Algebra & Number Theory

Volume 8
2014
No. 7

Bounded gaps between primes with a given primitive root

Paul Pollack

msp

ALGEBRA AND NUMBER THEORY 8:7 (2014)
dx.doi.org/10.2140/ant.2014.8.1769

Bounded gaps between primes with a given primitive root

Paul Pollack

Fix an integer $g \neq -1$ that is not a perfect square. In 1927, Artin conjectured that there are infinitely many primes for which g is a primitive root. Forty years later, Hooley showed that Artin's conjecture follows from the generalized Riemann hypothesis (GRH). We inject Hooley's analysis into the Maynard–Tao work on bounded gaps between primes. This leads to the following GRH-conditional result: *Fix an integer $m \geq 2$. If $q_1 < q_2 < q_3 < \cdots$ is the sequence of primes possessing g as a primitive root, then* $\liminf_{n\to\infty}(q_{n+(m-1)} - q_n) \leq C_m$, *where C_m is a finite constant that depends on m but not on g.* We also show that the primes $q_n, q_{n+1}, \ldots, q_{n+m-1}$ in this result may be taken to be consecutive.

1. Introduction

The following conjecture was proposed by Emil Artin in the course of a September 1927 conversation with Helmut Hasse:

Artin's primitive root conjecture. *Fix an integer $g \neq -1$ that is not a square. There are infinitely many primes p for which g is a primitive root modulo p. In fact, the number of such $p \leq x$ is (as $x \to \infty$) asymptotically $c_g \pi(x)$ for a certain $c_g > 0$.*

While there is a substantial literature surrounding Artin's conjecture (lovingly catalogued in the survey [Moree 2012]), we still know infuriatingly little. In particular, there is no specific value of g which is known to occur as a primitive root for infinitely many primes. However, thanks to work of Heath-Brown [1986] (refining earlier results of Gupta and Murty [1984]), we know that at least one of 2, 3, and 5 has this property. In fact, one can replace "2, 3, and 5" with any three multiplicatively independent integers satisfying mild conditions.

In a seminal paper, Hooley [1967] (see also his exposition in [Hooley 1976, Chapter 3]) showed that the Chebotarev density theorem with a sufficiently sharp error term would imply the quantitative form of Artin's conjecture. Moreover, he showed that such a variant of Chebotarev's density theorem — at least for the cases relevant for this application — follows from the generalized Riemann hypothesis

MSC2010: primary 11A07; secondary 11N05.
Keywords: primitive root, Artin's conjecture, bounded gaps, Maynard–Tao theorem.

(GRH) for Dedekind zeta functions. Thus, under GRH, we have a complete proof of Artin's conjecture.

In this paper, we combine Hooley's work on Artin's conjecture with recent methods used to study gaps between primes. In sensational work of Maynard [2013] and Tao, it is shown that $\liminf_{n\to\infty}(p_{n+m-1}-p_n)<\infty$ for every m. Here $p_1<p_2<p_3<\cdots$ is the sequence of all primes, in the usual order. Our main theorem is an analogous bounded gaps result for primes possessing a prescribed primitive root.

Theorem 1.1 (conditional on GRH). *Fix an integer $g\neq -1$ and not a square. Let $q_1<q_2<q_3<\cdots$ denote the sequence of primes for which g is a primitive root. Then, for each m,*

$$\liminf_{n\to\infty}(q_{n+m-1}-q_n)\le C_m,$$

where C_m is a finite constant depending on m but not on g.

In the last section of the paper, we show how to modify the proof of Theorem 1.1 to impose the additional restriction that the m primes $q_n, q_{n+1},\dots,q_{n+m-1}$ are in fact *consecutive* (Theorem 4.1).

We remark that other recent work producing bounded gaps between primes in special sets has been done by Thorner [2014], who handles primes restricted by Chebotarev conditions, and by Li and Pan [2014], who work with primes p for which $p+2$ is an "almost prime".

Notation. The letters p and q always denote primes. We use the Bachmann–Landau O and o notations, as well as the associated Vinogradov symbols $\ll$ and $\gg$, with their usual meanings.

2. Technical preparation

Configurations of quadratic residues and nonresidues. We will use that certain configurations of residues and nonresidues are guaranteed to appear for all large enough primes. This is a fairly standard consequence of the Riemann Hypothesis for curves, as proved by Weil, but we give the argument for completeness. The following lemma is a special case of [Wan 1997, Corollary 2.3].

Lemma 2.1. *Let p be a prime. Suppose that $f(T)$ is a monic polynomial in $\mathbb{F}_p[T]$ of degree d and that $f(T)$ is not a square in $\mathbb{F}_p[T]$. Then*

$$\left|\sum_{a \bmod p}\left(\frac{f(a)}{p}\right)\right|\le (d-1)\sqrt{p}.$$

Lemma 2.2. *Let p be a prime, and let k be a positive integer. Suppose that $h_1,\dots,h_k$ are integers, no two of which are congruent modulo p. Suppose*

$\epsilon_1, \dots, \epsilon_k \in \{\pm 1\}$. *The number of mod p solutions n to the system of equations*

$$\left(\frac{n+h_i}{p}\right) = \epsilon_i \quad \text{for all } 1 \le i \le k \tag{2-1}$$

is at least $p/2^k - (k-1)\sqrt{p} - k$.

Proof. For each n, let $\iota(n) = (1/2^k)\prod_{i=1}^{k}\big(1 + \epsilon_i\big(\frac{n+h_i}{p}\big)\big)$. If we suppose that $n \not\equiv -h_1, \dots, -h_k \pmod p$, then $\iota(n)$ equals 1 when (2-1) holds, and 0 otherwise. Since $|\iota(n)| \le 1$ for all n, the number of solutions to (2-1) is at least $-k + \sum_{n \bmod p} \iota(n)$. For each subset $S \subset \{1, 2, 3, \dots, k\}$, put $f_S(T) = \prod_{i\in S}(T + h_i) \in \mathbb{F}_p[T]$. Then

$$\sum_{n \bmod p} \iota(n) = \frac{1}{2^k} \sum_{S\subset\{1,2,\dots,k\}} \left(\prod_{i\in S} \epsilon_i\right) \sum_{n \bmod p} \left(\frac{f_S(n)}{p}\right).$$

If $S = \varnothing$, then $f_S = 1$, and we get a contribution of $p/2^k$. In all other cases, f_S is a nonsquare polynomial of degree at most k. By Lemma 2.1, the total contribution from all nonempty subsets of $\{1, 2, \dots, k\}$ is bounded in absolute value by $((2^k - 1)/2^k)(k-1)\sqrt{p} \le (k-1)\sqrt{p}$. Thus, $\sum_{n \bmod p} \iota(n) \ge p/2^k - (k-1)\sqrt{p}$, and the lemma follows. □

Effective Chebotarev. The next result is due in essence to Lagarias and Odlyzko [1977], although the precise formulation we give is due to Serre [1981, §2.4]:

Theorem 2.3 (conditional on GRH). *Let L be a finite Galois extension of $\mathbb{Q}$ with Galois group G, and let C be a conjugacy class of G. The number of unramified primes $p \le x$ whose Frobenius conjugacy class $(p, L/\mathbb{Q})$ is C is given by*

$$\frac{\#C}{\#G}\mathrm{Li}(x) + O\Big(\frac{\#C}{\#G} x^{1/2}\big(\log|\Delta_L| + [L:\mathbb{Q}]\log x\big)\Big)$$

for all $x \ge 2$. Here Δ_L denotes the discriminant of L and the O-constant is absolute.

To apply Theorem 2.3, we require an upper bound for the term $\log|\Delta_L|$. The following result, which is contained in [Serre 1981, Proposition 6], suffices for our applications.

Lemma 2.4. *For every Galois extension $L/\mathbb{Q}$, we have*

$$\log|\Delta_L| \le ([L:\mathbb{Q}] - 1)\sum_{p\mid\Delta_L} \log p + [L:\mathbb{Q}]\log[L:\mathbb{Q}].$$

3. Proof of Theorem 1.1

The Maynard–Tao strategy. We begin by recalling the strategy of [Maynard 2013] for producing bounded gaps between primes. Let $k \ge 2$ be a fixed positive integer, and let $\mathcal{H} = \{h_1 < h_2 < \cdots < h_k\}$ denote a fixed *admissible k-tuple*, i.e., a set of

k distinct integers that does not occupy all of the residue classes modulo p for any prime p. With N a large positive integer, we seek values of n belonging to the dyadic interval $[N, 2N)$ for which the shifted tuple $n+h_1, n+h_2, \dots, n+h_k$ contains several primes.

Let $W := \prod_{p \le \log\log\log N} p$. Choose an integer ν so that $\gcd(\nu + h_i, W) = 1$ for all $1 \le i \le k$; the existence of such a ν is implied by the admissibility of $\mathcal{H}$. We restrict attention to integers $n \equiv \nu \pmod W$. This has the effect of pre-sieving the values of n to ensure that none of the $n + h_i$ have any small prime factors. Let $w(n)$ denote nonnegative weights (to be chosen momentarily), and let $\chi_{\mathscr{P}}$ denote the characteristic function of the set $\mathscr{P}$ of prime numbers. One studies the sums

$$S_1 := \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W}} w(n) \quad \text{and} \quad S_2 := \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W}} \Bigg(\sum_{i=1}^{k} \chi_{\mathscr{P}}(n+h_i) \Bigg) w(n).$$

The ratio S_2/S_1 is a weighted average of the number of primes among $n+h_1, \dots, n+h_k$, as n ranges over $[N, 2N)$. Consequently, if $S_2 > (m-1)S_1$ for the positive integer m, then at least m of the numbers $n+h_1, \dots, n+h_k$ are primes. So, if the inequality $S_2 > (m-1)S_1$ is achieved for a sequence of n tending to infinity, then $\liminf(p_{n+m-1} - p_n) \le h_k - h_1 < \infty$.

As we have described it so far, this strategy goes back to Goldston, Pintz, and Yıldırım. The key innovation in the approach of Maynard and Tao is the choice of congenial weights $w(n)$. The following result, which is a restatement of [Maynard 2013, Proposition 4.1], is crucial.

Proposition 3.1. *Let θ be a real number, $0 < \theta < \frac{1}{4}$. Let F be a piecewise differentiable function supported on the simplex $\{(x_1, \dots, x_k) : \text{each } x_i \ge 0, \sum_{i=1}^k x_i \le 1\}$. With $R := N^\theta$, put*

$$\lambda_{d_1,\dots,d_k} := \Bigg(\prod_{i=1}^{k} \mu(d_i) d_i \Bigg) \sum_{\substack{r_1,\dots,r_k \\ d_i \mid r_i \ \forall i \\ (r_i, W) = 1 \ \forall i}} \frac{\mu\big(\prod_{i=1}^k r_i\big)^2}{\prod_{i=1}^k \varphi(r_i)} F\Bigg(\frac{\log r_1}{\log R}, \dots, \frac{\log r_k}{\log R} \Bigg)$$

whenever $\gcd\big(\prod_{i=1}^{k} d_i, W\big) = 1$, *and let* $\lambda_{d_1,\dots,d_k} = 0$ *otherwise. Let*

$$w(n) := \Bigg(\sum_{d_i \mid n+h_i \ \forall i} \lambda_{d_1,\dots,d_k} \Bigg)^2.$$

Then, as $N \to \infty$,

$$S_1 \sim \frac{\varphi(W)^k}{W^{k+1}} N (\log R)^k I_k(F) \quad \textit{and}$$

$$S_2 \sim \frac{\varphi(W)^k}{W^{k+1}} \frac{N}{\log N} (\log R)^{k+1} \sum_{m=1}^{k} J_k^{(m)}(F),$$

provided that $I_k(F) \neq 0$ *and* $J_k^{(m)}(F) \neq 0$ *for each* m, *where*

$$I_k(F) := \int \cdots \int_{[0,1]^k} F(t_1, \dots, t_k)^2 \, dt_1 \, dt_2 \cdots dt_k,$$

$$J_k^{(m)}(F) := \int \cdots \int_{[0,1]^{k-1}} \left(\int_0^1 F(t_1, \dots, t_k) \, dt_m \right)^2 dt_1 \cdots dt_{m-1} \, dt_{m+1} \cdots dt_k.$$

From our interpretation of S_2/S_1 as a weighted average, we know that there is an $n \in [N, 2N)$ for which at least S_2/S_1 of the numbers $n + h_1, \dots, n + h_k$ are prime. Proposition 3.1 shows that $S_2/S_1 \to (\theta/I_k(F)) \sum_{m=1}^k J_k^{(m)}(F)$ as $N \to \infty$. For each F satisfying the conditions of Proposition 3.1, put

$$M_k(F) := \frac{1}{I_k(F)} \sum_{m=1}^k J_k^{(m)}(F), \quad \text{and set } M_k := \sup_F M_k(F). \tag{3-1}$$

Upon choosing θ close to $\frac{1}{4}$ and F so that $M_k(F)$ is close to M_k, we find that, infinitely often, at least $\lceil \frac{1}{4} M_k \rceil$ of the numbers $n + h_1, \dots, n + h_k$ are prime. The following lower bound on M_k is due to Maynard [2013, Proposition 4.3].

Proposition 3.2. $M_k \to \infty$ *as* $k \to \infty$. *In fact, for all sufficiently large values of* k,

$$M_k > \log k - 2 \log \log k - 2.$$

Consequently, once k is a little larger than e^{4m}, we have $\lceil \frac{1}{4} M_k \rceil > m - 1$. From the above discussion, $\liminf_{n\to\infty}(p_{n+m-1} - p_n) \le h_k - h_1 < \infty$ for every admissible k-tuple $\mathcal{H}$. Choosing $\mathcal{H}$ carefully, this argument gives $\liminf_{n\to\infty}(p_{n+m-1} - p_n) \ll m^3 e^{4m}$; see the proof of [Maynard 2013, Theorem 1.1] for details.

Modifying Maynard–Tao. For the rest of the paper, we fix an integer $g \neq -1$ that is not a square. Let $\widetilde{\mathscr{P}}$ denote the set of primes having g as a primitive root. Fix an integer $k \ge 2$, and let

$$K := 9k^2 \cdot 4^k.$$

We fix $\mathcal{H}$ as the admissible k-tuple having $h_i = (i-1)K!$ for all $1 \le i \le k$; that is,

$$\mathcal{H} := \{0, K!, 2K!, \dots, (k-1)K!\}. \tag{3-2}$$

We work below with a fixed function F satisfying the conditions of Proposition 3.1. For the rest of the argument, implied constants may depend on g, k, and F without further mention.

In what follows, we think of N as very large, in particular much larger than g. We use the Maynard–Tao strategy to detect integers $n \in [N, 2N)$ for which the list $n + h_1, \dots, n + h_k$ contains several primes belonging to $\widetilde{\mathscr{P}}$. Let g_0 denote the

discriminant of the quadratic field $\mathbb{Q}(\sqrt{g})$. Set

$$W := \operatorname{lcm}\Big[g_0, \prod_{p \le \log\log\log N} p\Big].$$

Once again, we pre-sieve values of n by putting n in an appropriate residue class $\nu \bmod W$. Whereas Maynard could choose any ν with $\gcd(\nu + h_i, W) = 1$ for all $1 \le i \le k$, we must tread more carefully. We choose ν so that the primes detected by the sieve are heavily biased towards having g as a primitive root.

Lemma 3.3. *We can choose an integer ν with all of the following properties*:

(i) $\nu + h_i$ *is coprime to* W *for all* $1 \le i \le k$.

(ii) $\nu + h_i - 1$ *is coprime to* $\prod_{2 < p \le \log\log\log N} p$ *for all* $1 \le i \le k$.

(iii) *The Kronecker symbol* $\left(\frac{g_0}{\nu + h_i}\right)$ *equals* -1 *for all* $1 \le i \le k$.

Proof. Factor g_0 as a product $D_1 D_2 \dots D_\ell$ of coprime prime discriminants, where the *prime discriminants* are the numbers -4, -8, 8, and $(-1)^{(p-1)/2}p$ for odd primes p. Reordering the factorization if necessary, we can assume all of the following:

- If all $|D_i| \le K$ and g_0 is even, then $D_1 \in \{-4, -8, 8\}$.
- If all $|D_i| \le K$, g_0 is odd, and $\ell > 1$, then $|D_1| \ge 5$.
- If some $|D_i| > K$, then $|D_1| > K$.

We start by choosing any odd integer ν_1 that avoids the residue classes $-h_1, \dots, -h_k$, $1 - h_1, \dots, 1 - h_k$ modulo p for each odd prime $p \le \log\log\log N$ not dividing D_1. Note that when $p \le K$ the only requirement on ν_1 is that it avoids the residue classes 0 and 1 mod p, while when $p > K$ we are to avoid at most $2k$ of the $p > K > 2k$ residue classes modulo p. So such a choice of ν_1 certainly exists by the Chinese remainder theorem. We choose ν to satisfy

$$\nu \equiv \nu_1 \pmod{[W/D_1, 2]}.$$

To ensure (i), (ii), and (iii), it suffices to impose a further condition on ν guaranteeing

(i′) $\nu + h_i$ is coprime to all odd p dividing D_1 for all $1 \le i \le k$,

(ii′) $\nu + h_i - 1$ is coprime to all odd p dividing D_1 for all $1 \le i \le k$,

(iii′) $\left(\frac{D_1}{\nu + h_i}\right) = -\left(\frac{D_2 \cdots D_\ell}{\nu_1 + h_i}\right)$ for all $1 \le i \le k$.

Notice that for all $1 \le i \le k$ we have $\left(\frac{D_2 \cdots D_\ell}{\nu_1 + h_i}\right) \ne 0$, by the choice of ν_1.

Case I: all $|D_i| \le K$. In this case, (i′) and (ii′) are satisfied as long as $\nu \not\equiv 0$ or $1 \pmod p$ for any odd p dividing D_1, while (iii′) is satisfied as long as

$$\Big(\frac{D_1}{\nu}\Big) = -\Big(\frac{D_2 \cdots D_\ell}{\nu_1}\Big).$$

Assume first that g_0 is even. Then $D_1 \in \{-4, -8, 8\}$ and (i′) and (ii′) hold vacuously. Choose ν_2 so that $\big(\frac{D_1}{\nu_2}\big) = -\big(\frac{D_2 \cdots D_\ell}{\nu_1}\big)$. We ensure (iii′) by selecting ν as any solution to the simultaneous congruences

$$\nu \equiv \nu_1 \pmod{[W/D_1, 2]} \quad \text{and} \quad \nu \equiv \nu_2 \pmod{D_1}. \tag{3-3}$$

While the moduli here share a factor of 2, it is clear that these congruences still admit a simultaneous solution, since the only 2-adic information encoded by the first congruence is that ν is odd, which is certainly compatible with the second!

Now assume instead that g_0 is odd, so that $|D_1|$ is an odd prime. Either $|D_1| = 3$ and $\ell = 1$, or $|D_1| \ge 5$. If the former, then (i′), (ii′), and (iii′) hold upon selecting $\nu_2 = 2$ and choosing ν to satisfy (3-3). If the latter, choose $\nu_2 \not\equiv 1 \pmod{D_1}$ with $\big(\frac{D_1}{\nu_2}\big) = -\big(\frac{D_2 \cdots D_\ell}{\nu_1}\big)$ (possible since that equality of Kronecker symbols holds for a total of $\frac{1}{2}(|D_1| - 1) > 1$ residue classes $\nu_2 \bmod D_1$). Once again, choosing ν to satisfy (3-3) completes the proof.

Case II: some $|D_i| > K$. In this case, $|D_1| > K$. Since $K > 8$, we see that $|D_1|$ is an odd prime. To satisfy (i′), (ii′), and (iii′), it suffices to show that there is an integer $\nu_2 \not\equiv 1 - h_1, \dots, 1 - h_k \pmod{D_1}$ with

$$\left(\frac{\nu_2 + h_i}{|D_1|}\right) = -\left(\frac{D_2 \cdots D_\ell}{\nu_1 + h_i}\right) \quad \text{for all } 1 \le i \le k, \tag{3-4}$$

for then we can choose as ν any solution to (3-3). (We used here that $\big(\frac{D_1}{\nu + h_i}\big) = \big(\frac{\nu + h_i}{|D_1|}\big)$.) The integers $h_1, \dots, h_k$ are incongruent modulo D_1, as each nonzero difference $h_j - h_i = (j - i)K!$ has only prime factors smaller than K. So Lemma 2.2 gives that the number of $\nu_2 \bmod D_1$ satisfying (3-4) is at least $|D_1|/2^k - (k-1)\sqrt{|D_1|} - k$. Since $|D_1| > K = 9k^2 \cdot 4^k$, this count of solutions exceeds k. In particular, we can satisfy (3-4) with $\nu_2 \not\equiv 1 - h_1, \dots, 1 - h_k \pmod{D_1}$. □

Assume that ν has been chosen to satisfy the conditions of Lemma 3.3. We let $R = N^\theta$, with θ to be specified momentarily, and we define the weights $w(n)$ exactly as in the statement of Proposition 3.1. We let

$$\tilde{S}_1 := \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W}} w(n) \quad \text{and} \quad \tilde{S}_2 := \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W}} \Big(\sum_{i=1}^{k} \chi_{\widetilde{\mathscr{P}}}(n + h_i)\Big) w(n).$$

Theorem 1.1 is a consequence of the following result, established in the next section.

Proposition 3.4 (assuming GRH). *Fix a positive real number $\theta < \frac{1}{4}$. As $N \to \infty$, we have the same asymptotic estimates for $\tilde{S}_1$ and $\tilde{S}_2$ as those for S_1 and S_2 given in Proposition 3.1.*

Once Proposition 3.4 has been established, the earlier analysis we applied to Maynard's Proposition 3.1 applies, and we immediately obtain Theorem 1.1.

Proof of Proposition 3.4. The $\tilde{S}_1$ estimate is established in precisely the same way as Maynard's S_1 estimate in Proposition 3.1; see the proofs of Lemmas 5.1 and 6.2 in [Maynard 2013]. So we describe only the estimation of $\tilde{S}_2$. We write $\tilde{S}_2 = \sum_{m=1}^{k} \tilde{S}_2^{(m)}$, where

$$\tilde{S}_2^{(m)} := \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W}} \chi_{\tilde{\mathscr{P}}}(n + h_m) w(n).$$

This is precisely analogous to Maynard's decomposition of S_2 as $\sum_{m=1}^{k} S_2^{(m)}$, where

$$S_2^{(m)} := \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W}} \chi_{\mathscr{P}}(n + h_m) w(n).$$

Maynard's proof of Proposition 3.1 gives that each

$$S_2^{(m)} \sim \frac{\varphi(W)^k}{W^{k+1}} \frac{N}{\log N} (\log R)^{k+1} \cdot J_k^{(m)}(F).$$

So, to prove Proposition 3.4, it suffices to show that for each m we have

$$S_2^{(m)} - \tilde{S}_2^{(m)} = o\left(\frac{\varphi(W)^k}{W^{k+1}} N (\log N)^k \right) \tag{3-5}$$

as $N \to \infty$. From now on, we think of m as fixed, and we focus our energies on proving (3-5).

To prepare for the proof of (3-5), for each prime q we let $\mathscr{P}_q^{(0)}$ denote the set of all primes p satisfying

$$p \equiv 1 \pmod q \quad \text{and} \quad g^{(p-1)/q} \equiv 1 \pmod p. \tag{3-6}$$

Let

$$\mathscr{P}_q := \mathscr{P}_q^{(0)} \setminus \bigcup_{q' < q} \mathscr{P}_{q'}^{(0)}.$$

Provided that the argument is not a prime divisor of g,

$$0 \le \chi_{\mathscr{P}} - \chi_{\tilde{\mathscr{P}}} \le \sum_q \chi_{\mathscr{P}_q}. \tag{3-7}$$

Indeed, if p is a prime not dividing g, then either g is a primitive root mod p or g is a q-th power residue mod p for some prime q dividing $p-1$. From (3-7), it

follows immediately that

$$0 \le S_2^{(m)} - \tilde{S}_2^{(m)} \le \sum_q \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W}} \chi_{\mathscr{P}_q}(n + h_m) w(n). \tag{3-8}$$

We claim that the primes $q \le \log\log\log N$ make no contribution to the right-hand side of (3-8). Indeed, suppose $p := n + h_m$ is prime with $N \le n < 2N$ and $n \equiv \nu \pmod W$. By Lemma 3.3(ii), the number $p - 1$ has no odd prime factors up to $\log\log\log N$; it follows trivially that $\chi_{\mathscr{P}_q}(p) = 0$ for odd $q \le \log\log\log N$. By Lemma 3.3(iii), $\chi_{\mathscr{P}_2}(p) = 0$, since, modulo p,

$$g^{(p-1)/2} \equiv \left(\frac{g}{p}\right) = \left(\frac{g}{n+h_m}\right) = \left(\frac{g_0}{n+h_m}\right) = -1.$$

Thus, the right-hand side of (3-8) can be rewritten as $\Sigma_1 + \Sigma_2 + \Sigma_3 + \Sigma_4$, where each Σ_i represents a partial sum of (3-8) over values of q in the following ranges:

Σ_1: $\log\log\log N < q \le (\log N)^{100k}$,

Σ_2: $(\log N)^{100k} < q \le N^{1/2}(\log N)^{-100k}$,

Σ_3: $N^{1/2}(\log N)^{-100k} < q \le N^{1/2}(\log N)^{100k}$,

Σ_4: $q > N^{1/2}(\log N)^{100k}$.

We treat these ranges of q separately.

Estimation of Σ_2 *and* Σ_4. We need the following lemma, which facilitates later applications of Cauchy–Schwarz.

Lemma 3.5.
$$\sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W}} w(n)^2 \ll \frac{N}{W}(\log R)^{19k}.$$

Proof. Let $\boldsymbol{d} = (d_1, \dots, d_k)$, $\boldsymbol{e} = (e_1, \dots, e_k)$, $\boldsymbol{f} = (f_1, \dots, f_k)$, and $\boldsymbol{g} = (g_1, \dots, g_k)$ represent k-tuples of positive integers. Expanding the sum using the definition of $w(n)$ gives

$$\sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W}} \sum_{\substack{\boldsymbol{d},\boldsymbol{e},\boldsymbol{f},\boldsymbol{g} \\ [d_i,e_i,f_i,g_i] \mid n+h_i \ \forall i}} \lambda_{\boldsymbol{d}}\lambda_{\boldsymbol{e}}\lambda_{\boldsymbol{f}}\lambda_{\boldsymbol{g}} = \sum_{\boldsymbol{d},\boldsymbol{e},\boldsymbol{f},\boldsymbol{g}} \lambda_{\boldsymbol{d}}\lambda_{\boldsymbol{e}}\lambda_{\boldsymbol{f}}\lambda_{\boldsymbol{g}} \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W \\ [d_i,e_i,f_i,g_i] \mid n+h_i \ \forall i}} 1.$$

Remembering that $\lambda_{d_1,\dots,d_k}$ vanishes unless $d_1 \cdots d_k$ is prime to W, we see that a quadruple $\boldsymbol{d}, \boldsymbol{e}, \boldsymbol{f}, \boldsymbol{g}$ makes no contribution to the right-hand side unless the numbers $[d_i, e_i, f_i, g_i]$, for $1 \le i \le k$, are pairwise coprime and all coprime to W. In that case, the conditions on n in the inner sum put n in a uniquely determined congruence class modulo $W \prod_{i=1}^k [d_i, e_i, f_i, g_i]$. It follows that our sum is bounded

above by

$$\sum_{\boldsymbol{d},\boldsymbol{e},\boldsymbol{f},\boldsymbol{g}} |\lambda_{\boldsymbol{d}}\lambda_{\boldsymbol{e}}\lambda_{\boldsymbol{f}}\lambda_{\boldsymbol{g}}|\left(\frac{N}{W\prod_{i=1}^{k}[d_i,e_i,f_i,g_i]}+1\right).$$

Let

$$r := \prod_{i=1}^{k}[d_i,e_i,f_i,g_i]. \tag{3-9}$$

Since $\lambda_{d_1,\dots,d_k}$ vanishes unless $d_1\cdots d_k$ is a squarefree integer smaller than R, we may restrict attention to squarefree $r < R^4$. Given r, there are $\tau_{15k}(r)$ choices of $\boldsymbol{d}$, $\boldsymbol{e}$, $\boldsymbol{f}$, and $\boldsymbol{g}$ giving (3-9). Hence, writing $\lambda_{\max} = \max_{d_1,\dots,d_k}|\lambda_{d_1,\dots,d_k}|$, we find that

$$\begin{aligned}&\sum_{\boldsymbol{d},\boldsymbol{e},\boldsymbol{f},\boldsymbol{g}} |\lambda_{\boldsymbol{d}}\lambda_{\boldsymbol{e}}\lambda_{\boldsymbol{f}}\lambda_{\boldsymbol{g}}|\left(\frac{N}{W\prod_{i=1}^{k}[d_i,e_i,f_i,g_i]}+1\right)\\ &\le \lambda_{\max}^4\sum_{r<R^4}\mu^2(r)\tau_{15k}(r)\left(\frac{N}{Wr}+1\right) \le \lambda_{\max}^4\left(\frac{N}{W}+R^4\right)\sum_{r<R^4}\frac{\mu^2(r)\tau_{15k}(r)}{r}.\end{aligned} \tag{3-10}$$

The remaining sum on r is bounded above by $\prod_{p<R^4}(1+15k/p) \ll (\log R)^{15k}$. Since $R = N^{\theta}$ with $\theta < \frac{1}{4}$ fixed, we get that $R^4 \ll N/W$. Finally, we note that $\lambda_{\max} \ll (\log R)^k$ (see [Maynard 2013, equations (5.9) and (6.3)], and recall that our implied constants may depend on F). Inserting these estimates into (3-10) gives the lemma. □

Proof that $\Sigma_2 = o\big((\varphi(W)^k/W^{k+1})N(\log N)^k\big)$. Let $\mathscr{Q}$ be the union of the sets $\mathscr{P}_q$ for $(\log N)^{100k} < q \le N^{1/2}(\log N)^{-100k}$. Then

$$\Sigma_2 = \sum_{\substack{N\le n<2N\\ n\equiv \nu \pmod W}} \chi_{\mathscr{Q}}(n+h_m)w(n).$$

Applying Cauchy–Schwarz and Lemma 3.5, we see that

$$\Sigma_2 \ll W^{-1/2}N^{1/2}(\log R)^{9.5k}\left(\sum_{\substack{N\le n<2N\\ n\equiv \nu \pmod W}} \chi_{\mathscr{Q}}(n+h_m)\right)^{1/2}. \tag{3-11}$$

The remaining sum on n is certainly bounded above by the total number of primes $p \in [N, 3N]$ belonging to $\mathscr{Q}$. For each such p, we may select a q with $(\log N)^{100k} < q \le N^{1/2}(\log N)^{-100k}$ for which (3-6) holds. Given q, we count the number of corresponding p using effective Chebotarev.

Since g is fixed and q is large, we see that $g \notin (\mathbb{Q}^{\times})^q$. So, by a theorem of Capelli on irreducible binomials, the extension $\mathbb{Q}(\sqrt[q]{g})/\mathbb{Q}$ has degree q. For later use, we note that the discriminant of $\mathbb{Q}(\sqrt[q]{g})$ divides $(gq)^q$ — so the only ramified primes

divide gq. By a theorem of Dedekind and Kummer, a prime $p \in [N, 3N]$ satisfies (3-6) precisely when p splits completely in $L := \mathbb{Q}(\zeta_q, \sqrt[q]{g})$. To continue, we need to know the degree of $L/\mathbb{Q}$. Now $\sqrt[q]{g}$ is not contained in $\mathbb{Q}(\zeta_q)$ — otherwise, $\sqrt[q]{g}$ would generate a Galois extension of $\mathbb{Q}$, contradicting that $\mathbb{Q}(\sqrt[q]{g})$ contains only a single q-th root of unity (since it can be viewed as a subfield of $\mathbb{R}$). So, by another application of Capelli's theorem,

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\zeta_q)] \cdot [\mathbb{Q}(\zeta_q) : \mathbb{Q}] = q(q-1).$$

Moreover, since q is the only ramified prime in $\mathbb{Q}(\zeta_q)/\mathbb{Q}$, the only primes that may ramify in $L/\mathbb{Q}$ all divide gq. By Lemma 2.4, $\log|\Delta_L| \ll q^2 \log(|g|q) \ll q^2 \log N$. We plug this estimate into Theorem 2.3, taking C as the conjugacy class of the identity. We find that the number of $p \in [N, 3N]$ for which (3-6) holds for a given q is

$$\frac{1}{q(q-1)} \int_N^{3N} \frac{dt}{\log t} + O(N^{1/2} \log N).$$

Summing this upper bound over primes q with $(\log N)^{100k} < q \le N^{1/2}(\log N)^{-100k}$, we get that the total number of these p is $O(N(\log N)^{-100k})$.

Now, referring back to (3-11), we see that $\Sigma_2 \ll W^{-1/2} N (\log N)^{-40k}$. But this is $o(N)$, and so certainly also $o\big((\varphi(W)^k/W^{k+1})N(\log N)^k\big)$. □

Proof that $\Sigma_4 = o\big((\varphi(W)^k/W^{k+1})N(\log N)^k\big)$. We proceed as above, but now with $\mathscr{Q}$ equal to the union of the sets $\mathscr{P}_q$ for $q > N^{1/2}(\log N)^{100k}$. We will show that $\#\mathscr{Q} \cap [N, 3N] \ll N(\log N)^{-200k}$. By the previous Cauchy–Schwarz argument, this is (more than) enough. If $p \in \mathscr{Q} \cap [N, 3N]$, then the order of g modulo p, call it ℓ, divides $(p-1)/q$ for some $q > N^{1/2}(\log N)^{100k}$. In particular, $\ell < 3N^{1/2}(\log N)^{-100k}$. Since $g^\ell - 1$ has only $O(\ell)$ prime factors, summing on $\ell < 3N^{1/2}(\log N)^{-100k}$ shows there are $O(N(\log N)^{-200k})$ possibilities for p. □

Estimation of Σ_3. For each prime q, we let $\mathscr{A}_q$ denote the set of natural numbers $n \equiv 1 \pmod q$. We estimate Σ_3 using the trivial bound $\chi_{\mathscr{P}_q} \le \chi_{\mathscr{A}_q}$. To save space, write $\mathscr{J} := (N^{1/2}(\log N)^{-100k}, N^{1/2}(\log N)^{100k}]$. Then

$$\Sigma_3 \le \sum_{q \in \mathscr{J}} \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W}} \chi_{\mathscr{A}_q}(n + h_m) w(n).$$

Expanding out the right-hand side yields

$$\sum_{q \in \mathscr{J}} \sum_{\substack{d_1, \dots, d_k \\ e_1, \dots, e_k}} \lambda_{d_1, \dots, d_k} \lambda_{e_1, \dots, e_k} \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W \\ [d_i, e_i] \mid n + h_i \ \forall i}} \chi_{\mathscr{A}_q}(n + h_m). \tag{3-12}$$

We can assume $d_1 \cdots d_k$ is a squarefree integer coprime to W and not exceeding R, since otherwise $\lambda_{d_1, \dots, d_k} = 0$. A similar assumption can be made for $e_1 \cdots e_k$. Since

$q \in \mathcal{J}$, it follows that q is coprime to each d_i and each e_i, and W. Now the innermost sum in (3-12) vanishes unless $[d_1, e_1], [d_2, e_2], \dots, [d_k, e_k]$, and W are pairwise coprime. Using a $'$ to denote this restriction on the d_i and e_i, we get that

$$\sum_{q\in\mathcal{J}} \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \sum_{\substack{N\le n<2N\\ n\equiv \nu \pmod W\\ [d_i,e_i]\mid n+h_i\ \forall i}} \chi_{\mathscr{A}_q}(n+h_m)$$

$$= \sum_{q\in\mathcal{J}} \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}}{}' \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}\left(\frac{N}{qW\prod_{i=1}^k [d_i,e_i]} + O(1)\right).$$

The error here is

$$\ll \left(\sum_{q\in\mathcal{J}} 1\right)\left(\sum_{d_1,\dots,d_k} |\lambda_{d_1,\dots,d_k}|\right)^2 \ll N^{1/2}(\log N)^{100k}\,\lambda_{\max}^2\left(\sum_{r<R}\mu^2(r)\tau_k(r)\right)^2.$$

Recalling that $\lambda_{\max} \ll (\log R)^k$ and that $\sum_{r<R}\tau_k(r) \ll R(\log R)^{k-1}$, our final O error term is $O(N^{1/2}R^2\cdot(\log N)^{104k})$. Since $R = N^\theta$ with $\theta < \frac{1}{4}$, this error is $o(N)$ and so is negligible for us.

We now turn to the main term, which has the form

$$\left(\sum_{q\in\mathcal{J}}\frac{1}{q}\right)\left(\frac{N}{W}\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}}{}' \frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^k [d_i,e_i]}\right).$$

The first factor here is $O(\log\log N/\log N)$, and so in particular is $o(1)$. Maynard's analysis (see the proofs of [Maynard 2013, Lemmas 5.1, 6.2]) shows that the second factor here satisfies the asymptotic formula asserted for S_1 in Proposition 3.1. Hence, $\Sigma_3 = o\big((\varphi(W)^k/W^{k+1})N(\log N)^k\big)$, as desired.

Estimation of Σ_1. For this case, let $\mathcal{J} := (\log\log\log N, (\log N)^{100k}]$. Using the bound $\chi_{\mathscr{P}_q} \le \chi_{\mathscr{P}_q^{(0)}}$, we get that

$$\Sigma_1 \le \sum_{q\in\mathcal{J}} \sum_{N\le n<2N} \chi_{\mathscr{P}_q^{(0)}}(n+h_m)w(n).$$

Expanding out the right-hand side gives

$$\sum_{q\in\mathcal{J}} \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \sum_{\substack{N\le n<2N\\ n\equiv \nu \pmod W\\ [d_i,e_i]\mid n+h_i\ \forall i}} \chi_{\mathscr{P}_q^{(0)}}(n+h_m). \tag{3-13}$$

The inner sum can be written as a sum over a single residue class modulo $f := W\prod_{i=1}^k [d_i,e_i]$, provided that $W, [d_1,e_1], \dots, [d_k,e_k]$ are pairwise coprime; otherwise we get no contribution. We also need that $n+h_m$ lies in a residue class coprime to f, which happens precisely when $d_m = e_m = 1$. Also, $\chi_{\mathscr{P}_q^{(0)}}(n+h_m)$

vanishes unless $q \mid n+h_m-1$, and this implies that the inner sum in (3-13) vanishes unless q is coprime to each d_i and e_i. Indeed, if q divides d_i or e_i without the inner sum vanishing, then $q \mid h_m - h_i - 1$. But that divisibility cannot hold for $q \in \mathcal{J}$, since $0 < |h_m - h_i - 1| < k \cdot K!$.

Thus, we only see a contribution to (3-13) if $[d_1, e_1]$, $[d_2, e_2]$, $\dots$, $[d_k, e_k]$, W, and q are pairwise coprime. Under these conditions, we claim that

$$\sum_{\substack{N\le n<2N\\ n\equiv \nu \pmod W\\ [d_i,e_i]\mid n+h_i\ \forall i}} \chi_{\mathscr{P}_q^{(0)}}(n+h_m) = \frac{1}{q(q-1)\varphi(W)\prod_{i=1}^k \varphi([d_i,e_i])}\int_{N+h_m}^{2N+h_m}\frac{dt}{\log t} + O(N^{1/2}\log N). \quad (3\text{-}14)$$

To see this, let $p := n + h_m$. Then the prime $p \in [N + h_m, 2N + h_m)$ makes a contribution to the left-hand sum precisely when Frob_p is a certain element of $\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$ — determined by the congruence conditions modulo the $[d_i, e_i]$ and W — *and* when p splits completely in $\mathbb{Q}(\zeta_q, \sqrt[q]{g})$. Now $\mathbb{Q}(\sqrt[q]{g}) \not\subset \mathbb{Q}(\zeta_{qf})$, since $\mathbb{Q}(\sqrt[q]{g})$ is not a Galois extension of $\mathbb{Q}$. Thus, letting $L := \mathbb{Q}(\zeta_{qf}, \sqrt[q]{g})$, we find that

$$[L:\mathbb{Q}] = [L:\mathbb{Q}(\zeta_{qf})][\mathbb{Q}(\zeta_{qf}):\mathbb{Q}] = q\cdot\varphi(qf) = q(q-1)\varphi(W)\prod_{i=1}^k \varphi([d_i,e_i]).$$

Hence, $\mathbb{Q}(\zeta_f)$ and $\mathbb{Q}(\zeta_q, \sqrt[q]{g})$ are linearly disjoint extensions of $\mathbb{Q}$ with compositum L. Our conditions on p amount to placing Frob_p in a certain uniquely determined conjugacy class of size 1 in $\mathrm{Gal}(L/\mathbb{Q})$. Since the only primes that ramify in L divide qfg, Lemma 2.4 gives that

$$\log|\Delta_L| \ll [L:\mathbb{Q}](\log(qfg) + \log[L:\mathbb{Q}]) \ll [L:\mathbb{Q}]\log N.$$

Inserting this estimate into Theorem 2.3 yields (3-14).

Returning now to (3-13), we see that the error term in (3-14) yields a total error of size

$$\ll N^{1/2}\log N\Big(\sum_{q\in\mathcal{J}} 1\Big)\Big(\sum_{d_1,\dots,d_k}|\lambda_{d_1,\dots,d_k}|\Big)^2$$

$$\ll N^{1/2}(\log N)^{100k+1}\lambda_{\max}^2\Big(\sum_{r<R}\tau_k(r)\Big)^2 \ll N^{1/2}R^2(\log N)^{104k+1}.$$

This is $o(N)$ and so is again negligible for us. Letting

$$X_N := \int_{N+h_m}^{2N+h_m}\frac{dt}{\log t},$$

the main term has the shape

$$\sum_{q\in\mathcal{P}}\frac{1}{q(q-1)}\left(\frac{X_N}{\varphi(W)}\sideset{}{'}\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ d_m=e_m=1}}\frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^k\varphi([d_i,e_i])}\right). \tag{3-15}$$

Here the $'$ on the sum indicates that $W, [d_1,e_1],\dots,[d_k,e_k]$, and q are pairwise coprime. Owing to the support of the λ's, this restriction on the sum has the same effect as requiring that $(d_i,e_j)=1$ for all $i\neq j$ and that $(d_i,q)=(e_j,q)=1$ for all $1\le i,j\le k$. We incorporate the restrictions that $(d_i,e_j)=1$ by multiplying through by $\sum_{s_{i,j}|d_i,e_j}\mu(s_{i,j})$ for $i\neq j$. Similarly, we incorporate the restrictions that $(d_i,q)=(e_j,q)=1$ by multiplying through by $\sum_{\delta_i|d_i,q}\mu(\delta_i)$ and $\sum_{\epsilon_j|e_j,q}\mu(\epsilon_j)$, for all pairs of i and j.

Let g be the completely multiplicative function defined by $g(p)=p-2$ for all primes p, and note that

$$\frac{1}{\varphi([d_i,e_i])}=\frac{1}{\varphi(d_i)\varphi(e_i)}\sum_{u_i|d_i,e_i}g(u_i)$$

for squarefree d_i and e_i. This allows us to rewrite the parenthesized portion of (3-15) as

$$\frac{X_N}{\varphi(W)}\sum_{u_1,\dots,u_k}\left(\prod_{i=1}^k g(u_i)\right)\sideset{}{^*}\sum_{s_{1,2},\dots,s_{k,k-1}}\left(\prod_{\substack{1\le i,j\le k\\ i\neq j}}\mu(s_{i,j})\right)\sum_{\substack{\delta_1,\dots,\delta_k|q\\ \epsilon_1,\dots,\epsilon_k|q}}\left(\prod_{i=1}^k\mu(\delta_i)\prod_{j=1}^k\mu(\epsilon_j)\right)$$
$$\times\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ u_i|d_i,e_i\ \forall i\\ s_{i,j}|d_i,e_j\ \forall i\neq j\\ \delta_i|d_i,\epsilon_j|e_j\ \forall i,j\\ d_m=e_m=1}}\frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^k\varphi(d_i)\varphi(e_i)}, \tag{3-16}$$

where the $*$ on the sum indicates that $s_{i,j}$ is restricted to be coprime to u_i, u_j, $s_{i,a}$, and $s_{b,j}$ for all $a\neq j$ and $b\neq i$. (The other values of $s_{i,j}$ make no contribution.) Introducing the new variables

$$y^{(m)}_{r_1,\dots,r_k}:=\left(\prod_{i=1}^k\mu(r_i)g(r_i)\right)\sum_{\substack{d_1,\dots,d_k\\ r_i|d_i\ \forall i\\ d_m=1}}\frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^k\varphi(d_i)},$$

we may rewrite (3-16) as

$$\frac{X_N}{\varphi(W)}\sum_{u_1,\dots,u_k}\Big(\prod_{i=1}^{k}g(u_i)\Big)\sideset{}{^*}\sum_{s_{1,2},\dots,s_{k,k-1}}\Big(\prod_{\substack{1\le i,j\le k\\ i\ne j}}\mu(s_{i,j})\Big)\sum_{\substack{\delta_1,\dots,\delta_k\mid q\\ \epsilon_1,\dots,\epsilon_k\mid q}}\Big(\prod_{i=1}^{k}\mu(\delta_i)\prod_{j=1}^{k}\mu(\epsilon_j)\Big)$$
$$\times\Big(\prod_{i=1}^{k}\frac{\mu(a_i)}{g(a_i)}\Big)\Big(\prod_{j=1}^{k}\frac{\mu(b_j)}{g(b_j)}\Big)y^{(m)}_{a_1,\dots,a_k}y^{(m)}_{b_1,\dots,b_k},$$

where $a_i=\operatorname{lcm}\big[u_i\prod_{j\ne i}s_{i,j},\delta_i\big]$ and $b_j=\operatorname{lcm}\big[u_j\prod_{i\ne j}s_{i,j},\epsilon_j\big]$. Define $\delta_i'\in\{1,q\}$ and $\epsilon_j'\in\{1,q\}$ by the equations

$$a_i=\Big(u_i\prod_{j\ne i}s_{i,j}\Big)\delta_i',\quad b_j=\Big(u_j\prod_{i\ne j}s_{i,j}\Big)\epsilon_j'.$$

Exploiting coprimality, we can write $\mu(a_i)=\big(\mu(u_i)\prod_{j\ne i}\mu(s_{i,j})\big)\mu(\delta_i')$, and similarly for $\mu(b_j)$, $g(a_i)$, and $g(b_j)$. This transforms (3-16) into

$$\frac{X_N}{\varphi(W)}\sum_{u_1,\dots,u_k}\Big(\prod_{i=1}^{k}\frac{\mu(u_i)^2}{g(u_i)}\Big)\sideset{}{^*}\sum_{s_{1,2},\dots,s_{k,k-1}}\Big(\prod_{\substack{1\le i,j\le k\\ i\ne j}}\frac{\mu(s_{i,j})}{g(s_{i,j})^2}\Big)$$
$$\times\sum_{\substack{\delta_1,\dots,\delta_k\mid q\\ \epsilon_1,\dots,\epsilon_k\mid q}}\Big(\prod_{i=1}^{k}\frac{\mu(\delta_i)\mu(\delta_i')}{g(\delta_i')}\prod_{j=1}^{k}\frac{\mu(\epsilon_j)\mu(\epsilon_j')}{g(\epsilon_j')}\Big)y^{(m)}_{a_1,\dots,a_k}y^{(m)}_{b_1,\dots,b_k}.$$

Let $y^{(m)}_{\max}=\max_{r_1,\dots,r_k}\big|y^{(m)}_{r_1,\dots,r_k}\big|$. From [Maynard 2013, equation (6.10)], we have $y^{(m)}_{\max}\ll(\varphi(W)/W)\log R$. Inserting these bounds into the previous display, we find that (3-16) is

$$\ll\frac{X_N}{\varphi(W)}\Big(\sum_{\substack{u<R\\ \gcd(u,W)=1}}\frac{\mu(u)^2}{g(u)}\Big)^{k-1}\Big(\sum_{s}\frac{\mu(s)^2}{g(s)^2}\Big)^{k(k-1)}{y^{(m)}_{\max}}^2$$
$$\ll\frac{X_N}{\varphi(W)}\Big(\frac{\varphi(W)}{W}\Big)^{k+1}(\log R)^{k+1}\ll\Big(\frac{\varphi(W)^k}{W^{k+1}}\Big)N(\log N)^k.$$

We used here that there are only $O(1)$ possibilities for the δ_i and ϵ_j, and that for each of these, $\prod_i(1/g(\delta_i'))\prod_j(1/g(\epsilon_j'))\le 1$. Referring back to (3-15), we see that our original main term contributes

$$\ll\Big(\frac{\varphi(W)^k}{W^{k+1}}\Big)N(\log N)^k\sum_{q\in\mathcal{Y}}\frac{1}{q(q-1)}=o\Big(\frac{\varphi(W)^k}{W^{k+1}}N(\log N)^k\Big),$$

as desired.

Remark. The truth of Theorem 1.1 could also have been predicted on heuristic grounds. Indeed, there are well-known heuristics for Artin's primitive root conjecture, suggesting even the "correct" value of c_g (see [Moree 2012, §§2–5]), as well as heuristics for the prime k-tuples conjecture (see, for instance, [Crandall and Pomerance 2005, pp. 14–15]), and these can be fitted together. As an example, this combined heuristic suggests that the count of twin prime pairs p, $p+2$ with $p \le x$ and with 2 a primitive root of both p and $p+2$ should be approximately

$$\mathfrak{S} \int_2^x \frac{dt}{(\log t)^2}, \quad \text{where } \mathfrak{S} := \frac{1}{4} \prod_{p>3} \left(1 - \frac{3}{(p-1)^2}\right).$$

Quantitative conjectures of this kind, but in the context of primes represented by a single irreducible polynomial rather than primes produced by linear forms, appear in recent work of Moree [2007] and of Akbary and Scholten [2013].

4. Concluding remarks

We conclude with a proof of the following result, which seems of independent interest:

Theorem 4.1 (conditional on GRH). *Fix an integer $g \neq -1$ and not a square. For every positive integer m, there are m consecutive primes all of which possess g as a primitive root.*

Theorem 4.1 might be compared with Shiu's celebrated result [2000] that each coprime residue class $a \bmod q$ contains arbitrarily long runs of consecutive primes. Our proof of Theorem 4.1 is similar in spirit to a short proof of Shiu's theorem recently given by Banks, Freiberg, and Turnage-Butterbaugh [Banks et al. 2013].

It will be useful to first translate the proof of Theorem 1.1 into probabilistic terms. Let k be a fixed positive integer, and let $h_1, \dots, h_k$ be given by (3-2). We view the set of $n \in [N, 2N)$ with $n \equiv \nu \pmod W$ as a finite probability space where the probability mass at each n_0 is given by

$$w(n_0) \Big/ \sum_{\substack{N \le n < 2N \\ n \equiv \nu \pmod W}} w(n).$$

Here the weights $w(n)$ are assumed to be of the form specified in Proposition 3.1. Introduce the random variables

$$X := \sum_{i=1}^k \chi_{\mathscr{P}}(n+h_i) \quad \text{and} \quad Y := \sum_{i=1}^k \chi_{\mathscr{P}\setminus\widetilde{\mathscr{P}}}(n+h_i).$$

Then $\mathbb{E}[X] = S_2/S_1$. Given suitable parameters F and θ, Proposition 3.1 gives us the limiting value of $\mathbb{E}[X]$ as $N \to \infty$. Combining Propositions 3.1 and 3.2, we see

that for k large enough in terms of m, we can choose parameters so this limiting value exceeds $m-1$. On the other hand, it was shown in Section 3 that (with the same choice of parameters) $\mathbb{E}[Y] = o(1)$ as $N \to \infty$. Thus, $\mathbb{E}[X-Y] > m-1$ for all large N. But $X - Y = \sum_{i=1}^{m} \chi_{\widetilde{\mathscr{P}}}(n+h_i)$. Hence, for some $n \in [N, 2N)$, the list $n+h_1, \dots, n+h_k$ contains at least m primes having g as a primitive root. Theorem 1.1 follows, with $C_m = h_k - h_1$.

We now present the minor variation of this argument needed to establish Theorem 4.1.

Proof of Theorem 4.1. Given m, we fix a large enough value of k (and parameters F and θ) so that the limiting value of $\mathbb{E}[X]$ exceeds $m-1$. Then, for all large N,

$$\Pr(X \geq m) \geq \mathbb{E}\Big[\frac{X-(m-1)}{k}\Big] = \frac{1}{k}(\mathbb{E}[X] - (m-1)) \gg 1.$$

Note that $\Pr(Y > 0) \leq \mathbb{E}[Y] = o(1)$, as $N \to \infty$. So, for large N, there is a positive probability that both $X \geq m$ and $Y = 0$. This allows us to select $n \in [N, 2N)$ with $n \equiv \nu \pmod{W}$ satisfying

(i) at least m of $n+h_1, \dots, n+h_k$ are prime,

(ii) all of the primes among $n+h_1, \dots, n+h_k$ possess g as a primitive root.

We will argue momentarily that we can also assume

(iii) the only primes in the interval $[n+h_1, n+h_k]$ are the primes in the list $n+h_1, \dots, n+h_k$.

From (i), (ii), and (iii), we see that the set of primes in $[n+h_1, n+h_k]$ contains at least m elements, all of which have g as a primitive root. Theorem 4.1 follows.

In order to show we may assume (iii), we tweak the choice of the residue class ν mod W from which n is sampled. In the proof of Lemma 3.3, we chose ν_1 as any odd integer avoiding $-h_1, \dots, -h_k, 1-h_1, \dots, 1-h_k$ modulo p, for all odd $p \leq \log\log\log N$ not dividing D_1. We now add an extra condition on ν_1. Choose distinct primes $p^{(h)} \in [\frac{1}{2}\log\log\log N, \log\log\log N)$ for all even $h \in [h_1, h_k] \setminus \mathscr{H}$. We add the requirement that $\nu_1 \equiv -h \pmod{p^{(h)}}$ for each such h. This is consistent with our earlier restrictions, since h is not congruent modulo $p^{(h)}$ to any of $h_1, \dots, h_k$ (since $h \notin \mathscr{H}$) or to any of $h_1 - 1, \dots, h_k - 1$ (since h and the h_i are all even). Using the resulting value of ν from Lemma 3.3, we see that for even $h \in [h_1, h_k] \setminus \mathscr{H}$, we have $p_h \mid n+h$ whenever $n \equiv \nu \pmod{W}$. For all odd $h \in [h_1, h_k]$, we have trivially that $2 \mid n+h$ whenever $n \equiv \nu \pmod{W}$. Thus, $n+h$ is composite if $h \in [h_1, h_k] \setminus \mathscr{H}$, and so (iii) holds. □

Acknowledgement

The author thanks the referee for a careful reading of the manuscript.

References

[Akbary and Scholten 2013] A. Akbary and K. Scholten, "Artin prime producing polynomials", preprint, 2013. To appear in *Math. Comp.* arXiv 1310.5198

[Banks et al. 2013] W. D. Banks, T. Freiberg, and C. L. Turnage-Butterbaugh, "Consecutive primes in tuples", preprint, 2013. To appear in *Acta Arith.* arXiv 1311.7003

[Crandall and Pomerance 2005] R. Crandall and C. Pomerance, *Prime numbers: A computational perspective*, 2nd ed., Springer, New York, 2005. MR 2006a:11005 Zbl 1088.11001

[Gupta and Murty 1984] R. Gupta and M. R. Murty, "A remark on Artin's conjecture", *Invent. Math.* **78**:1 (1984), 127–130. MR 86d:11003 Zbl 0549.10037

[Heath-Brown 1986] D. R. Heath-Brown, "Artin's conjecture for primitive roots", *Quart. J. Math. Oxford Ser.* (2) **37**:145 (1986), 27–38. MR 88a:11004 Zbl 0586.10025

[Hooley 1967] C. Hooley, "On Artin's conjecture", *J. Reine Angew. Math.* **225** (1967), 209–220. MR 34 #7445 Zbl 0221.10048

[Hooley 1976] C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge Tracts in Mathematics **70**, Cambridge University Press, 1976. MR 53 #7976 Zbl 0327.10044

[Lagarias and Odlyzko 1977] J. C. Lagarias and A. M. Odlyzko, "Effective versions of the Chebotarev density theorem", pp. 409–464 in *Algebraic number fields: L-functions and Galois properties* (Durham, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR 56 #5506 Zbl 0362.12011

[Li and Pan 2014] H. Li and H. Pan, "Bounded gaps between primes of the special form", preprint, 2014. arXiv 1403.4527

[Maynard 2013] J. Maynard, "Small gaps between primes", preprint, 2013. To appear in *Ann. Math.* arXiv 1311.4600v2

[Moree 2007] P. Moree, "Artin prime producing quadratics", *Abh. Math. Sem. Univ. Hamburg* **77** (2007), 109–127. MR 2008m:11194 Zbl 1214.11107

[Moree 2012] P. Moree, "Artin's primitive root conjecture—a survey", *Integers* **12**:6 (2012), 1305–1416. MR 3011564 Zbl 1271.11002

[Serre 1981] J.-P. Serre, "Quelques applications du théorème de densité de Chebotarev", *Inst. Hautes Études Sci. Publ. Math.* 54 (1981), 323–401. MR 83k:12011 Zbl 0496.12011

[Shiu 2000] D. K. L. Shiu, "Strings of congruent primes", *J. London Math. Soc.* (2) **61**:2 (2000), 359–373. MR 2001f:11155 Zbl 0973.11083

[Thorner 2014] J. Thorner, "Bounded gaps between primes in Chebotarev sets", *Res. Math. Sci.* **1**:4 (2014), 1–16.

[Wan 1997] D. Wan, "Generators and irreducible polynomials over finite fields", *Math. Comp.* **66**:219 (1997), 1195–1212. MR 97j:11060 Zbl 0879.11072

Communicated by Andrew Granville
Received 2014-04-27 Revised 2014-06-21 Accepted 2014-07-19

pollack@uga.edu *Department of Mathematics, University of Georgia, Boyd Graduate Studies Building, Athens, GA 30602, United States*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2014 is US $225/year for the electronic version, and $400/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 8 No. 7 2014