International Mathematics Research Notices, 2024, **2024**(16), 11865–11877
https://doi.org/10.1093/imrn/rnae149
Advance access publication date 3 July 2024
Article

On a Goldbach-Type Problem for the Liouville Function

Alexander P. Mangerel*

Department of Mathematical Sciences, Durham University, Stockton Road, Durham, DH1 3LE, UK
*Correspondence to be sent to: e-mail: smangerel@gmail.com
Communicated by Prof. Sound Soundararajan

Let λ denote the Liouville function. We show that for all $N \geq 11$, the (non-trivial) convolution sum bound

$$\left|\sum_{n<N} \lambda(n)\lambda(N-n)\right| < N-1$$

holds. We also determine all N for which no cancellation in the convolution sum occurs. This answers a question posed at the 2018 AIM workshop on Sarnak's conjecture.

1 Introduction

1.1 Main result

The following problem was posed at the 2018 AIM workshop on Sarnak's conjecture.

Problem 1.1. ((Problem 5.1 of [5]).) Prove that for every sufficiently large N the sum

$$\mathcal{L}_\lambda(N) := \sum_{1\leq n<N} \lambda(n)\lambda(N-n)$$

satisfies $|\mathcal{L}_\lambda(N)| < N-1$. (Actually, no range for N was given in the problem, and it is our presumption that the bound was meant to be shown for large enough N.)

Obviously, the triangle inequality furnishes the trivial bound $|\mathcal{L}_\lambda(N)| \leq N-1$. Thus, the problem is to show *any savings* over this bound. This should be interpreted as an analogue of the binary Goldbach problem for the Liouville function. Indeed, if $N \geq 4$ is even and λ is replaced by the prime-supported von Mangoldt function $\Lambda_1(n) := (\log n)1_{n \text{ prime}}$, then proving the existence of primes p, q with $p+q=N$ is equivalent to

$$\mathcal{L}_{\Lambda_1}(N) := \sum_{n<N} \Lambda_1(n)\Lambda_1(N-n) > 0,$$

Received: April 23, 2024. **Revised:** May 22, 2024. **Accepted:** June 11, 2024

that is, showing any improvement over the trivial lower bound $\mathcal{L}_{\Lambda_1}(N) \geq 0$. Problem 1.1 is far weaker than what we expect to be true regarding the convolution sum $\mathcal{L}_\lambda(N)$. It is natural to compare the problem at hand with what ought to follow from Chowla's conjecture [1], namely that for all (fixed) $h \geq 1$,

$$\frac{1}{x}\left|\sum_{n\leq x} \lambda(n)\lambda(n+h)\right| = o(1) \text{ as } x \to \infty.$$

On the heuristic basis that the additively coupled values $\lambda(n)$ and $\lambda(N-n)$ ought to also be "almost orthogonal" on average, Corrádi and Kátai [3] have conjectured that $|\mathcal{L}_\lambda(N)| = o(N)$ as $N \to \infty$. As far as we are aware, the only result in this direction is a theorem of De Koninck, Germán and Kátai [4], who proved the conjecture of Corrádi and Kátai under the assumption that there are infinitely many Siegel zeroes. Nevertheless, because N is a large shift, recent methods that have proven effective in bounding binary correlations of multiplicative functions seem unsuited to the estimation of the convolution sum $\mathcal{L}_\lambda(N)$, and thus the problem at hand remains non-trivial unconditionally. Our main theorem, whose proof is completely elementary, solves Problem 1.1.

Theorem 1.2. If $N \geq 11$ then $|\mathcal{L}_\lambda(N)| < N-1$. Moreover, $|\mathcal{L}_\lambda(N)| = N-1$ if and only if $N \in \{2, 3, 5, 10\}$.

Remark 1. In a previous version of this paper we proved that $|\mathcal{L}_\lambda(N)| < N-1$ whenever $N \geq N_0$, for some *ineffective* constant N_0. We are most grateful to both Bryce Kerr and to the anonymous referee for independently pointing out how to render our result effective, which had the additional byproduct of shortening the paper.

1.2 Proof strategy

We briefly explain our strategy as follows. As we show below (see Lemma 2.1), in order to prove Theorem 1.2 we may restrict to the case in which $N = p^k$ is a prime power, and it is instructive to first consider the case $k = 1$. In this case, it is readily observed that if $|\mathcal{L}_\lambda(p)| = p-1$ in contradiction to the claim, then $\lambda(m)\lambda(p-m)$ is constant over all $1 \leq m < p$, in fact

$$\lambda(m)\lambda(p-m) = \lambda(p-1)\lambda(1) = \lambda(p-1).$$

But note that if $\chi_p = \left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol modulo p then the same is true of χ_p:

$$\chi_p(m)\chi_p(p-m) = \chi_p(-1)\chi_p(m)^2 = \chi_p(p-1).$$

Inspired by this comparison, we seek to show that $\lambda(m) = \chi_p(m)$ in the fundamental domain $[1, p-1]$ for χ_p. Using harmonic analysis over $\mathbb{Z}/p\mathbb{Z}$, the problem reduces to understanding the Fourier coefficients of $n \mapsto \lambda(n)1_{[1,p-1]}(n)$, that is, exponential sums

$$S_\lambda(\xi) := \sum_{1\leq n<p} \lambda(n)e(n\xi/p), \quad \xi \pmod p,$$

where as usual $e(t) = e^{2\pi i t}$ for $t \in \mathbb{R}$. The corresponding sums with λ replaced by χ_p are the twisted Gauss sums

$$\tau(\chi_p, \xi) := \sum_{1\leq n\leq p} \chi_p(n)e\left(\frac{n\xi}{p}\right) = \chi_p(\xi)\tau(\chi_p, 1), \quad \xi \pmod p.$$

In particular, we have the *dilation property* that for each $1 \leq d < p$,

$$\tau(\chi_p, d\xi) = \chi_p(d)\tau(\chi_p, \xi) \text{ for all } \xi \pmod p.$$

We prove below (see Proposition 2.4) that whenever $|\mathcal{L}_\lambda(p)| = p-1$ a similar dilation property holds for S_λ, that is, for each $1 \le d < p$,

$$S_\lambda(d\xi) = \lambda(d)S_\lambda(\xi) \text{ for all } \xi \pmod{p}. \tag{1}$$

The upshot of this is that when d is a primitive root modulo p we may determine all of the sums $S_\lambda(\xi)$, $\xi \neq 0$, which coincide precisely with the twisted Gauss sums given above. In this way, verifying (1) allows us to determine that $\lambda(n) = \chi_p(n)$ for all $1 \le n < p$. It turns out that, under the assumption $|\mathcal{L}_\lambda(p)| = p-1$, proving the dilation property (1) is equivalent to proving that

$$\lambda(m)\lambda(m+jp) = +1 \text{ whenever } 1 \le m < p,\ 0 \le j < d \text{ and } m \equiv -jp \pmod{d}.$$

We prove that this property holds for all pairs of (m, j) in question using an iterative argument (see Section 3). The rough idea of that argument is to

$$\text{replace } \lambda(m)\lambda(m+jp) \text{ by a prescribed sign multiplied by } \lambda(m')\lambda(m'+j'p),$$

in which $m' \equiv -j'p \pmod{d}$ and $0 \le j' < j$; crucially, the parameter j has been decremented. Iterating this procedure must eventually result in $j' = 0$, in which case the product on the right-hand side is simply $+1$. We are then able to calculate the original product $\lambda(m)\lambda(m+jp)$ to be $+1$ as well. Our argument may be seen as extending the "periodic" behaviour imposed on λ by the relation $\lambda(m)\lambda(p-m) = \lambda(p-1)$ for all $m \in \{1, \dots, p-1\}$, to the larger domain $[1, dp-1]$. Having showed that $\lambda(n) = \chi_p(n)$ for all $n < p$, we return to the general prime power case $N = p^k$, and deduce upper bounds both for p and for k. First, an elementary result of Chowla, Cowles, and Cowles [2] implies that if $p > 5$ then there is a prime $q < p$ that is a quadratic residue modulo p. As a consequence of this and the above, $|\mathcal{L}_\lambda(p)| < p-1$ for all $p > 5$, and thus any N with $|\mathcal{L}_\lambda(N)| = N-1$ must be a product of powers of primes from the set $\{2, 3, 5\}$. Next, we check by hand that $|\mathcal{L}_\lambda(p^2)| < p^2-1$ for each of the latter three primes, from which we deduce also that $|\mathcal{L}_\lambda(p^k)| < p^k-1$ for any $k \ge 2$. It follows that N must be squarefree, and hence divides 30. For the divisors of 30 not belonging to the set $\{2, 3, 5, 10\}$ it may be checked by hand that $|\mathcal{L}_\lambda(N)| < N-1$, as required.

Remark 2. One may also ask another natural Goldbach-type problem regarding the Liouville function: given an even integer $N \ge 4$, must there exist $1 \le a, b \le N$ with $a + b = N$, such that $\lambda(a) = \lambda(b) = -1$? (We thank Mark Shusterman for pointing out this problem to us, which he asked in the the MathOverflow post https://mathoverflow.net/questions/307479/goldbachs-conjecture-for-the-liouville-function.) This is obviously implied by the binary Goldbach conjecture, and therefore a weakening of it. The methods of this paper appear to be far too rigid to address this problem directly. Note, however, that even a result of the form

$$\left|\sum_{n<N} \lambda(n)\lambda(N-n)\right| < N - g(N), \tag{2}$$

where $g : \mathbb{R} \to \mathbb{R}$ is a (sufficiently quickly) increasing function satisfying $g(x) = o(x)$, would suffice to prove the existence of such a pair (a, b). Indeed, suppose otherwise. Then for any $1 \le n < N$, $(1-\lambda(n))(1-\lambda(N-n)) = 0$. It follows that

$$0 = \sum_{1 \le n < N} (1-\lambda(n))(1-\lambda(N-n)) = N - 1 - 2\sum_{n<N} \lambda(n) + \sum_{n<N} \lambda(n)\lambda(N-n).$$

We deduce from this and the prime number theorem that, for example,

$$\left|\sum_{n<N} \lambda(n)\lambda(N-n)\right| \ge N - 1 - 2\left|\sum_{n<N} \lambda(n)\right| \ge N - CNe^{-\sqrt{\log N}},$$

for some absolute constant $C > 0$ and all $N \geq 3$. Thus, the choice $g(x) = Cxe^{-\sqrt{\log x}}$ would suffice to this end. It is natural to ask to what extent the techniques in this paper may be perturbed in order to prove a bound like (2). We plan to return to this problem in a future paper.

2 Reduction to the Prime Power Case

Assume that $N \geq 2$ satisfies $|\mathcal{L}_\lambda(N)| \geq N-1$. By the triangle inequality, we must have $|\mathcal{L}_\lambda(N)| = N-1$. Our first lemma shows that we may restrict our attention to prime power values of N.

Lemma 2.1. Let $N \in \mathbb{N}$ and assume that there is a divisor $d|N$ such that $|\mathcal{L}_\lambda(d)| < d-1$. Then $|\mathcal{L}_\lambda(N)| < N-1$. In particular, if $|\mathcal{L}_\lambda(N)| = N-1$ then $|\mathcal{L}_\lambda(d)| = d-1$ for all $d|N$. Moreover, if $|\mathcal{L}_\lambda(N)| = N-1$ then $\mathcal{L}_\lambda(d) = \lambda(d-1)(d-1)$ and $\lambda(N-1) = \lambda(d-1)$ for all $d|N$, $d \geq 2$.

Proof. Write $N = md$. Splitting the sum over n defining $\mathcal{L}_\lambda(N)$ according to whether $m|n$ or not, the triangle inequality implies

$$\begin{aligned} |\mathcal{L}_\lambda(N)| &\leq |\sum_{\substack{n<N \\ m|n}} \lambda(n)\lambda(N-n)| + |\sum_{\substack{n<N \\ m\nmid n}} \lambda(n)\lambda(N-n)| \\ &\leq |\sum_{k<d} \lambda(mk)\lambda(m(d-k))| + N - 1 - |\{1 \leq n < N : m|n\}| \\ &= |\sum_{k<d} \lambda(k)\lambda(d-k)| + N - 1 - (d-1) = |\mathcal{L}_\lambda(d)| + N - d. \end{aligned}$$

Thus, if $|\mathcal{L}_\lambda(d)| < d-1$ then $|\mathcal{L}_\lambda(N)| < d-1+N-d = N-1$, as required. For the second claim, since each summand of $\mathcal{L}_\lambda(d)$ is ± 1 and there are $d-1$ terms in its support, we have $|\mathcal{L}_\lambda(d)| = d-1$ if and only if

$$\lambda(n)\lambda(d-n) = \lambda(1)\lambda(d-1) = \lambda(d-1) \text{ for all } 1 \leq n < d.$$

It thus follows that $\mathcal{L}_\lambda(d) = \lambda(d-1)(d-1)$, as claimed. Finally, since

$$\lambda(n)\lambda(N-n) = \lambda(N-1) \text{ for all } n < N,$$

specialising to $n = km$ for $k \in \mathbb{N}$, we find

$$\lambda(N-1) = \lambda(km)\lambda(m(d-k)) = \lambda(k)\lambda(d-k) = \lambda(d-1),$$

as required. ■

In view of Lemma 2.1, we may analyse the condition $|\mathcal{L}_\lambda(N)| = N-1$ by considering the implied constraints $|\mathcal{L}_\lambda(p^j)| = p^j - 1$, whenever $p^j|N$. In the next subsection we will obtain constraints both on the size of $p|N$, as well as the multiplicity k such that $p^k||N$.

2.1 Bounds on the size and multiplicity of prime divisors of N

In the sequel, write

$$S_\lambda(\xi) := \sum_{1 \leq n < p} \lambda(n)e(n\xi/p), \quad \xi \in \mathbb{Z}/p\mathbb{Z}.$$

For the purposes of illustration let us observe that the condition $|\mathcal{L}_\lambda(p)| = p-1$ imposes rigid constraints on the exponential sums $S_\lambda(\xi)$. Indeed, we have that

$$\frac{1}{p}\sum_{\xi \pmod p} S_\lambda(\xi)^2 = \sum_{1 \leq n,m < p} \lambda(n)\lambda(m)\frac{1}{p}\sum_{\xi \pmod p} e\left(\frac{(n+m)\xi}{p}\right) = \sum_{1 \leq n < p} \lambda(n)\lambda(p-n) = \mathcal{L}_\lambda(p),$$

since $n+m \equiv 0 \pmod p$ with $1 \le n, m < p$ if and only if $n+m = p$. As noted in the proof of Lemma 2.1, if $|\mathcal{L}_\lambda(p)| = p-1$ then

$$\lambda(m)\lambda(p-m) = \lambda(p-1)\lambda(1) = \lambda(p-1) \text{ for all } 1 \le m < p. \tag{3}$$

and also $\mathcal{L}_\lambda(p) = \lambda(p-1)(p-1)$. Therefore,

$$\frac{\lambda(p-1)}{p} \sum_{\xi \pmod p} S_\lambda(\xi)^2 = p - 1 = \frac{1}{p} \sum_{\xi \pmod p} |S_\lambda(\xi)|^2.$$

To motivate our forthcoming arguments, we explicitly observe the following relations, which will imply further rigidity in the values of $S_\lambda(\xi)$.

Lemma 2.2. Let $p > 2$ be prime and let $1 \le m < p$. Suppose $|\mathcal{L}_\lambda(p)| = p-1$. Then,

(a) if m is odd then $\lambda(p+m) = \lambda(m)$;
(b) if $m \equiv p \pmod 3$ then $\lambda(2p+m) = \lambda(m)$; and
(c) if $m \equiv 2p \pmod 3$ then $\lambda(2p-m) = \lambda(p-1)\lambda(m)$.

Proof. (a) If $1 \le m < p$ is odd then $(p \pm m)/2 \in \mathbb{Z} \cap [1, p-1]$, and we have

$$p = \frac{p+m}{2} + \frac{p-m}{2}.$$

As $|\mathcal{L}_\lambda(p)| = p-1$, using (3) with m replaced by $(p-m)/2$ we get

$$\lambda(p-1) = \lambda\left(\frac{p+m}{2}\right)\lambda\left(\frac{p-m}{2}\right) = \lambda(p+m)\lambda(p-m).$$

Since also $\lambda(p-1) = \lambda(m)\lambda(p-m)$, the first claim follows. (b) The argument here is similar: if $m \equiv p \pmod 3$ then $(2p+m)/3, (p-m)/3 \in \mathbb{Z} \cap [1, p-1]$ and also

$$p = \frac{2p+m}{3} + \frac{p-m}{3},$$

whence we obtain by (3) that

$$\lambda(p-1) = \lambda\left(\frac{2p+m}{3}\right)\lambda\left(\frac{p-m}{3}\right) = \lambda(2p+m)\lambda(p-m) = \lambda(p-1)\lambda(2p+m)\lambda(m),$$

from which the claim follows. (c) Suppose $m \equiv 2p \pmod 3$. Again, the above idea yields

$$\lambda(p-1) = \lambda\left(\frac{2p-m}{3}\right)\lambda\left(\frac{p+m}{3}\right) = \lambda(2p-m)\lambda(p+m).$$

If m is odd then $\lambda(p+m) = \lambda(m)$ by (a), and the claim follows immediately. Otherwise, if m is even then note that since $p > 2$, $p - m$ is odd and hence (a) again yields

$$\lambda(2p-m) = \lambda(p+(p-m)) = \lambda(p-m) = \lambda(p-1)\lambda(m).$$

Thus, claim (c) follows in this case as well. ■

The three relations given in Lemma 2.2 allows us to deduce the following.

Lemma 2.3. Let $p > 3$ and assume that $|\mathcal{L}_\lambda(p)| = p-1$. Then,

$$S_\lambda(3\xi) = S_\lambda(2\xi) = -S_\lambda(\xi) \text{ for all } \xi \pmod p. \tag{4}$$

In particular, for any $j, k \geq 0$ we have

$$S_\lambda(3^j) = (-1)^j S_\lambda(1), \quad S_\lambda(2^k) = (-1)^k S_\lambda(1).$$

Proof. The second claim follows by induction on j and k from the former, so it suffices to prove (4). First, note that as $p > 3$ the maps $\xi \mapsto 2\xi$ and $\xi \mapsto 3\xi$ are both bijections on $\mathbb{Z}/p\mathbb{Z}$. By Plancherel's theorem,

$$\frac{1}{p}\sum_{\xi \pmod p} |S_\lambda(m\xi)|^2 = \frac{1}{p}\sum_{\xi' \pmod p} |S_\lambda(\xi')|^2 = p-1 \text{ for all } m \in \{1,2,3\}. \tag{5}$$

Next, note that

$$\frac{1}{p}\sum_{\xi \pmod p} S_\lambda(2\xi)\overline{S}_\lambda(\xi) = \sum_{m,n<p} \lambda(n)\lambda(m)\frac{1}{p}\sum_{\xi \pmod p} e\left(\xi\frac{2n-m}{p}\right) = \sum_{\substack{m,n<p \\ 2n\equiv m \pmod p}} \lambda(m)\lambda(n).$$

Among $m, n < p$ with $2n \equiv m \pmod p$ we have that either $2n = m$ precisely when m is even, or else $2n = m+p$ precisely when m is odd. If $2n = m$ then

$$\lambda(n)\lambda(m) = \lambda(m/2)\lambda(m) = -\lambda(m)^2 = -1,$$

while if $2n = p+m$ then by Lemma 2.2(a) we have

$$\lambda(n)\lambda(m) = \lambda\left(\frac{p+m}{2}\right)\lambda(m) = -\lambda(p+m)\lambda(m) = -1.$$

It follows that

$$\begin{aligned}\frac{1}{p}\sum_{\xi \pmod p} S_\lambda(2\xi)\overline{S}_\lambda(\xi) &= \sum_{\substack{m<p \\ m \text{ even}}} \lambda(m)\lambda(m/2) + \sum_{\substack{m<p \\ m \text{ odd}}} \lambda(m)\lambda\left(\frac{p+m}{2}\right) \\ &= -\left(\sum_{\substack{m<p \\ m \text{ even}}} 1 + \sum_{\substack{m<p \\ m \text{ odd}}} 1\right) = -(p-1).\end{aligned}$$

This latter sum being real-valued, it follows from this and (5) that

$$\begin{aligned}\frac{1}{p}\sum_{\xi \pmod p} |S_\lambda(2\xi) + S_\lambda(\xi)|^2 &= \frac{1}{p}\sum_{\xi \pmod p} \left(|S_\lambda(\xi)|^2 + |S_\lambda(2\xi)|^2 + 2\mathrm{Re}(S_\lambda(2\xi)\overline{S}_\lambda(\xi))\right) \\ &= 2(p-1) - 2(p-1) = 0.\end{aligned}$$

Therefore, $S_\lambda(2\xi) = -S_\lambda(\xi)$ for all $\xi \pmod p$, as claimed. The proof with 2 replaced by 3 follows similar lines, using Lemma 2.2. Here, instead we must treat pairs $1 \leq n, m < p$ with $3n \equiv m \pmod p$, or equivalently $3n = m + jp$, where $0 \leq j < 3$ and $m + jp \equiv 0 \pmod 3$ in each case. (Note that as $p > 3$, the residue classes $0, -p, -2p \pmod 3$ cover all integers $1 \le m < p$.) Precisely,

$$\frac{1}{p}\sum_{\xi \pmod p} S_\lambda(3\xi)\overline{S}_\lambda(\xi) = \sum_{m,n<p} \lambda(n)\lambda(m)\frac{1}{p}\sum_{\xi \pmod p} e\left(\xi\frac{3n-m}{p}\right) = \sum_{\substack{m,n<p \\ 3n\equiv m \pmod p}} \lambda(m)\lambda(n)$$

$$= \left(\sum_{\substack{m<p \\ 3|m}} \lambda(m/3)\lambda(m) + \sum_{\substack{m<p \\ m\equiv -2p \pmod 3}} \lambda(m)\lambda\left(\frac{2p+m}{3}\right) + \sum_{\substack{m<p \\ m\equiv -p \pmod 3}} \lambda(m)\lambda\left(\frac{p+m}{3}\right)\right).$$

By (b) and (c) of Lemma 2.2,

$$\lambda(m)\lambda(m/3) = \lambda(3)\lambda(m)^2 = -1 \qquad \text{if } 3|m,$$

$$\lambda(m)\lambda\left(\frac{2p+m}{3}\right) = \lambda(3)\lambda(m)^2 = -1 \qquad \text{if } m \equiv -2p \equiv p \pmod 3,$$

$$\lambda(m)\lambda\left(\frac{p+m}{3}\right) = \lambda(m)\lambda(p-1)\lambda\left(\frac{2p-m}{3}\right) = \lambda(3)\lambda(m)^2 = -1 \qquad \text{if } m \equiv -p \equiv 2p \pmod 3.$$

We thus conclude that

$$\frac{1}{p}\sum_{\xi \pmod p} S_\lambda(3\xi)\overline{S}_\lambda(\xi) = -\left(\sum_{\substack{m<p \\ 3|m}} 1 + \sum_{\substack{m<p \\ m\equiv -2p \pmod 3}} 1 + \sum_{\substack{m<p \\ m\equiv -p \pmod 3}} 1\right) = -(p-1).$$

The claim that $S_\lambda(3\xi) = -S_\lambda(\xi)$ for all $\xi \pmod p$ now follows as it did with 2ξ. ■

It is natural, then, to speculate that 2 or 3 may be replaced by other primes as well. In fact, we will prove the following more general result in the next section.

Proposition 2.4. Let p be a prime with $|\mathcal{L}_\lambda(p)| = p-1$, and let $1 \le d < p$. Then we have

$$S_\lambda(d\xi) = \lambda(d)S_\lambda(\xi) \text{ for all } \xi \pmod p. \tag{6}$$

Proposition 2.4 will be beneficial in light of the following result.

Lemma 2.5. Let $p > 2$ be a prime satisfying $|\mathcal{L}_\lambda(p)| = p-1$. Suppose $2 \le d < p$ is a primitive root modulo p such that (6) holds. Then $\lambda(n) = \chi_p(n)$ for all $n < p$.

Proof. As d is a primitive root, every $\xi \not\equiv 0 \pmod p$ can be written as $\xi \equiv d^k \pmod p$ for some $1 \le k \le p-1$, and thus $S_\lambda(\xi) = S_\lambda(d^k)$. By (6) and induction, it follows that $S_\lambda(d^k) = \lambda(d)^k S_\lambda(1)$ for all $k \ge 1$. In particular, $|S_\lambda(\xi)| = |S_\lambda(1)|$ for all $\xi \not\equiv 0 \pmod p$. On the basis of these observations, we first verify that $\lambda(d) = -1$. Since p is odd,

$$0 = \sum_{\xi \pmod p} S_\lambda(\xi) = S_\lambda(0) + \sum_{k=1}^{p-1} S_\lambda(d^k) = S_\lambda(0) + S_\lambda(1)\sum_{k=1}^{p-1}\lambda(d)^k$$

$$= S_\lambda(0) + (p-1)S_\lambda(1)1_{\lambda(d)=+1}. \tag{7}$$

Now supposing $\lambda(d) = +1$ then we have $S_\lambda(0) = -(p-1)S_\lambda(1)$. On the other hand, since $|S_\lambda(\xi)| = |S_\lambda(1)|$ for all $\xi \not\equiv 0 \pmod p$, we find using (5) that

$$p(p-1) = \sum_{\xi \pmod p} |S_\lambda(\xi)|^2 = |S_\lambda(0)|^2 + |S_\lambda(1)|^2(p-1) = |S_\lambda(1)|^2((p-1)^2 + p - 1) = |S_\lambda(1)|^2 p(p-1).$$

We deduce that $|S_\lambda(1)| = 1$, and thus $|S_\lambda(0)| = p-1$. But if $p = 3$ we have $|S_\lambda(0)| = 0 \neq 2$ since $\lambda(1) = -\lambda(2)$, and for $p > 3$ we have

$$|S_\lambda(0)| = \left|\sum_{1\le n<p} \lambda(n)\right| = \left|\sum_{3\le n<p} \lambda(n)\right| \le p-3 < p-1,$$

a contradiction. Thus, we conclude that $\lambda(d) = -1$, and it follows further from (7) that $S_\lambda(0) = 0$. Next, as d is a primitive root and χ_p is a non-principal character, $\chi_p(d) = -1$. Hence,

$$S_\lambda(d^k) = \lambda(d)^k S_\lambda(1) = (-1)^k S_\lambda(1) = \chi_p(d)^k S_\lambda(1) \text{ for all } k.$$

Now for each $n < p$, we have using $S_\lambda(0) = 0$ that

$$\lambda(n) = \sum_{m<p} \lambda(m) 1_{m\equiv n \pmod p} = \frac{1}{p}\sum_{\xi \pmod p} e\left(-\frac{n\xi}{p}\right)\sum_{m<p}\lambda(m)e\left(\frac{m\xi}{p}\right) = \frac{1}{p}\sum_{\substack{\xi \pmod p\\ \xi\not\equiv 0 \pmod p}} S_\lambda(\xi)e\left(-\frac{n\xi}{p}\right).$$

Reparametrising $\xi \in (\mathbb{Z}/p\mathbb{Z})^\times$ as $d^k \pmod p$ for $1 \le k \le p-1$, we get

$$\lambda(n) = \frac{1}{p}\sum_{k=1}^{p-1} S_\lambda(d^k)e\left(-\frac{nd^k}{p}\right) = \frac{S_\lambda(1)}{p}\sum_{k=1}^{p-1}\chi_p(d)^k e\left(-\frac{nd^k}{p}\right) = \frac{S_\lambda(1)}{p}\sum_{\xi \pmod p}\chi_p(\xi)e\left(-\frac{n\xi}{p}\right).$$

Using standard relations for Gauss sums, we readily find that for any $n < p$,

$$\lambda(n) = \chi_p(n)\cdot\frac{S_\lambda(1)\overline{\tau(\chi_p)}}{p},$$

where, as usual,

$$\tau(\chi_p) := \sum_{a \pmod p}\chi_p(a)e\left(\frac{a}{p}\right).$$

If we set $n = 1$ then we plainly have $S_\lambda(1)\overline{\tau(\chi_p)} = p$, and the claim follows. ■

There are clearly two ways in which Lemma 2.5 may be used. One is to derive information about the Liouville function using corresponding behaviour of Dirichlet characters; this appears hard to do since we only know that λ and χ_p are comparable within the fundamental domain $[1, p-1]$. The other way is to obtain constraints on the behaviour of Dirichlet characters from the rigidity of the Liouville function, in particular at primes. In this direction we deduce the following from a result of Chowla, Cowles, and Cowles [2].

Proposition 2.6. If $|\mathcal{L}_\lambda(N)| = N-1$ then $N|30$.

Proof. By Lemma 2.1, we deduce that $|\mathcal{L}_\lambda(p)| = p-1$ for each prime $p|N$. For each such $p > 2$ let $2 \le d_p < p$ be a primitive root modulo p. By Proposition 2.4, d_p satisfies (6) for all $\xi \pmod p$, and thus Lemma 2.5 implies that $\lambda(n) = \chi_p(n)$ for all $n < p$. In particular, for each prime $q < p$ we have $\chi_p(q) = -1$. Now suppose $p > 5$. If $p \equiv \pm 1 \pmod 8$ then by the law of quadratic reciprocity we have

$$\chi_p(2) = (-1)^{\frac{p^2-1}{8}} = +1,$$

which is a contradiction. On the other hand, if $p \equiv \pm 3 \pmod 8$ then from the elementary results of [2] there is a prime $q \le (p+1)/4 < p$ such that $\chi_p(q) = +1$, again a contradiction. It follows that $p \in \{2, 3, 5\}$, and thus $N = 2^a 3^b 5^c$, for some non-negative integers a, b, c, not all zero. It remains to show that $0 \le a, b, c \le 1$, from which the claim $N|30$ follows. Appealing once again to Lemma 2.1, it is sufficient to show that $|\mathcal{L}_\lambda(p^2)| < p^2 - 1$ for each of $p \in \{2,3,5\}$. In order to do this it suffices to find, in each case, distinct pairs (a_1, b_1) and (a_2, b_2) of positive integers with $a_1 + b_1 = a_2 + b_2 = p^2$, yet $\lambda(a_1)\lambda(b_1) = -\lambda(a_2)\lambda(b_2)$. For $p = 2$ we have $1+3 = 2+2 = 4$, and

$$\lambda(1)\lambda(3) = -1, \quad \lambda(2)^2 = +1.$$

For $p = 3$ we have $1+8 = 2+7 = 9$, and

$$\lambda(1)\lambda(8) = -1, \quad \lambda(2)\lambda(7) = +1.$$

For $p = 5$ we have $2+23 = 3+22 = 25$, and

$$\lambda(2)\lambda(23) = +1, \quad \lambda(3)\lambda(22) = -1.$$

The claim therefore follows. ■

Proof of Theorem 1.2. By Proposition 2.6, we know that if $|\mathcal{L}_\lambda(N)| = N-1$ then $N|30$. It can be checked by hand that $|\mathcal{L}_\lambda(N)| = N-1$ for each $N \in \{2,3,5,10\}$. For instance, we have

$$\mathcal{L}_\lambda(10) = 2(\lambda(1)\lambda(9) + \lambda(2)\lambda(8) + \lambda(3)\lambda(7) + \lambda(4)\lambda(6)) + \lambda(5)^2 = 2\cdot 4 + 1 = 9.$$

It therefore remains to verify that $|\mathcal{L}_\lambda(N)| < N-1$ for each of $N \in \{6,15,30\}$. Similarly to the proof of Proposition 2.6, we do this by finding distinct pairs (a_1, b_1), (a_2, b_2) of positive integers with $a_1 + b_1 = a_2 + b_2 = N$, yet $\lambda(a_1)\lambda(b_1) = -\lambda(a_2)\lambda(b_2)$. For $N = 6$ we have $1+5 = 3+3 = 6$, and

$$\lambda(1)\lambda(5) = -1, \quad \lambda(3)^2 = +1.$$

For $N = 15$ we have $2+13 = 4+11 = 15$, and

$$\lambda(2)\lambda(13) = +1, \quad \lambda(4)\lambda(11) = -1.$$

For $N = 30$ we have $1+29 = 2+28 = 30$, and

$$\lambda(1)\lambda(29) = -1, \quad \lambda(2)\lambda(28) = +1.$$

The proof is now complete. ■

3 Proof of Proposition 2.4

In this section we prove Proposition 2.4. As we show later, it suffices to consider the case when d is prime. Having shown the cases $d = 2$ and 3 in Lemma 2.3, we focus here on $d > 3$.

3.1 An iterative argument for $d = q$ prime

As previously, let $p > 3$ be a prime with $|\mathcal{L}_\lambda(p)| = p-1$. Let $3 < q < p$ be an odd prime. We wish to show that

$$S_\lambda(q\xi) = -S_\lambda(\xi) \text{ for all } \xi \pmod p.$$

As in the proof of Lemma 2.3, it suffices to show that

$$-(p-1) = \frac{1}{p}\sum_{\xi \pmod p} S_\lambda(q\xi)\overline{S}_\lambda(\xi) = \sum_{m,n<p} \lambda(m)\lambda(n)\frac{1}{p}\sum_{\xi \pmod p} e\left(\xi\frac{qn-m}{p}\right)$$
$$= \sum_{\substack{m,n<p \\ qn\equiv m \pmod p}} \lambda(m)\lambda(n).$$

As before, we split the set of $1 \le m, n < p$ according to the choice of $0 \le j < q$ for which $qn = m + jp$; in each case we have $m \equiv -jp \pmod q$, and thus we must show that

$$-(p-1) = \sum_{j=0}^{q-1} \sum_{\substack{m<p \\ m \equiv -jp \pmod q}} \lambda(m)\lambda\left(\frac{m+jp}{q}\right) = -\sum_{j=0}^{q-1} \sum_{\substack{m<p \\ m \equiv -jp \pmod q}} \lambda(m)\lambda\left(m+jp\right).$$

Equivalently, it is our goal to prove that for every $0 \le j < q$ and $1 \le m < p$ we have

$$\lambda(m)\lambda(m+jp) = +1 \text{ whenever } m \equiv -jp \pmod q. \tag{8}$$

For $1 \le r \le q-1$ we define the sets

$$\mathcal{A}_{q,r} := \{(m,j) \in \{1,\ldots,p-1\} \times \{0,\ldots,q-1\} : \frac{pq}{r+1} < m + jp < \frac{pq}{r}\}, \quad \mathcal{A}_{q,q} := \{(m,0) : 1 \le m < p\}.$$

Note that the sets $\{\mathcal{A}_{q,r}\}_{1 \le r \le q}$ partition the set of all pairs $(m,j) \in \{1,\ldots,p-1\} \times \{0,\ldots,q-1\}$, in view of the following observations:

(a) for each such pair, $1 \le m + jp < pq$, and therefore must either satisfy $1 \le m + jp < p$ (so $j = 0$), or else $pq/(r+1) \le m + jp < pq/r$ for some $1 \le r \le q-1$;
(b) as p and q are prime we can never have $m + jp = pq/(r+1)$ for any $1 \le r \le q-1$ unless $r = q-1$, but in this case $m + jp = p$ is not solvable with $1 \le m < p-1$; and
(c) if $(m,j) \notin \mathcal{A}_{q,r}$ for all $1 \le r \le q-1$ then $1 \le m + jp < p$, equivalently, $j = 0$ and $(m,0) \in \mathcal{A}_{q,q}$.

For each $1 \le r \le q-1$ define a map ψ_r on pairs $(m,j) \in \mathcal{A}_{q,r}$ via

$$\psi_r(m,j) := \left(\left\lceil \frac{rm}{p} \right\rceil p - rm, q - jr - \left\lceil \frac{rm}{p} \right\rceil\right),$$

where, as usual, given $t \in \mathbb{R}$ we denote by $\lceil t \rceil$ the least integer $k \ge t$.

Lemma 3.1. Let $(m,j) \in \mathcal{A}_{q,r}$ for some $1 \le r \le q-1$, and set $(m',j') := \psi_r(m,j)$. The following properties hold:

(a) $m' + j'p \equiv 0 \pmod q$ whenever $m + jp \equiv 0 \pmod q$;
(b) $m' = \{-rm/p\}p = p\left(1 - \{rm/p\}\right)$;
(c) $(m',j') \in \bigcup_{r+1 \le s \le q} \mathcal{A}_{q,s}$; and
(d) if $m + jp \equiv 0 \pmod q$ then $\lambda(m+jp) = \lambda(r)\lambda(p-1)\lambda(m'+j'p)$.

In fact, (d) may be rewritten as

$$\lambda(m)\lambda(m+jp) = \left[\lambda(rm)\lambda\left(p\left\{\frac{rm}{p}\right\}\right)\right]\lambda(m')\lambda(m'+j'p). \tag{9}$$

Proof. (a) We observe that

$$m' + j'p = \left(\left\lceil \frac{rm}{p} \right\rceil p - rm\right) + \left(q - jr - \left\lceil \frac{rm}{p} \right\rceil\right)p = p(q-jr) - rm = pq - r(m+jp), \tag{10}$$

so that if $m + jp \equiv 0 \pmod q$ then $m' + j'p \equiv 0 \pmod q$ as well. (b) Note that since $r, m < p$, $rm/p \notin \mathbb{Z}$. Whenever $\alpha \notin \mathbb{Z}$, we have

$$\lceil \alpha \rceil = \alpha + 1 - \{\alpha\} = \alpha + \{-\alpha\},$$

so we therefore conclude that

$$m' = p\left(\frac{rm}{p} + \left\{-\frac{rm}{p}\right\}\right) - rm = p\left\{-\frac{rm}{p}\right\} = p\left(1 - \left\{\frac{rm}{p}\right\}\right),$$

as required. (c) Using $pq/(r+1) < m + jp < pq/r$ together with (10), we deduce that

$$m' + j'p < pq - r\cdot\frac{pq}{r+1} = pq\left(1 - \frac{r}{r+1}\right) = \frac{pq}{r+1}$$
$$m' + j'p > pq - r\cdot\frac{pq}{r} = 0.$$

Together with (b), the latter bound implies that $1 \le m' < p$. Furthermore,

$$j' = q - \left(jr + \left\lceil\frac{rm}{p}\right\rceil\right) \ge q - 1 - \frac{r}{p}(jp+m) > q - 1 - \frac{r}{p}\cdot\frac{pq}{r} = -1,$$

so as j' is an integer with $j' > -1$, and $\lceil rm/p\rceil \ge 1$, we have $0 \le j' < q$. As $0 < m' + j'p < pq/(r+1)$, it follows that $(m', j') \in \mathcal{A}_{q,s}$ for some $r+1 \le s \le q$, as required. (d) Since $(m,j) \in \mathcal{A}_{q,r}$ and $q|(m+jp)$, we see that

$$1 \le \frac{m+jp}{q} < \frac{1}{q}\cdot\frac{pq}{r} = \frac{p}{r}.$$

It follows that $(rm + rjp)/q \in \mathbb{Z}\cap[1, p-1]$, and so using (3),

$$\begin{aligned}\lambda(m+jp) &= \lambda(qr)\lambda\left(\frac{rm+rjp}{q}\right) = \lambda(qr)\lambda(p-1)\lambda\left(p - \frac{rm+rjp}{q}\right) = \lambda(qr)\lambda(p-1)\lambda\left(\frac{(q-rj)p - rm}{q}\right)\\ &= \lambda(r)\lambda(p-1)\lambda\left(\left(\left\lceil\frac{rm}{p}\right\rceil p - rm\right) + p\left(q - rj - \left\lceil\frac{rm}{p}\right\rceil\right)\right)\\ &= \lambda(r)\lambda(p-1)\lambda(m' + j'p),\end{aligned}$$

as claimed. To prove (9), it suffices to note using (b) that

$$\lambda(m') = \lambda(p - p\{rm/p\}) = \lambda(p-1)\lambda(p\{rm/p\}),$$

after which the identity follows immediately from (d) upon multiplying both sides by $\lambda(m)$. ■

The upshot of Lemma 3.1(c) is that ψ_r maps $\mathcal{A}_{q,r}$ to a set of pairs (m', j') for which $m' + j'p$ has strictly decreased (and in particular (m', j') belongs to $\mathcal{A}_{q,r'}$ where $r' > r$). We see therefore that by iteratively composing maps ψ_r, $r < q$, we must eventually find an image pair in $\mathcal{A}_{q,q}$, that is, where the j component is 0. With this in mind, we introduce the following definition.

Definition 1. We say that the *signature* of a pair (m, j), $1 \le m < p$ and $0 \le j < q$, is the tuple $(r_1, \ldots, r_k)$ such that $1 \le r_1 < r_2 < \cdots < r_k < q$, with

$$\psi_{r_k} \circ \cdots \circ \psi_{r_1}(m, j) = (\tilde{m}, 0) \in \mathcal{A}_{q,q},$$

for some $1 \le \tilde{m} < p$. (Here, we implicitly have that the indices r_i are determined such that $(m, j) \in \mathcal{A}_{q,r_1}$, $\psi_{r_1}(m, j) \in \mathcal{A}_{q,r_2}$, $\psi_{r_2} \circ \psi_{r_1}(m, j) \in \mathcal{A}_{q,r_3}$, and so on.)

Lemma 3.2. Let (m, j) have signature $(r_1, \ldots, r_k)$. Then

$$\lambda(m)\lambda(m+jp) = \prod_{i=0}^{k-1}\lambda(m_i r_{i+1})\lambda\left(p\left\{\frac{r_{i+1}m_i}{p}\right\}\right),$$

where we have set

$$(m_0, j_0) := (m, j), \quad (m_{i+1}, j_{i+1}) := \psi_{r_{i+1}}(m_i, j_i) \text{ for } 0 \le i \le k-1.$$

Proof. By iteratively invoking (9), we obtain

$$\begin{aligned}\lambda(m)\lambda(m+jp) = \lambda(m_0)\lambda(m_0+j_0p) &= \left[\lambda(m_0r_1)\lambda\left(p\left\{\frac{r_1m_0}{p}\right\}\right)\right]\lambda(m_1)\lambda(m_1+j_1p)\\ &= \prod_{i=0}^{1}\left[\lambda(m_ir_{i+1})\lambda\left(p\left\{\frac{r_{i+1}m_i}{p}\right\}\right)\right]\lambda(m_2)\lambda(m_2+j_2p)\\ &= \cdots = \prod_{i=0}^{k-1}\left[\lambda(m_ir_{i+1})\lambda\left(p\left\{\frac{r_{i+1}m_i}{p}\right\}\right)\right]\lambda(m_k)\lambda(m_k+j_kp).\end{aligned}$$

By the definition of signature, we have $j_k = 0$, and thus $\lambda(m_k)\lambda(m_k + j_kp) = \lambda(m_k)^2 = +1$. The claim follows. ■

3.2 Periodicity via dilation

In connection with Lemma 3.1 we next show the following lemma, which shows that if S_λ satisfies the dilation property in Proposition 2.4 with $d = r < p$ then λ exhibits mod p periodicity in $[1, rp-1]$.

Lemma 3.3. Assume that $1 \le r < p$ satisfies

$$S_\lambda(r\xi) = \lambda(r)S_\lambda(\xi) \text{ for all } \xi \pmod{p}. \tag{11}$$

Then for any $1 \le m < p$, $\lambda(p\{rm/p\}) = \lambda(r)\lambda(m)$.

Proof. Note that by making the bijective change of variables $\xi \mapsto r^{-1}\xi \pmod{p}$ and rearranging, (11) yields

$$S_\lambda(r^{-1}\xi) = \lambda(r)S_\lambda(\xi) \text{ for all } \xi \pmod{p}.$$

From this, we derive that

$$\begin{aligned}0 = S_\lambda(r^{-1}\xi) - \lambda(r)S_\lambda(\xi) &= \sum_{n<p}\lambda(n)e(nr^{-1}\xi/p) - \sum_{m<p}\lambda(mr)e(m\xi/p)\\ &= \sum_{m<p} e(m\xi/p)\left(\sum_{\substack{n<p\\ n\equiv rm \pmod{p}}}\lambda(n) - \lambda(mr)\right).\end{aligned}$$

Since this holds for all $\xi \pmod{p}$ we deduce that for all $1 \le m < p$,

$$\sum_{\substack{n<p\\ n\equiv rm \pmod{p}}}\lambda(n) = \lambda(m)\lambda(r). \tag{12}$$

On the other hand, the condition $n \equiv rm \pmod{p}$ with $1 \le n < p$ is equivalent to $n = p\{rm/p\}$. Combining these two facts, we deduce that

$$\lambda(p\{rm/p\}) = \lambda(m)\lambda(r),$$

as claimed. ■

We are now in a position to prove Proposition 2.4.

Proof of Proposition 2.4. We proceed by induction on d. When $d = 1$ there is nothing to prove. Thus, assume that for every $1 \le d < q$ the equation

$$S_\lambda(d\xi) = \lambda(d)S_\lambda(\xi) \text{ holds for all } \xi \pmod p. \tag{13}$$

We thus must establish (13) for $d = q$ (provided $q < p$). First, we observe that if q is composite then writing $q = ab$ with $1 < a, b < q$ we have that for any $\xi \pmod p$,

$$S_\lambda(q\xi) = S_\lambda(a(b\xi)) = \lambda(a)S_\lambda(b\xi) = \lambda(a)\lambda(b)S_\lambda(\xi) = \lambda(q)S_\lambda(\xi),$$

as required. Hence, the claim holds whenever q is composite. Thus, we may assume that q is prime. Assuming the induction hypothesis, we see that for any $1 \le r < q$ (necessarily coprime to p) we have

$$S_\lambda(r\xi) = \lambda(r)S_\lambda(\xi) \text{ for all } \xi \pmod p.$$

By Lemma 3.3, we see that for any $1 \le m < p$,

$$\lambda\left(p\left\{rm/p\right\}\right) = \lambda(r)\lambda(m) = \lambda(rm), \tag{14}$$

a fact that we will use momentarily. As discussed above, in order to prove (13) holds with $d = q$ it suffices to show that

$$\lambda(m)\lambda(m + jp) = +1 \text{ for all } 0 \le j < q,\ 1 \le m < p \text{ with } m \equiv -jp \pmod q.$$

Now, given $1 \le m < p$ and $0 \le j < q$, let $(r_1, \ldots, r_k)$ denote the signature of (m, j), recalling that $1 \le r_1 < \cdots < r_k < q$. By Lemma 3.2, we have

$$\lambda(m)\lambda(m + jp) = \prod_{i=0}^{k-1} \lambda(m_i r_{i+1})\lambda\left(p\left\{\frac{r_{i+1}m_i}{p}\right\}\right).$$

But since $r_{i+1} < q$ for all $0 \le i \le k-1$, we know that (14) holds with each $r = r_{i+1}$. Thus, every factor in the right-hand product is simply $+1$, and hence $\lambda(m)\lambda(m + jp) = +1$, as required. Hence, (13) holds when q is prime as well. The inductive claim therefore follows in all cases, and so by induction, the proof is complete. ■

Acknowledgments

We warmly thank Bryce Kerr and the anonymous referee for (separately) indicating to us how to render effective the lower bound on N in Theorem 1.2 that we derived in a previous version of this paper. We would also like to thank Oleksiy Klurman, Brad Rodgers, and Mark Shusterman for useful comments and encouragement.

References

1. Chowla, S. *The Riemann Hypothesis and Hilbert's Tenth Problem*. New York–London–Paris: Gordon and Breach Science Publishers, 1965.
2. Chowla, S., J. Cowles, and M. Cowles. "The least prime quadratic residue and the class number." *J. Number Theory* **22**, no. 1 (1986): 1–3. https://doi.org/10.1016/0022-314X(86)90026-0.
3. Corrádi, C. A. and I. Kátai. "Some problems concerning the convolutions of number-theoretical functions." *Arch. Math.* **20** (1969): 24–9. https://doi.org/10.1007/BF01898987.
4. De Koninck, J.-M., L. Germán, and I. Kátai. "On the convolution of the Liouville function under the existence of Siegel zeros." *Lith. Math. J.* **55**, no. 3 (2015): 331–42. https://doi.org/10.1007/s10986-015-9284-x.
5. American Insitute of Mathematics. *AIM Problem List: Sarnak's Conjecture*. http://aimpl.org/sarnakconjecture/5/, 2018.