NONNEGATIVE MULTIPLICATIVE FUNCTIONS ON SIFTED SETS, AND THE SQUARE ROOTS OF -1 MODULO SHIFTED PRIMES

PAUL POLLACK

Abstract. An oft-cited result of Peter Shiu bounds the mean value of a nonnegative multiplicative function over a coprime arithmetic progression. We prove a variant where the arithmetic progression is replaced by a sifted set. As an application, we show that the normalized square roots of $-1 \pmod m$ are equidistributed (mod 1) as m runs through the shifted primes $q-1$.

1. Introduction

Many problems in elementary and analytic number theory require estimates for mean values of arithmetic functions. One of our most useful tools for obtaining estimates from above is the following theorem of Peter Shiu [15], which bounds the mean value of a nonnegative-valued multiplicative function over a coprime arithmetic progression.

Let $\mathscr{M}$ be the collection of nonnegative-valued multiplicative functions f satisfying the following two conditions:

(I) There is a constant $A_1 > 0$ such that $f(p^k) \le A_1^k$ for all prime powers p^k.
(II) For every $\epsilon > 0$, there is a constant $A_2(\epsilon) > 0$ such that

$$f(n) \le A_2(\epsilon) n^\epsilon \qquad \text{for all } n \ge 1.$$

Theorem A (Brun–Titchmarsh for multiplicative functions, [15]). *Let $f \in \mathscr{M}$, $0 < \alpha, \beta < \frac{1}{2}$, and let a, k be integers satisfying $0 \le a < k$ and $\gcd(a,k) = 1$. Then for all sufficiently large x, we have that*

$$\sum_{\substack{x-y < n \le x \\ n \equiv a \pmod k}} f(n) \ll \frac{y}{\varphi(k)} \frac{1}{\log x} \exp\left(\sum_{\substack{p \le x \\ p \nmid k}} \frac{f(p)}{p} \right), \tag{1.1}$$

whenever a, k, y satisfy

$$k < y^{1-\alpha}, \quad x^\beta < y \le x.$$

Here the implied constant in (1.1)*, as well as the threshold for "sufficiently large", depends only on α, β, the constant A_1 in* (I) *above, and the function $A_2(\epsilon)$ in* (II).

Most of the ideas necessary to prove Theorem A were already in circulation when [15] appeared (see [7], [16], [1], [4], and [17]), but Theorem A has proved more influential than many of its precursors. (MathSciNet records over 70 citations to Shiu's paper so far.) No doubt this is due to its impressive generality and the ease with which it can be "plugged in" as an auxiliary tool in number-theoretic investigations.

In this paper, we put forward a variant of Theorem A where the role of the coprime progression $a \bmod k$ is taken by a sifted set.

2010 *Mathematics Subject Classification.* 11N37 (primary), 11N36, 11J71 (secondary).

Theorem 1.1 (Brun's upper bound sieve for multiplicative functions)**.** *Let $f \in \mathscr{M}$, let $0 < \beta < \frac{1}{2}$, and let k be a nonnegative integer. For each prime $p \le x$, let $\mathscr{E}_p$ be a union of $\nu(p)$ nonzero residue classes modulo p, where we suppose that each $\nu(p) \le k$. Let*

$$\mathscr{S} = \bigcap_{p \le x} \mathscr{E}_p^{\mathsf{c}}.$$

(In words, $\mathscr{S}$ is the set of all positive integers n not belonging to any $\mathscr{E}_p$.) If x is sufficiently large, then

$$\sum_{\substack{x-y<n\le x\\ n\in\mathscr{S}}} f(n) \ll \frac{y}{\log x} \exp\left(\sum_{p\le x} \frac{f(p)-\nu(p)}{p}\right) \tag{1.2}$$

for all y satisfying

$$x^\beta < y \le x.$$

Here the implied constant in (1.2)*, as well as the threshold for "sufficiently large", depends only on β, k, the constant A_1 in* (I) *above, and the function $A_2(\epsilon)$ in* (II)*.*

Remarks.

(i) Theorem 1.1, while obviously a close relative of Theorem A, does not obviously imply it (nor vice versa).

(ii) It may initially seem strange that we require $\mathscr{E}_p$ to only contain nonzero residue classes. This does not entail any loss of generality, since we can effectively remove n not coprime to a given P by replacing the function $f(n)$ with $\mathbb{1}_{\gcd(n,P)} \cdot f(n)$.

(iii) Keeping the last remark in mind, one easily deduces from Theorem 1.1 that the number of $n \le x$ that avoid any prescribed $\nu(p) \le k$ residue classes modulo p, for each prime $p \le x$, is

$$\ll_k x \exp\left(-\sum_{p\le x} \frac{\nu(p)}{p}\right);$$

this is a familiar form of Brun's upper bound sieve.

An immediate, but interesting, application of Theorem 1.1 is an upper bound for the mean value of $f(n)$ with n restricted to shifted primes, or shifted twin primes.

Corollary 1.2. *Let f be a function belonging to $\mathscr{M}$. Let $0 < \beta < 1/2$. For all $x \ge 3$ and $y \in (x^\beta, x]$,*

$$\sum_{\substack{x-y<q\le x\\ q \text{ prime}}} f(q-1) \ll_{f,\beta} \frac{x}{\log x} \exp\left(\sum_{p\le x} \frac{f(p)-1}{p}\right),$$

and

$$\sum_{\substack{x-y<q\le x\\ q-2,\ q \text{ prime}}} f(q-1) \ll_{f,\beta} \frac{x}{(\log x)^2} \exp\left(\sum_{p\le x} \frac{f(p)-1}{p}\right),$$

The first statement of Corollary 1.2 was shown, implicitly, by Barban and Levin [3] in the special case $y = x$.[1] Their argument would also prove the second statement of the Corollary when $y = x$. However, a different method seems to be needed to get these results for short intervals.

[1] "Implicitly" means that Barban and Levin only discuss the the conjugate problem of estimating $\sum_{p<N} f(N-p)$. Their conditions on f are also slightly more restrictive than ours.

Taking $f(n) = t^{\omega(n)}$ and $y = x$ in the second statement of Corollary 1.2, we deduce that for each fixed t_0, and all $x \geq 3$,

$$\sum_{\substack{q \leq x \\ q-2,\ q \text{ prime}}} t^{\omega(q-1)} \ll_{t_0} \frac{x}{(\log x)^2} (\log x)^{t-1}.$$

One can now extract information on the distribution of $\omega(q-1)$ by varying t. For example, mimicking the proof of Theorem 010 in [8] yields: *Uniformly for* $0 \leq \psi \leq (\log\log x)^{1/6}$, *the number of prime pairs* $q-2, q$ *in* $[1,x]$ *with* $|\omega(q-1) - \log\log x| > \psi\sqrt{\log\log x}$ *is* $O(x(\log x)^{-2}\exp(-\psi^2/2))$. This last statement is a strengthened form of a theorem of Barban [2].

We now describe our original motivation for proving Theorem 1.1. The application is a riff on two theorems of Hooley.

An infamous conjecture of Landau (one of his "four unattackable problems") predicts that there are infinitely many primes of the form $x^2 + 1$. This is still open, but the analogous problem for primes of the form $x^2 + y^2 + 1$ was settled by Hooley in 1957 [9]. Put

$$r(n) = \#\{(x,y) \in \mathbb{Z}^2 : x^2 + y^2 = n\}.$$

Hooley gives the mean value of $r(n)$ along the shifted primes $q - 1$.

Theorem B. *For a certain positive constant* K, *we have*

$$\sum_{\substack{q \leq x \\ q \text{ prime}}} r(q-1) \sim K \frac{x}{\log x} \qquad (x \to \infty).$$

Actually, Hooley's work was conditional on GRH, but the discovery of the Bombieri–Vinogradov theorem allowed for this dependence to be removed with minimal changes to Hooley's argument. See [6]. (In the intervening years, Linnik gave an alternative proof of Theorem B [13].)

The following variant of Hooley's result was shown by Kátai in 1968 [11] (see also [12]).

Theorem B′. *For a certain positive constant* K', *we have*

$$\sum_{\substack{q \leq x \\ q \text{ prime} \\ q-1 \text{ squarefree}}} r(q-1) \sim K' \frac{x}{\log x} \qquad (x \to \infty).$$

It is elementary that for squarefree n, the number of square roots of -1 modulo n is precisely $\frac{r(n)}{4}$. In particular, Theorem B′ implies that -1 is a square modulo $q-1$ for infinitely many primes q.

We now bring in the second theorem of Hooley. First, a definition: If $P(T)$ is a polynomial with integer coefficients, and k is any positive integer, then a *normalized root of* P, *modulo* k, is a rational number of the form ϖ/k, where

$$f(\varpi) \equiv 0 \pmod{k}, \qquad 0 \leq \varpi < k.$$

In 1964, Hooley proved the following equidistribution theorem for normalized roots [10].

Theorem C. *Let* $P(T) \in \mathbb{Z}[T]$ *be an irreducible polynomial of degree at least* 2. *For each positive integer* k, *list the normalized roots of* P *modulo* k *(in any order), and then concatenate the lists sequentially for* $k = 1, 2, 3, \ldots$. *The resulting sequence is uniformly distributed in* $[0,1)$.

After this set-up, the reader can perhaps guess where we are headed. We prove that when $P(T) = T^2 + 1$, the conclusion of Hooley's Theorem C holds with the moduli restricted to the shifted primes $q - 1$.

Theorem 1.3. *Let $P(T) = T^2 + 1$. For each prime q, list the normalized roots of P modulo $q - 1$, and then concatenate the lists successively for $q = 2, 3, 5, 7, \ldots$. The resulting sequence is uniformly distributed in $[0, 1)$.*

Remark. By a different (deeper) method, Duke, Friedlander, and Iwaniec [5] have shown that Theorem 1.3 holds with the moduli running over primes q rather than shifted primes $q - 1$.

Notation. Most of our notation is standard. A possible exeption is our use of $P^+(n)$ and $P^-(n)$ for the largest and smallest prime factors of n (respectively); we adopt the convention that $P^+(1) = 1$ while $P^-(1) = \infty$. We let $\mathbb{1}$ denote the function that is identically $\mathbb{1}$, and we use $\mathbb{1}_C$ for the characteristic function of a property or set C. We write $e(x)$ for $e^{2\pi i x}$. We reserve the letter p for prime numbers.

2. Proof of Theorem 1.1

2.1. **Generalities.** Let $f \in \mathscr{M}$, and let A_1 and $A_2(\epsilon)$ be as in (I) and (II). Let $x \geq 3$, and let $\theta \in (0, 1)$. For each integer $n \in [1, x]$, we may write

$$n = p_1 \ldots p_j p_{j+1} \cdots p_J,$$

where

$$p_1 \leq p_2 \leq \cdots \leq p_J,$$

and where j is chosen as the largest index for which

$$p_1 \cdots p_j \leq x^\theta \quad \text{and} \quad p_1 \cdots p_j \parallel n.$$

We let

$$d := p_1 \cdots p_j,$$

and we refer to d as the *canonical unitary prefix divisor* of n.

We will assume that n has no proper prime power divisor in the interval $(x^{\theta/2}, x^\theta]$ and that

$$\Omega(n/d) \geq 2\theta^{-1}.$$

(In our eventual application, we will be able to handle the excluded values of n by a separate argument.)

Since $p_{j+1}^{\Omega(n/d)} \leq p_{j+1} \cdots p_J \leq n \leq x$, we see that

$$p_{j+1} \leq x^{1/\Omega(n/d)} \leq x^{\theta/2}. \tag{2.1}$$

Let t be the largest positive integer for which

$$p_{j+1} = p_{j+2} = \cdots = p_{j+t}.$$

Then $p_1 \cdots p_{j+t}$ is a unitary divisor of n, so that the choice of j forces $p_1 \cdots p_{j+t} > x^\theta$. Thus,

$$d = p_1 \cdots p_j > x^\theta / p_{j+1}^t.$$

If $p_{j+1}^t > x^{\theta/2}$, then $t > 1$, by (2.1); moreover, some power of p_{j+1} is then a proper prime power divisor of n belonging to $(x^{\theta/2}, x^\theta]$, contradicting our assumptions on n. So $p_{j+1}^t \leq x^{\theta/2}$, and, from the last displayed equation,

$$d > x^{\theta/2}.$$

From (2.1), there is a (unique) integer $r \geq 2$ satisfying

$$x^{\theta/(r+1)} < p_j \leq x^{\theta/r}.$$

Since

$$x \geq p_{j+1}^{\Omega(n/d)} \geq x^{\Omega(n/d)\cdot\theta/(r+1)},$$

we have $\Omega(n/d) \leq (r+1)\cdot\theta^{-1}$, so that

$$\begin{aligned} f(n) &= f(p_1\cdots p_j)f(p_{j+1}\cdots p_J) \\ &\leq f(p_1\cdots p_j)A_1^{\Omega(n/d)} \leq f(d)A_1^{(r+1)\theta^{-1}}. \end{aligned}$$

We collect the salient results in the following proposition.

Proposition 2.1. *Let $f \in \mathscr{M}$, and let $\theta \in (0,1)$. Let $x \geq 3$. Let n be an integer in $[1,x]$, and assume n does not have a squarefull divisor in $(x^{\theta/2}, x^{\theta}]$. Let d be the canonical unitary prefix divisor of n. If $\Omega(n/d) \geq 2/\theta$, then*

$$x^{\theta/2} < d \leq x^{\theta}, \quad x^{\theta/(r+1)} < P^+(d) \leq x^{\theta/r} \quad \text{for some integer } r \geq 2, \tag{2.2}$$

and

$$f(n) \leq \exp(O(r))f(d).$$

Here the implied constants depend only on θ, A_1, and $A_2(\epsilon)$.

2.2. **Completion of the proof of Theorem 1.1.** Fix $\theta = \beta/4$. We put those $n \in \mathscr{S}$ belonging to $(x-y,x]$ into the following three (possibly overlapping) categories. For each category we then bound the corresponding contribution to $\sum_{n\in\mathscr{S}\cap(x-y,x]} f(n)$.

(1) Arithmetically atypical n: Here we include all n with a proper prime power divisor in $(x^{\theta/2}, x^{\theta}]$. We also put in this category all n which have a $\log(x^{\theta})$-smooth divisor in the interval $(x^{\theta/2}, x^{\theta}]$.
(2) Those n for which $\Omega(n/d) \leq 2/\theta$, where (as above) d is the canonical unitary prefix divisor.
(3) All remaining $n \in \mathscr{S}$.

We handle category (1) using the crude pointwise bound $f(n) \ll_\epsilon n^\epsilon$. The number of $n \in (x-y,x]$ divisible by a proper prime power $p^k \in (x^{\theta/2}, x^{\theta}]$ does not exceed

$$\sum_{\substack{x^{\theta/2}<p^k\leq x^{\theta}\\ k\geq 2}} \left(\frac{y}{p^k}+1\right) \leq x^{\theta} + y \sum_{\substack{m>x^{\theta/2}\\ m \text{ squarefull}}} \frac{1}{m} \ll x^{\theta} + yx^{-\theta/4} \ll yx^{-\theta/4}.$$

Similarly, the number of $n \in (x-y,x]$ possessing a $\log(x^{\theta})$-smooth divisor $e \in (x^{\theta/2}, x^{\theta}]$ is at most

$$\begin{aligned} x^{\theta} + y \sum_{\substack{x^{\theta/2}<e\leq x^{\theta}\\ P^+(e)\leq \log(x^{\theta})}} \frac{1}{e} &\leq x^{\theta} + yx^{-\theta/2}\cdot \#\{e \leq x^{\theta} : P^+(e) \leq \log(x^{\theta})\} \\ &\ll x^{\theta} + yx^{-\theta/3} \ll yx^{-\theta/3}. \end{aligned}$$

(To justify passing from the first to the second line, we use that the count $\log T$-smooth numbers up to T is $T^{o(1)}$, as $T \to \infty$; see, e.g., [14, Corollary 7.9, p. 209].) Since $f(n) \ll x^{\theta/8}$ (say), it follows that the contribution to $\sum_{n\in\mathscr{S}\cap(x-y,x]} f(n)$ from arithmetically inconvenient n is

$$\ll (yx^{-\theta/4} + yx^{-\theta/3})x^{\theta/8} \ll yx^{-\theta/8}.$$

This is negligible, since the our target upper bound — the right-hand side of (1.2) — is $\gg y(\log x)^{-k}$.

For n falling into category (2), we have that $n = dp_{j+1}\cdots p_J$, where $J - j < 2\theta^{-1}$. If all of $p_{j+1}, p_{j+2}, \dots, p_J$ are bounded by $x^{\theta^2/2}$, then $n \le d(x^{\theta^2/2})^{2/\theta} \le x^{2\theta}$. Since $f(n) \ll x^\theta$, these n contribute $\ll x^{3\theta} \ll yx^{-\theta}$, which is once again negligible. So we may assume that $p_{j+t} > x^{\theta^2/2}$ for some positive integer $t \le J$. If t is chosen minimally, then putting

$$d' = p_1 p_2 \cdots p_{j+t-1},$$

we see that d' is a unitary divisor of n, that

$$d' \le x^{2\theta},$$

that

$$P^-(n/d') > x^{\theta^2/2},$$

and that

$$\begin{aligned} f(n) &= f(d')f(n/d') \\ &\le f(d')A_1^{2\theta^{-1}} \ll f(d'). \end{aligned}$$

Thus, these n make a contribution that its

$$\ll \sum_{d' \le x^{2\theta}} f(d') \cdot \#\{m : \frac{x-y}{d'} < m \le \frac{x}{d'}, md' \in \mathscr{S}, P^-(m) > x^{\theta^2/2}\}. \tag{2.3}$$

We use Brun's upper bound sieve to bound the count of m appearing in (2.3). Let p be a prime not exceeding $x^{\theta^2/2}$. The stated conditions imply that m avoids the residue class of 0 modulo p and, if $p \nmid d$, also an additional $\nu(p)$ residue classes modulo p. Keeping in mind that each $\nu(p) \le k$, Brun's sieve bounds the sum as

$$\begin{aligned} &\ll \frac{y}{d'} \prod_{\substack{p \le x^{\theta^2/2} \\ p \nmid d'}} \left(1 - \frac{\nu(p)+1}{p}\right) \prod_{\substack{p \le x^{\theta^2/2} \\ p \mid d'}} \left(1 - \frac{1}{p}\right) \\ &\ll \frac{y}{d' \log x} \prod_{\substack{p \le x^{\theta^2/2} \\ p \nmid d'}} \left(1 - \frac{\nu(p)}{p}\right). \end{aligned}$$

We can extend the product over all primes $p \le x$ without changing the order of magnitude. We conclude that

$$\begin{aligned} \sum_{\substack{\frac{x-y}{d'} < m \le \frac{x}{d'} \\ md' \in \mathscr{S} \\ P^-(m) > x^{\theta^2/2}}} 1 &\ll \left(\frac{y}{\log x} \prod_{p \le x} \left(1 - \frac{\nu(p)}{p}\right)\right) \prod_{p \mid d'} \left(1 - \frac{\nu(p)}{p}\right)^{-1} \\ &\ll \left(\frac{y}{\log x} \prod_{p \le x} \left(1 - \frac{\nu(p)}{p}\right)\right) g(d'), \end{aligned}$$

where

$$g(d') := \prod_{p \mid d'} \left(1 - \frac{\min\{k, p-1\}}{p}\right)^{-1}.$$

Inserting these bounds back into (2.3), we find that the remaining n in category (2) contribute

$$\ll \left(\frac{y}{\log x}\prod_{p\le x}\left(1-\frac{\nu(p)}{p}\right)\right)\sum_{d'\le x^{2\theta}}\frac{f(d')g(d')}{d'}$$
$$\ll \left(\frac{y}{\log x}\prod_{p\le x}\left(1-\frac{\nu(p)}{p}\right)\right)\prod_{p\le x}\left(1+\frac{f(p)g(p)}{p}+\frac{f(p^2)g(p^2)}{p^2}+\dots\right).$$

Now $f(p)g(p)/p = f(p)/p + O(1/p^2)$, while $\sum_{p\le x}\sum_{k\ge 2} f(p^k)g(p^k)/p^k \ll 1$. It follows that the last displayed product on p is $\ll \exp(\sum_{p\le x} f(p)/p)$, leading to an upper bound for the entire expression of

$$\ll \left(\frac{y}{\log x}\prod_{p\le x}\left(1-\frac{\nu(p)}{p}\right)\right)\prod_{p\le x}\left(1+\frac{f(p)}{p}\right),$$

which in turn is

$$\ll \frac{y}{\log x}\exp\left(\sum_{p\le x}\frac{f(p)-\nu(p)}{p}\right).$$

This expression coincides with that on the right-hand side of (1.2), and so the contribution from the n in category (2) is acceptable.

Finally, we turn to category (3). We subdivide the n in that category according to the value of r for which (2.2) holds. Since we are assuming that n does not have a $\log(x^\theta)$-smooth divisor in $(x^{\theta/2}, x^\theta]$, we only consider r for which $x^{\theta/r} \ge \log(x^\theta)$, so that

$$2 \le r \le \frac{\log(x^\theta)}{\log\log(x^\theta)}. \tag{2.4}$$

By Proposition 2.1, for each fixed r in the range (2.4), the corresponding n make a contribution that is

$$\ll \exp(O(r))\sum_{\substack{x^{\theta/2}<d\le x^\theta\\ P^+(d)\le x^{\theta/r}}} f(d)\cdot \#\{m : \frac{x-y}{d} < m \le \frac{x}{d}, P^+(m) > x^{\theta/(r+1)}, md\in\mathscr{S}\}.$$

In this case, Brun's sieve gives that the count of m is

$$\ll \frac{y}{d}\prod_{\substack{p\le x^{\theta/(r+1)}\\ p\nmid d}}\left(1-\frac{\nu(p)+1}{p}\right)\prod_{\substack{p\le x^{\theta/(r+1)}\\ p\mid d}}\left(1-\frac{1}{p}\right) \ll (r\theta^{-1})^{k+1}\left(\frac{y}{\log x}\prod_{p\le x}\left(1-\frac{\nu(p)}{p}\right)\right)\frac{g(d)}{d},$$

where g has the same meaning as above. Since $(r\theta^{-1})^{k+1} = \exp(O(r))$, we see that these n contribute

$$\ll \exp(O(r))\left(\frac{y}{\log x}\prod_{p\le x}\left(1-\frac{\nu(p)}{p}\right)\right)\sum_{\substack{x^{\theta/2}<d\le x^\theta\\ P^+(d)\le x^{\theta/r}}}\frac{f(d)g(d)}{d}. \tag{2.5}$$

The sum on d is estimated by the following special case of [15, Lemma 4].

Lemma 2.2. *Let $F \in \mathscr{M}$. Then, for all sufficiently large Z,*

$$\sum_{\substack{n \geq Z^{1/2} \\ P^+(n) \leq Z^{1/R}}} \frac{F(n)}{n} \ll \exp\bigg(\sum_{p \leq Z} \frac{F(p)}{p} - \frac{1}{10} R \log R\bigg),$$

uniformly for R satisfying $1 \leq R \leq \frac{\log Z}{\log\log Z}$. Here the threshold for "sufficiently large", as well as the implied constant, depends at most on the constant A_1 and the function $A_2(\epsilon)$ associated to F in the definition of $\mathscr{M}$.

Let $F = fg$, $Z = x^\theta$, and $R = r$. Using that $f \in \mathscr{M}$, it is straightforward to check that $F \in \mathscr{M}$; moreover, the A_1 and $A_2(\epsilon)$ corresponding to f suffice to determine, together with k, choices for A_1 and $A_2(\epsilon)$ corresponding to F. By (2.4), $2 \leq R \leq \frac{\log Z}{\log\log Z}$. Applying Lemma 2.2,

$$\begin{aligned}\sum_{\substack{x^{\theta/2} < d \leq x^\theta \\ P^+(d) \leq x^{\theta/r}}} \frac{f(d)g(d)}{d} &\ll \exp\bigg(\sum_{p \leq x^\theta} \frac{f(p)g(p)}{p} - \frac{1}{10} r \log r\bigg) \\ &\ll \exp\bigg(-\frac{1}{10} r \log r\bigg) \exp\bigg(\sum_{p \leq x} \frac{f(p)}{p}\bigg).\end{aligned}$$

(We used once more than $f(p)g(p)/p = f(p)/p + O(1/p^2)$.) We put this estimate back into (2.5) and then sum on r in the range (2.4). Since

$$\sum_r \exp(O(r)) \exp(-\frac{1}{10} r \log r) \ll 1,$$

we conclude that the total contribution of n from category (3) is

$$\ll \bigg(\frac{y}{\log x} \prod_{p \leq x} \Big(1 - \frac{\nu(p)}{p}\Big)\bigg) \exp\bigg(\sum_{p \leq x} \frac{f(p)}{p}\bigg),$$

which is

$$\ll \frac{y}{\log x} \exp\bigg(\sum_{p \leq x} \frac{f(p) - \nu(p)}{p}\bigg),$$

as desired. This completes the proof of Theorem 1.1.

3. Equidistribution of square roots of -1 modulo shifted primes: Proof of Theorem 1.3

We follow the original arguments of Hooley [10] as closely as possible.

For each positive integer k, let $\varrho(k)$ denote the number of square roots of -1 modulo k. From elementary number theory, ϱ is multiplicative and $\varrho(p^s) \leq 2$ for all prime powers p^s, so that $\varrho(k) \leq 2^{\omega(k)}$. Moreover, as noted in the introduction, $\varrho(k) = \frac{1}{4} r(k)$ for squarefree values of k. Thus, letting

$$\mathscr{K} = \{q - 1 : q \text{ prime}\},$$

Theorem B′ gives that

$$\sum_{\substack{k \leq x \\ k \in \mathscr{K}}} \varrho(k) \gg \frac{x}{\log x}. \tag{3.1}$$

For each pair of integers h, k with $k > 0$, let

$$S(h,k) = \sum_{\substack{\varpi \bmod k \\ \varpi^2 \equiv -1 \pmod k}} e(h\varpi/k).$$

Trivially, $|S(h,k)| \le \varrho(k)$. By Weyl's criterion and the lower bound (3.1), to prove Theorem 1.3 it will suffice to show that

$$\sum_{\substack{k \le x \\ k \in \mathscr{K}}} S(h,k) = o(x/\log x) \qquad (x \to \infty)$$

for each fixed $h \neq 0$. (Cf. the discussion on p. 48 of [10].)

In what follows, we let

$$X = x^{1/\log\log x}.$$

For each positive integer $k \le x$, we write $k = k_1 k_2$, where k_1 is X-smooth and k_2 is "X-rough" (meaning that $P^-(k_2) > X$). We decompose

$$\sum_{\substack{k \le x \\ k \in \mathscr{K}}} S(h,k) = \sum_{\substack{k \le x \\ k \in \mathscr{K} \\ k_1 \le x^{1/3}}} S(h,k) + \sum_{\substack{k \le x \\ k \in \mathscr{K} \\ k_1 > x^{1/3}}} S(h,k) = \sum\nolimits_1 + \sum\nolimits_2,$$

say. Concerning $\sum_2$, Cauchy–Schwarz gives

$$\sum\nolimits_2 \le \Bigg(\sum_{\substack{k \le x \\ k_1 > x^{1/3}}} 1 \Bigg)^{1/2} \Bigg(\sum_{\substack{k \le x \\ k_1 > x^{1/3}}} |S(h,k)|^2 \Bigg)^{1/2}. \tag{3.2}$$

Since $|S(h,k)| \le 2^{\omega(k)}$, we have that

$$\sum_{\substack{k \le x \\ k_1 > x^{1/3}}} |S(h,k)|^2 \le \sum_{k \le x} 2^{2\omega(k)} \ll x(\log x)^3;$$

the final estimate here follows, for instance, from Shiu's Theorem A (or the much more elementary Theorem 01 in [8]). On the other hand, by the estimate for '$\Theta(x,y,z)$' appearing at the bottom of p. 9 of [8],

$$\sum_{\substack{k \le x \\ k_1 > x^{1/3}}} 1 \le x \exp\left(-\left(\frac{1}{3} + o(1) \right) \log\log x \cdot \log\log\log x \right),$$

as $x \to \infty$. Putting these estimates back into (3.2), we see that

$$\sum\nolimits_2 = O(x/(\log x)^A)$$

for each fixed A. Thus, it will suffice to show that $\sum_1 = o(x/\log x)$, as $x \to \infty$.

Exactly as in [10] (see that paper's Lemma 3), we have $S(h,k) = S(h\bar{k}_2, k_1) S(h\bar{k}_1, k_2)$, where $\bar{k}_1$ denotes the inverse of k_1 modulo k_2, and $\bar{k}_2$ denotes the inverse of k_2 modulo k_1.

Now using k_1 and k_2 for generic X-smooth and X-rough numbers,

$$\sum\nolimits_1 = \sum_{\substack{k_1k_2\le x\\ k_1k_2\in\mathscr{K},\ k_1\le x^{1/3}}} S(h\bar{k}_2,k_1)S(h\bar{k}_1,k_2)$$
$$\ll \sum_{\substack{k_1k_2\le x\\ k_1k_2\in\mathscr{K},\ k_1\le x^{1/3}}} \varrho(k_2)|S(h\bar{k}_2,k_1)| \ll \sum_{k_1\le x^{1/3}} \Theta(x/k_1,k_1),$$

where, for $y\ge x^{2/3}$ and $k_1\le x^{1/3}$, we set

$$\Theta(y,k_1) = \sum_{\substack{k_2\le y\\ k_1k_2\in\mathscr{K}}} \varrho(k_2)|S(h\bar{k}_2,k_1)|.$$

Note that by Cauchy–Schwarz,

$$\Theta(y,k_1)^2 \le \Bigg(\sum_{\substack{k_2\le y\\ k_1k_2+1 \text{ prime}}} \varrho(k_2)^2\Bigg)\Bigg(\sum_{\substack{k_2\le y\\ k_1k_2+1 \text{ prime}}} |S(h\bar{k}_2,k_1)|^2\Bigg). \tag{3.3}$$

The first parenthesized sum in (3.3) can be handled by Theorem 1.1. With P the product of the primes not exceeding X, we have that

$$\sum_{\substack{k_2\le y\\ k_1k_2+1 \text{ prime}}} \varrho(k_2)^2 \le \sum_{\substack{n\le y\\ k_1n+1 \text{ prime}}} \mathbb{1}_{\gcd(n,P)=1}2^{2\omega(n)}.$$

To proceed, we observe that for k_1n+1 to be prime, either $n\le y^{1/2}$, or n avoids the class of $-k_1^{-1}$ mod p for all primes $p\le X$ not dividing k_1. The former case accounts for $O(y^{1/2})$ values of n. By Theorem 1.1, the latter case contributes

$$\ll \frac{y}{\log y}\exp\Bigg(\sum_{\substack{p\le X\\ p\nmid k_1}}\frac{-1}{p}+\sum_{X<p\le y}\frac{4}{p}\Bigg) \ll \frac{y}{\log y}\frac{1}{\log X}\Bigg(\frac{\log y}{\log X}\Bigg)^4\exp\Bigg(\sum_{p\mid k_1}\frac{1}{p}\Bigg) \ll \frac{y(\log\log x)^6}{(\log x)^2}.$$

such values. (We used here that $\log y \asymp \log x$, that $\log X = \log x/\log\log x$, and that $\exp(\sum_{p\mid k_1}\frac{1}{p}) \ll \frac{k_1}{\varphi(k_1)} \ll \log\log 3k_1 \ll \log\log x$.) The contribution of $y^{1/2}$ is negligible compared to this, and so

$$\sum_{\substack{k_2\le y\\ k_1k_2+1 \text{ prime}}} \varrho(k_2)^2 \ll \frac{y(\log\log x)^6}{(\log x)^2}.$$

Turning to the second parenthesized sum in (3.3), we have that

$$\sum_{\substack{k_2\le y\\ k_1k_2+1 \text{ prime}}} |S(h\bar{k}_2,k_1)|^2 = \sum_{0\le a<k_1} |S(ah,k_1)|^2\cdot \#\{k_2\le y : k_2\equiv \bar{a} \pmod{k_1}, k_1k_2+1 \text{ prime}\}.$$

Writing a_0 for the least nonnegative residue of $\bar{a}$ modulo k_1, we see that the values of k_2 counted here have the form a_0+k_1t for some $t\le y/k_1$. Moreover, either $t\le (y/k_1)^{1/2}$, or both a_0+k_1t and $k_1(a_0+k_1t)+1$ have no prime factors exceeding X. Brun's sieve now implies that the count of k_2 is

$$\ll \frac{y}{k_1(\log X)^2}\exp\Bigg(\sum_{p\mid k_1}\frac{2}{p}\Bigg) \ll \frac{y(\log\log x)^4}{k_1(\log x)^2},$$

and thus

$$\sum_{0\le a<k_1} |S(ah,k_1)|^2 \cdot \#\{k_2 \le y : k_2 \equiv \bar{a} \pmod{k_1}, k_1k_2+1 \text{ prime}\} \ll \frac{y(\log\log x)^4}{k_1(\log x)^2} \sum_{0\le a<k_1} |S(ah,k_1)|^2.$$

Exactly as in [10] (see Lemma 1 there), the sum on a is at most $\varrho(k_1)k_1 \gcd(h,k_1)$, and now collecting estimates yields

$$\sum_{\substack{k_2\le y\\ k_1k_2+1 \text{ prime}}} |S(h\bar{k}_2,k_1)|^2 \ll \frac{y(\log\log x)^4}{(\log x)^2}\varrho(k_1)$$

where here and for the remainder of the argument, the implied constants may depend on h.

Referring back to (3.3),

$$\Theta(y,k_1) \ll \frac{y}{(\log x)^2}(\log\log x)^5 \varrho(k_1)^{1/2},$$

so that

$$\sum\nolimits_1 \ll \sum_{k_1\le x^{1/3}} \Theta(x/k_1,k_1) \ll \frac{x}{(\log x)^2}(\log\log x)^5 \sum_{k_1\le x^{1/3}} \frac{\varrho(k_1)^{1/2}}{k_1}.$$

Bounding the sum on k_1 by an Euler product, as in [10] (cf. the display immediately preceding that paper's eq. (12)), we find that

$$\sum_{k_1\le x^{1/3}} \frac{\varrho(k_1)^{1/2}}{k_1} \ll (\log x)^{1/\sqrt{2}}.$$

We conclude that

$$\sum\nolimits_1 \ll \frac{x}{(\log x)^{2-\frac{1}{\sqrt{2}}}}(\log\log x)^5.$$

Since $2-\frac{1}{\sqrt{2}} > 1$, this implies that $\sum_1 = o(x/\log x)$, as desired. This completes the proof of Theorem 1.3.

Acknowledgments

The author is supported by NSF award DMS-1402268. He thanks the referee for a careful reading of the manuscript.

References

[1] M. B. Barban, *Multiplicative functions of ${}^{\Sigma}R-$equidistributed sequences*, Izv. Akad. Nauk UzSSR Ser. Fiz.–Mat. Nauk **1964** (1964), no. 6, 13–19 (Russian).

[2] ———, *On the number of divisors of "translations" of the prime number-twins*, Acta Math. Acad. Sci. Hungar. **15** (1964), 285–288 (Russian).

[3] M. B. Barban and B. V. Levin, *Multiplicative functions on "shifted" prime numbers*, Dokl. Akad. Nauk SSSR **181** (1968), 778–780 (Russian).

[4] M. B. Barban and P. P. Vehov, *Summation of multiplicative functions of polynomials*, Mat. Zametki **5** (1969), 669–680 (Russian).

[5] W. Duke, J. B. Friedlander, and H. Iwaniec, *Equidistribution of roots of a quadratic congruence to prime moduli*, Ann. of Math. (2) **141** (1995), 423–441.

[6] P. D. T. A. Elliott and H. Halberstam, *Some applications of Bombieri's theorem*, Mathematika **13** (1966), 196–203.
[7] P. Erdős, *On the sum* $\sum_{k=1}^{x} d(f(k))$, J. London Math. Soc. **27** (1952), 7–15.
[8] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics, vol. 90, Cambridge University Press, Cambridge, 1988.
[9] C. Hooley, *On the representation of a number as the sum of two squares and a prime*, Acta Math. **97** (1957), 189–210.
[10] ———, *On the distribution of the roots of polynomial congruences*, Mathematika **11** (1964), 39–49.
[11] I. Kátai, *A note on a sieve method*, Publ. Math. Debrecen **15** (1968), 69–73.
[12] ———, *On an application of the large sieve: Shifted prime numbers, which have no prime divisors from a given arithmetical progression*, Acta Math. Acad. Sci. Hungar **21** (1970), 151–173.
[13] Yu. V. Linnik, *An asymptotic formula in the Hardy–Littlewood additive problem*, Izv. Akad. Nauk SSSR, Ser. Mat. **24** (1960), 629–706 (Russian).
[14] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.
[15] P. Shiu, *A Brun-Titchmarsh theorem for multiplicative functions*, J. Reine Angew. Math. **313** (1980), 161–170.
[16] A. I. Vinogradov and Yu. V. Linnik, *Estimate of the sum of the number of divisors in a short segment of an arithmetic progression*, Uspehi Mat. Nauk (N.S.) **12** (1957), no. 4(76), 277–280 (Russian).
[17] D. Wolke, *Multiplikative Funktionen auf schnell wachsenden Folgen*, J. Reine Angew. Math. **251** (1971), 54–67.

Department of Mathematics, University of Georgia, Athens, GA 30602
Email address: pollack@uga.edu