Relevance of the Residue Class to the Abundance of Primes

John B. Friedlander* and Andrew Granville

1. For q a positive integer, one sees immediately that, apart from those (finite number) which divide q, the primes are found within the $\phi(q)$ ″reduced″ residue classes modulo q, that is those consisting of integers a relatively prime to q. The question of how these primes are distributed within those classes is one of the central problems in analytic number theory.

It was proved by Dirichlet that each reduced class contains infinitely many primes and by de la Vallée - Poussin that each such class contains asymptotically the same proportion of the total, a fact we shall express in the slightly stronger form

$$|\psi(x;q,a) - x/\phi(q)| \ll x\log^{-A} x \tag{1.1}$$

where A is arbitrary and

$$\psi(x;q,a) = \sum_{\substack{p^m \le x \\ p^m \equiv a (\mathrm{mod}\ q)}} \log p\ .$$

The question of the range of uniformity for which (1.1) may be shown to hold is one of intrinsic interest and of importance for numerous applications. Unfortunately this result has been verified only under the rather severe restriction (Siegel-Walfisz Theorem) that q be bounded above by a fixed power of $\log x$. Much more than this is expected and differing degrees of optimism have led to the conjectures that the restriction $q < \log^N x$ can be relaxed to (A) $q < x^{1/2-\varepsilon}$ (which would follow from the Generalized Riemann Hypothesis), (B) $q < x^{1-\varepsilon}$ (which is probably true but presently unapproachable), and (C) $q < x\log^{-B} x$ (which has recently [FG] been disproved).

* Partially supported by NSERC grant A5123.

For many applications it is sufficient to have knowledge of (1.1) in a certain averaged sense and the estimate (Bombieri-Vinogradov Theorem)

$$\sum_{q\sim Q} \max_{(a,q)=1} |\psi(x;q,a) - x/\phi(q)| \ll x \log^{-A} x, \tag{1.2}$$

where $q \sim Q$ means $Q < q \leq 2Q$, is known to hold [Bo] under the much weaker restriction $Q < x^{1/2} \log^{-B} x$, $B = B(A)$, than is required in the Siegel-Walfisz Theorem.

In both of the above theorems the emphasis has been on the size of the integer q, the role of the integer a being insignificant, beyond the trivial fact that it is required to be coprime to q. The attempts to further relax the restriction on Q in (1.2) have not succeeded but have led instead to consideration of the easier problem of bounding the sum $\sum_{\substack{q\sim Q \\ (q,a)=1}} |\psi(x;q,a) - x/\phi(q)|$ or the more general weighted sum,

$$\sum_{\substack{q\sim Q \\ (q,a)=1}} \gamma_q(\psi(x;q,a) - x/\phi(q)) \tag{1.3}$$

which may be attacked with greater success and where now the methods lead to statements in which the integer a plays some non-trivial role. We note that in some applications (e.g. twin primes) a may be taken to be fixed, whereas in others (e.g. Goldbach type problems) a is rather large.

As the problem of bounding the sums (1.1), (1.2), (1.3) grows progressively easier, so the conjectures about the admissible size of q in (1.1) lead to corresponding weaker conjectures about the sums (1.2) and (1.3), (A) being true by virtue of the Bombieri-Vinogradov Theorem, (B) being in doubt, and (C) being false, at least for (1.2), by [FG]. In recent work [FGHM] limits were found to the size of q (resp. Q) for which good upper bounds could hold for the above sums. These lower bounds were highly sensitive to the integer a and indicate that, for a given upper bound, say to (1.3), the maximum allowable Q may well depend on a in some significant manner. For most of the interesting sets of weights γ_q, for example the sum of absolute values, the known upper bounds are far too weak for this phenomenon to be directly verified. In one special case however, namely when γ_q is identically one (a case which is of interest in part by virtue of its relation to the Titchmarsh divisor problem), it is possible to establish upper and lower bounds which are sufficiently close together that some dependence on a may be explicitly exhibited. Such is our purpose here.

The upper bound, which occurs in only slightly weaker forms in [BFI,Fo_1,FGHM] is given by

Theorem 1: *Let $\varepsilon > 0, A > 0$ be given. Then uniformly for $0 < |a| < x^{1/4-\varepsilon}, 2 \le Q \le x/3$ we have*

$$(1.4) \qquad \sum_{\substack{q\sim Q \\ (q,a)=1}} (\psi(x;q,a) - x/\phi(q)) \underset{\varepsilon,A}{\ll} 2^{\nu(a)} Q \log\log(x/Q) + x\log^{-A} x + Q\log|a|$$

where $\nu(a)$ is the number of distinct prime factors of a.

Remarks:

(I) If a is not a prime power the term $Q\log|a|$ may be deleted.

(II) If Q is not in the interval $[x^{1/2-\varepsilon}, x^{1/2+\varepsilon}]$ then the restriction $|a| < x^{1/4-\varepsilon}$ may be relaxed to $|a| < x^A$.

(III) If Q is not in the interval $[x^{1/2-\varepsilon}, x^{1/2+\varepsilon}]$ and one assumes the Generalized Riemann Hypothesis then the error term $x\log^{-A} x$ may be replaced by $x^{1-\varepsilon/2}$.

The main difference between this and the earlier versions is the wider range of a, which previously had been required ([BFI],[Fo_1],[Fo_2]) to at least satisfy $|a| < \log^A x$. In fact, in virtually all of the previous upper bound results concerning the more general sum (1.3), a may be taken as large as x^δ for some small fixed δ depending on the set of weights. Thus, for instance, in the case of the Iwaniec well-factorable weights of sieve theory [BFI, Theorem 10] one may take any $\delta < 1/28$ and still obtain the result for any $Q < x^{4/7-\varepsilon}$. In §2 we indicate how the proof in [BFI] may be modified to give Theorem 1.

It is not however the size of a which seems to limit the parameter Q in bounding (1.3) but rather the arithmetic structure, more specifically the number of prime factors of a. The lower bound we give follows from a simple modification of Theorem A3 of [FGHM].

Theorem 2: *Let $\varepsilon > 0$. Then, for some $c > 0$, for all $x \geq x_0(\varepsilon)$, for all Q^* satisfying*

$$x\ \exp(-c\sqrt{\log x}) < Q^* \ \leq\ x/(\log x)^{1+\varepsilon}$$

and all ν satisfying

$$(1.5) \qquad (\log\log x)^{6/5+\varepsilon} < \nu \leq \exp((\log(x/Q^*))^{1/2-\varepsilon})$$

there exists Q with $Q^*/2 < Q \leq 2Q^*$ and an integer a with $\nu/2 < \nu(a) \leq 2\nu$ and $|a| < x$, such that

$$(1.6) \qquad \left| \sum_{\substack{q\sim Q \\ (q,a)=1}} \psi((x;q,a) - x/\phi(q)) \right| \ \geq\ \frac{x}{\log\log x}(x/Q)^{-(1+\varepsilon)\delta}$$

where $\delta = \log(\log(x/Q)/\log\nu)/\log\nu$. In case the Riemann Hypothesis is assumed the constant $6/5+\varepsilon$ in (1.5) can be replaced by $1+\varepsilon$.

By combining Theorems 1 and 2 we get results of the following type.

Corollary 1: *Fix $A > 1, M > 1, \varepsilon > 0$.*

(I) *For some B (depending on A and M) and all large x the estimate*

$$(1.7) \qquad \left| \sum_{\substack{q\sim Q \\ (q,a)=1}} (\psi(x;q,a) - x/\phi(q)) \right| < x\log^{-A} x$$

holds for every $Q < x \log^{-B} x$ *and every* $a,\ 0 < |a| < x$ *provided that*

$$\nu(a) < M \log\log x.$$

(II) *For every* B *and all large* x *the estimate*

$$\left| \sum_{\substack{q \sim Q \\ (q,a)=1}} (\psi(x;q,a) - x/\phi(q)) \right| < x \log^{-A} x \tag{1.7}$$

fails for some $Q < x \log^{-B} x$ *and some* $a,\ 0 < |a| < x$ *satisfying*

$$\nu(a) < (\log\log x)^{6/5+\varepsilon}.$$

In case the Riemann Hypothesis is assumed, $6/5 + \varepsilon$ *may be replaced by* $1 + \varepsilon$.

Since, for most a with $0 < |a| < x$, we have $\nu(a) < (1+\varepsilon)\log\log x$, it is the first case of the Corollary that applies to most a.

Especially in case the Riemann Hypothesis is assumed, we are thus able to say fairly precisely how large $\nu(a)$ must be before the estimate (1.7) begins to fail for Q in the given range. This gap could probably be further narrowed and it would be of some interest to do so.

If Q is taken somewhat smaller the corresponding results have less precision. Thus we have:

Corollary 2: *Assume the Generalized Riemann Hypothesis. Let* $\varepsilon > 0, \frac{1}{2} < \alpha < 1$. *Then for all large* x,

(I) *the estimate*

$$\left| \sum_{\substack{q \sim Q \\ (q,a)=1}} (\psi(x;q,a) - x/\phi(q)) \right| < x(Q/x)^{\alpha} \tag{1.8}$$

holds for every $Q < x/\exp(\log^{\alpha-\varepsilon} x)$ *and every* $a,\ 0 < |a| < x$ *provided that*

$$\nu(a) \ < \ (1-\alpha)\log(x/Q)\ .$$

(II) *the estimate* (1.8) *fails for some* $Q < x/\exp(\log^{\alpha-\varepsilon} x)$ *and some* $a,\ 0 < |a| < x$ *satisfying*

$$\nu(a) \ < \ \log^{1/\alpha+\varepsilon}(x/Q).$$

Finally we mention that, while attending the extremely enjoyable Amalfi Symposium, the authors succeeded in proving (to appear in Comp. Math.) that even for a fixed (indeed for any fixed non-zero integer a) the inequality (1.1) and even the asymptotic formula itself will fail to hold uniformly in the range $q < x\log^{-N} x$. The corresponding problem for the sum (1.3) with absolute values remains open.

2. The proofs of Corollaries 1 and 2 are immediate. The proof of Theorem 2 is, as already indicated, essentially that of Theorem A3 of [FGHM]. We merely do not specify the choice $z = \frac{1}{2}\log x$ as there but rather keep z free subject to the restrictions there imposed by Theorem B3; this in turn leads to the bounds for ν specified here in (1.5).

The only proof that requires more detailed comment is that of Theorem 1 and here too the only point we belabour is how the restriction a fixed in Theorem 9 of [BFI] may be relaxed to $|a| < x^{1/4-\varepsilon}$ in case $Q < x^{1/2+\delta}$. The remainder of the argument then follows as in the proof of Proposition 2.1 of [FGHM].

We begin as in §15 of [BFI]. It suffices to obtain a bound of the type

$$\sum_{\substack{q\sim Q\\ (q,a)=1}} \Big(\sum_{\substack{n\sim x\\ n\equiv a(q)}}{}^{*} \ \Lambda(n) \ - \ \frac{1}{\phi(q)} \sum_{\substack{n\sim x\\ (n,q)=1}}{}^{*} \ \Lambda(n)\Big) \ \ll \ x\log^{-A} x$$

where Σ^* indicates that the summation is restricted to integers having no prime factors less than $\exp(\log x/(\log\log x)^2)$.

We apply a special case of the Heath-Brown identity

$$\Lambda(n) \ = \ \sum_{j=1}^{7}(-1)^{j-1}\binom{7}{j} \sum\cdots\sum_{m_1,\cdots,m_j\le x^{1/7}} \mu(m_1)\cdots\mu(m_j) \sum\cdots\sum_{n_1\cdots n_j m_1\cdots m_j=n} \log n_1$$

valid for $n < 2x$. Following a splitting up argument we reduce the problem to the estimation of sums of the type

(2.1)

$$\sum_{\substack{q\sim Q\\(q,a)=1}}\left(\sideset{}{^*}\sum\cdots\sideset{}{^*}\sum_{\substack{m_1\cdots m_j n_1\cdots n_j\equiv a(q)\\ m_i\epsilon\mathcal{M}_i,n_i\epsilon\mathcal{N}_i}}\mu(m_1)\cdots\mu(m_j)-\frac{1}{\phi(q)}\sideset{}{^*}\sum\cdots\sideset{}{^*}\sum_{\substack{(m_1\cdots m_j n_1\cdots n_j,q)=1\\ m_i\epsilon\mathcal{M}_i,n_i\epsilon\mathcal{N}_i}}\mu(m_1)\cdots\mu(m_j)\right).$$

Here $\mathcal{M}_i, \mathcal{N}_i$ are intervals of the type $((1-\Delta)M_i, M_i]$, $((1-\Delta)N_i, N_i]$ with $\Delta = \log^{-B} x$ for a suitable B, and $M_i = x^{\mu_i}$, $N_i = x^{\nu_i}$ with

$$(2.2)\qquad 0\le\mu_j\le\cdots\le\mu_1\le 1/7,\ 0\le\nu_j\le\cdots\le\nu_1,\ \mu_1+\cdots+\mu_j+\nu_1+\cdots+\nu_j=1.$$

We require to show that every sum (2.1) in the range (2.2) may be given an upper bound $\ll x\log^{-A}x$ for arbitrary A.

We note that the above multiple sums may be transformed into bilinear or trilinear forms by grouping together the intervals $\mathcal{M}_1,\cdots,\mathcal{M}_j,\mathcal{N}_1,\cdots,\mathcal{N}_j$ into two or three disjoint sets, the coefficients of the resulting form being convolutions of the Möbius function and the constant function one.

As in the proof of the corresponding Theorem 9 of [BFI,§16] we consider two different cases for the sums (2.1).

Case I: There exists a partial sum, say λ, of (2.2) with $\varepsilon<\lambda<\frac{1}{4}+\varepsilon$.

In [BFI] this case was treated by Theorem 6 of that paper. An examination of the proof of that result shows that it is easily modified to give the following version which is uniform in a. (Unfortunately, to avoid introducing a considerable amount of notation and assumptions we shall have to refer the reader to [BFI].)

Theorem 6′: *Under the assumptions of* [BFI, *Theorem* 6, §13], *the conclusion holds uniformly for* $0<|a|<x^{1/3}$ *provided that*

$$(2.3)\qquad x^{\varepsilon}R<N<x^{-\varepsilon}\min\{(x/R)^{1/3},(x^2/|a|Q^2R)^{1/3}\}.$$

In the case of our application we have $R = 1$ and $Q < x^{1/2+\varepsilon}$. We choose $N = x^{\lambda}$; in view of the restriction $|a| < x^{1/4-\varepsilon}$, this choice satisfies (2.3). (Note that the precise meaning of ε is changing from one line to the next.)

Case II: There does not exist any partial sum of (2.2) with $\varepsilon < \lambda < 1/4 + \varepsilon$.

In this remaining case, we see that the terms of (2.2) which are $\leq \varepsilon$ give in total, say τ, where $\tau \leq \varepsilon$. Of course τ contains all $\mu_1, \cdots, \mu_j$ and possibly some ν_i. It follows that (2.2) can be partitioned as follows:

$$\nu_1 + \cdots + \nu_k + \tau \;=\; 1$$

with $\nu_1 \geq \cdots \geq \nu_k \geq 1/4 + \varepsilon,\ \varepsilon \geq \tau$. This implies that $1 \leq k \leq 3$.

In [BFI,§16] this case was treated by Theorem 7^* of that paper. As with Theorem 6 above, it is not difficult to modify Theorem 7^* so as to obtain a version uniform in a. However, when used to complete the proof of our current Theorem 1, this result would require a more severe restriction on the size of a. We avoid this by appealing instead to Lemma 2^* of [BFI_2]. Lemma 2^* is stated on p. 365; its application to Case II here is identical with its application there to Case 5, p. 392.

References

[Bo] E. Bombieri, On the large sieve, Mathematatika, 12 (1965) 201-225.

[BFI] E. Bombieri, J.B. Friedlander and H. Iwaniec, Primes in arithmetic progressions to large moduli, Acta Math. 156 (1986) 203-251.

[BFI_2] ____________,____________ II, Math. Ann. 277 (1987) 361-393.

[Fo_1] E. Fouvry, Sur le problème des diviseurs de Titchmarsh, J. Reine Angew. 357 (1985) 51-76.

[Fo_2] E. Fouvry, Autour du théorème de Bombieri-Vinogradov II, Ann. Sci. École Norm. Sup. (4) 20 (1987) 617-640.

[FG] J. Friedlander and A. Granville, Limitations to the equi-distribution of primes I, Ann. Math. 129 (1989) 363-382.

[FGHM] J. Friedlander, A. Granville, A. Hildebrand and H. Maier, Oscillation theorems for primes in arithmetic progressions and for sifting functions, to appear.

[Ma] H. Maier, Primes in short intervals, Michigan Math. J., 32 (1985) 221-225.

Scarborough College, University of Toronto

Institute for Advanced Study, Princeton