eta} + \frac{\log q}{q}\right)\right], \tag{3}$$

where $|\theta| \le c_2$ and

$$\eta = \eta(q) = \frac{c_3 \log(2 + \frac{2}{(1-\beta)\log q})}{\log q}.$$

If $p > 2$, then the real character modulo p^a has conductor p, hence $\beta(p^a) = \beta(p)$. If $p = 2$ then any real character modulo p^a has conductor 4 or 8 and $\beta(2^a) = \frac{1}{2}$. By a classical theorem [2, Section 14 (12)], there is an effective constant $c > 0$ so that we have

$$\beta(p^a) \le 1 - \frac{c}{p^{1/2}\log^2 p}.$$

Fix a prime power $p^a \ge 8$ and let $\beta = \beta(p)$, $\eta = \eta(p^{a+1})$. By (3) with $q = p^a$ and with $q = p^{a+1}$, we have

$$\Psi(x; p^a, 1) - \Psi(x; p^{a+1}, 1) = \frac{x}{p^a}\left[1 - \frac{x^{\beta(p)-1}}{\beta(p)} + \theta'\left(x^{-\eta} + \frac{\log p^a}{p^a}\right)\right], \tag{4}$$

where $|\theta'| \le c_2\frac{p+1}{p-1} \le 3c_2$. If $\beta \le 1 - 1/\log p^a$, then the left side of (4) is $\ge x/(2p^a)$ if p^a and K_2 are sufficiently large. If $\beta > 1 - 1/\log p^a$, let $\delta = 1-\beta$, so that

$$\begin{aligned} 1 - \frac{x^{\beta-1}}{\beta} \ge \beta - x^{-\delta} \ge 1 - \delta - e^{-\delta K_2 \log p^a} \\ \ge -\delta + \frac{\delta K_2 \log p^a}{1+\delta K_2 \log p^a} \ge \delta\left(-1 + \frac{K_2 \log p^a}{1+K_2}\right) \\ \ge \frac{K_2}{2+2K_2}(\delta \log p^a) \end{aligned}$$

and

$$x^{-\eta} \le \left(\frac{\delta \log p^a}{2}\right)^{c_3K_2} \le 2^{-K_2c_3}(\delta \log p^a).$$

Hence,

$$\Psi(x;p^a,1) - \Psi(x;p^{a+1},1) \gg \frac{x}{p^a}(\delta \log p^a) \gg \frac{x}{p^{a+1/2}\log p}.$$

Finally,

$$\pi(x;p^a,1) - \pi(x;p^{a+1},1) \ge \frac{\Psi(x;p^a,1) - \Psi(x;p^{a+1},1) - O(\sqrt{x})}{\log x}$$

and the proof is complete. □

Our next tool is an upper bound for the number of *prime chains* of a certain type. A *prime chain* is a sequence $p_1, \ldots, p_k$ of primes such that $p_i | (p_{i+1} - 1)$ for $1 \le i \le k-1$. The following is a result from [3].

Lemma 8. *For every $\varepsilon > 0$ there is an effective constant $C(\varepsilon)$ so that for any prime p, the number of prime chains with $p_1 = p$ and $p_k \le x$ (varying k) is $\le C(\varepsilon)(x/p)^{1+\varepsilon}$.*

Remark. At the moment, the method of [3] gives

$$C(\varepsilon) = \exp\exp\left((1+o(1))\frac{1}{\varepsilon}\log\frac{1}{\varepsilon}\right)$$

as $\varepsilon \to 0^+$. We need a numerical value of $C(\varepsilon)$ in one case. By the argument in Section 3 of [3], if $y < p$, w is the product of the primes $\le y$, and $s > 1$, then the number of prime chains in question is at most the largest column sum of

$$x^s \sum_{0 \le k \le \frac{\log x}{\log 2}} M^k, \quad M = \Bigg(\sum_{\substack{m \ge 1 \\ am+1 \equiv b (\bmod w)}} m^{-s}\Bigg)_{b,a \in (\mathbb{Z}/w\mathbb{Z})^*}.$$

If all the eigenvalues of M lie inside the unit circle, then $\sum_{k=0}^{\infty} M^k = (I-M)^{-1}$. Taking $s = \frac{5}{4}$ and $w = 210$, we compute that M is a 48×48 matrix all whose eigenvalues lie inside the unit cirle. The largest column sum of $(I-M)^{-1}$ is ≤ 7.37, so $C(\frac{1}{4}) = 7.37$ is admissible.

Lemma 9. *For* $0 < \varepsilon \le 1$ *and* $y \ge 10^{10}$, *we have*

$$\#\{q \le x : f(q) \ge y\} \le \frac{c(\varepsilon)x^{1+\varepsilon}}{y^{1/2+\varepsilon}\log y},$$

where

$$c(\varepsilon) = C(\varepsilon)(2^{-1-\varepsilon} - 6^{-1-\varepsilon})\zeta(1+\varepsilon)\left(0.44 + \frac{2.43}{1+2\varepsilon}\right).$$

Proof. For a prime power $s^b \ge y$ with $b \ge 2$, let q be a prime with $f(q) = s^b$. Then there is a prime $r \equiv 1 \pmod{s^b}$ and a prime chain with $p_1 = r$ and $p_k = q$. Write $r = ks^b + 1$. By Lemma 8, the number of such $q \le x$ is at most

$$\sum_{\substack{r \le x \\ r \equiv 1 \pmod{s^b}}} C(\varepsilon)\left(\frac{x}{r}\right)^{1+\varepsilon} \le C(\varepsilon)\left(\frac{x}{s^b}\right)^{1+\varepsilon} \sum_{\substack{k \ge 1 \\ ks^b+1 \text{ prime}}} k^{-1-\varepsilon}.$$

If $s > 3$, we note that k is even and among any three consecutive even values of k, r is prime for at most two of them. For such s, the sum on k is at most $(2^{-1-\varepsilon} - 6^{-1-\varepsilon})\zeta(1+\varepsilon)$. For $s \in \{2, 3\}$, we bound the sum on k trivially as $\zeta(1+\varepsilon)$. The number of $q \le x$ is therefore at most

$$C(\varepsilon)x^{1+\varepsilon}\zeta(1+\varepsilon)\left[\sum_{2^b \ge y} \frac{1}{(2^b)^{1+\varepsilon}} + \sum_{3^b \ge y} \frac{1}{(3^b)^{1+\varepsilon}} + (2^{-1-\varepsilon} - 6^{-1-\varepsilon})\sum_{s^b \ge y} \frac{1}{(s^b)^{1+\varepsilon}}\right]. \tag{5}$$

The first two sums in (5) total $\le \frac{7}{2}y^{-1-\varepsilon}$. To estimate the third sum, let $S(t)$ denote the number of proper prime powers $\le t$. By Theorem 1 and Corollay 1 of [7], we have

$$\frac{x}{\log x} \le \pi(x) \le \frac{x}{\log x}\left(1 + \frac{3}{2\log x}\right) \qquad (x \ge 17).$$

If $t \ge 10^{10}$, then $S(t) > \pi(t^{1/2}) \ge \frac{2t^{1/2}}{\log t}$ and

$$\begin{aligned} S(t) = \sum_{k \ge 2} \pi(t^{1/k}) &\le \sum_{k=2}^{7} \pi(t^{1/k}) + \left(\frac{\log t}{\log 2} - 7\right)\pi(t^{1/8}) \\ &\le \sum_{k=2}^{7} \frac{kt^{1/k}}{\log t}\left(1 + \frac{3k}{2\log t}\right) + \left(\frac{\log t}{\log 2} - 7\right)\frac{8t^{1/8}}{\log t}\left(1 + \frac{12}{\log t}\right) \\ &\le 2.43\frac{t^{1/2}}{\log t}. \end{aligned}$$

By partial summation,

$$\sum_{s^b \geq y} \frac{1}{(s^b)^{1+\varepsilon}} = -\frac{S(y^-)}{y^{1+\varepsilon}} + (1+\varepsilon)\int_y^\infty \frac{S(t)}{t^{2+\varepsilon}}\,dt$$

$$\leq -\frac{2}{y^{1/2+\varepsilon}\log y} + \frac{2.43(1+\varepsilon)}{\log y}\int_y^\infty \frac{dt}{t^{3/2+\varepsilon}} \tag{6}$$

$$= \frac{0.43 + \frac{2.43}{1+2\varepsilon}}{y^{1/2+\varepsilon}\log y}.$$

Combined with (5), this completes the proof. □

Lemma 10. *Let p be a prime and $p^{a+1} \geq 10^{10}$. Then*

$$\#\{q \leq x : p^a \| (q-1), f(q) \geq p^{a+1}\} \leq \frac{x}{p^{\frac{3a+1}{2}}\log(p^{a+1})}\left[2.86 + c(\varepsilon)(1+1/\varepsilon)\frac{x^\varepsilon}{p^{(2a+1)\varepsilon}}\right].$$

Proof. If $p^a \| (q-1)$ and $f(q) \geq p^{a+1}$, then either $p^a s^b | (q-1)$ for some proper prime power s^b with $s \neq p$ and $s^b \geq p^{a+1}$, or there is a prime $r | (q-1)$ with $f(r) \geq p^{a+1}$. The number of such $q \leq x$ is, using Lemma 9, (6) and partial summation,

$$\leq \sum_{s^b \geq p^{a+1}} \frac{x}{p^a s^b} + \sum_{\substack{r \leq x/p^a \\ f(r) \geq p^{a+1}}} \frac{x}{p^a r}$$

$$\leq \frac{2.86x}{p^{(3a+1)/2}\log(p^{a+1})} + c(\varepsilon)\frac{x}{p^{a+(1/2+\varepsilon)(a+1)}\log(p^{a+1})}\left[\left(\frac{x}{p^a}\right)^\varepsilon + \int_{p^{a+1}}^{x/p^a} u^{-1+\varepsilon}\,du\right].$$

This completes the proof of the lemma. □

Proof of Theorem 6. Let $p^a \geq \max(10^{10}, K_1)$, $x = p^{aK_2}$ and $\varepsilon = \frac{1}{2K_2}$. By Lemmas 7 and 10,

$$\begin{aligned}\#\{q \leq x : p^a \| (q-1), f(q) < p^{a+1}\} &= \pi(x; p^a, 1) - \pi(x; p^{a+1}, 1) \\ &\quad - \#\{q \leq x : p^a \| (q-1), f(q) \geq p^{a+1}\} \\ &\geq K_3 \frac{x/\log x}{p^{a+1/2}\log p} - c'(\varepsilon)\frac{x}{p^{\frac{3a+1}{2}}\log(p^{a+1})}p^{(K_2-2)a\varepsilon} \\ &> 0\end{aligned}$$

if p^a is large enough, where $c'(\varepsilon)$ is a constant depending only on ε. □

3. Proof of Theorem 5

We first take care of small p^a. If $a = 1$ and $p \le 18000000$ (1151367 primes) and when $a \ge 2$ and $p^a \le 10^{10}$ (10084 prime powers), we find a prime q with $p^a \| (q-1)$ and $q < p^{2a+1}$. By (1), $f(q) < p^{a+1}$ for such q. The calculations were performed using PARI/GP.

Next, suppose $a = 1$, $p > 18000000$ and put $x = p^3$. By (2),

$$\begin{aligned}\pi(x;p,1) - \pi(x;p^2,1) &\ge \frac{\mathrm{li}(x)}{p-1} - \sqrt{x}\log(xp^2) - \frac{x}{p^2} \\ &\ge \frac{p^2}{\log p}\left[\frac{1}{3} - 5\frac{\log^2 p}{p^{1/2}} - \frac{\log p}{p}\right] > 0,\end{aligned}$$

as desired.

Lastly, suppose $a \ge 2$ and $p^a > 10^{10}$, and put $x = p^{3a}$. By (2),

$$\begin{aligned}\pi(x;p^a,1) - \pi(x;p^{a+1},1) &\ge \frac{\mathrm{li}(x)}{p^a} - \sqrt{x}\log(x^2p^{4a+2}) \\ &\ge \frac{p^{2a}}{\log(p^a)}\left[\frac{1}{3} - 11\frac{\log^2(p^a)}{p^{a/2}}\right] \qquad (7) \\ &\ge 0.275\frac{p^{2a}}{\log(p^a)}.\end{aligned}$$

Since we may take $C(\frac{1}{4}) = 7.37$ in Lemma 8, we have $c(\frac{1}{4}) \le 22$ for Lemma 9. By Lemma 10 and (7),

$$\begin{aligned}\#\{q \le x : p^a \| (q-1), f(q) < p^{a+1}\} &\ge 0.275\frac{p^{2a}}{\log(p^a)} - \frac{p^{\frac{3a-1}{2}}}{\log(p^{a+1})}\left[2.86 + 110p^{\frac{a-1}{4}}\right] \\ &\ge \frac{p^{2a}}{\log(p^a)}\left[0.275 - \frac{2.03}{p^{a/2}} - \frac{66}{p^{a/4}}\right] \\ &> 0,\end{aligned}$$

as desired.

Acknowledgements. We thank the referee for useful suggestions. This work started during a visit of the second author at the Mathematics Department of the University of Illinois in Urbana-Champaign in January of 2007. He thanks the people of that department for their hospitality. Research of the first author supported by National Science Foundation grants DMS-0555367 and DMS-0901339. Research of the second author was supported in part by Grants SEP-CONACyT 79685 and PAPIIT 100508.

References

[1] W. D. Banks, J. Friedlander, F. Luca, F. Pappalardi and I. E. Shparlinski, *Coincidences in the values of the Euler and Carmichael functions*, Acta Arith. **122** (2006), 207–234.

[2] H. Davenport, *Multiplicative number theory*, 3rd ed., Graduate Texts in Mathematics vol. 74, Springer-Verlag, New York, 2000.

[3] K. Ford, S. Konyagin and F. Luca, *Prime chains and Pratt trees*, preprint (2009).

[4] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[5] J. Oesterlé, *Versions effective du théorème de Chebotarev sous l'hypothése de Riemann généralisée*, Astérisque **61** (1979), 165–167. [French].

[6] V. Pratt, *Every prime has a succinct certificate*, SIAM J. Comput. **4** (1975), no. 3, 214–220.

[7] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **1962**, 64–94.