Collaborative Research:
Distribution of multiplicative functions and primes

1. Mean Values of Multiplicative functions

A central theme of multiplicative number theory is the estimation of mean-values of multiplicative functions. Many of the main results and conjectures of number theory can be viewed as results and conjectures on this kind of question, indeed everything from the Riemann Hypothesis, to the recently proved Taniyama Conjecture, to the mysterious eigenvalue distribution problems of Sato-Tate and Lang-Trotter, and recently to the growing circle of ideas in quantum chaos. Rather than focusing on these applications we are more interested in building a general body of theory, which may lead to proofs of some of the outstanding questions in the area. Although the task of building a general body of theory has been around for a long time there have been several interesting recent advances that lead one to believe that significant progress may soon be made on the central problems of the field.

We describe below some of these recent advances. The PIs have been involved in several of these new directions (and thus the "results from prior NSF support" are mixed into the text below) and, as we shall describe, we have plans to go further. By collaborating we hope that we will be able to combine some of these methods and move forward in new ways.

1a. The absolute value of the mean value.

Unless otherwise stated we assume that f is a multiplicative function with $|f(n)| \le 1$ for all n. It is easy to show that

$$\sum_{n\le x} f(n) \sim c_f x$$

where

$$c_f = \prod_p (1-1/p)(1+f(p)/p+f(p^2)/p^2+f(p^3)/p^3)+\dots),$$

if $\sum_p (1-\Re f(p))/p$ converges; but what if this sum diverges? In 1967 Wirsing showed the remarkable result that if f is real-valued then, in this case, $\sum_{n\le x} f(n) = o(x)$. However Wirsing's result does not directly generalize to the complex case, for in the example $f(n) = n^{it}$ we have $(1/x)\sum_{n\le x} f(n)$ does not converge while $\sum_p (1-\Re f(p))/p$ diverges. In 1975 Halasz showed the beautiful, unexpected result that the above provides, essentially, the only counterexample to generalizing Wirsing's Theorem. More precisely that if $\sum_p (1-\Re(f(p)/p^{it}))/p$ diverges *for every real* t, then $\sum_{n\le x} f(n) = o(x)$. Halasz also provided an quantitative version of his result, and there has been considerable subsequent effort dedicated to giving a "best possible" version. Moreover several important technical tools of analytic number theory (such as the Halasz-Montgomery lemma) were created for this quest. In recent work, Granville and Soundararajan have (for the first time) made the main term in such results entirely explicit, and showed that these are best possible up to

a factor of 10 (as a function of $\min_{t\le T}\sum_{p\le x}(1-\Re(f(p)/p^{it}))/p$). This should be quite valuable in applications of this result.

The function used in the above upper bound is hard to compute. It has become traditional to try to give bounds in terms of the more accessible $\sum_{p\le x}(1-\Re f(p))/p$. In order to get interesting results in this case we now restrict $f(p)$ to be in a closed convex subset S of the unit circle. Granville and Soundararajan have (for the first time) made the main term in such results, and Hall has shown that such results would be best possible up to a constant. Again this is useful for applications, for example in hybrid sieve problems. In [GS5] they gave, for each integer $m \ge 2$ a constant $\pi_m > 0$ such that if x is sufficiently large then, for any prime p, there are at least $\pi_m x$ integers $n \le x$ for which n is an mth power residue mod p.

1b. Determining mean values.

In the literature there seem to be two situations in which authors have been able to determine the mean values of multiplicative functions:

• When there is sufficient convergence (as above) so that the mean value is asymptotically equal to the Euler product

$$\prod_{p\le x}(1-1/p)(1+f(p)/p+f(p^2)/p^2+\dots).$$

• When the values of f are very special and the function can be "modeled" by an integral delay equation. The best known example is where $f(p)=1$ for all $p\le y$ and $f(p)=0$ otherwise, and the mean value is $\sim \rho(u)$ where $x=y^u$ (in an appropriate range), and $\rho(u)=1$ for $u\le 1$, with $\rho(u)=(1/u)\int_0^1 \rho(u-t)dt$ for $u>1$.

Most research in the subject has focussed on getting sharp error terms in examples of the above two cases, sometimes for fascinating applications (especially in certain sieve problems), sometimes for the sake of it (which is not very often interesting), and sometimes because a sharp enough error term would imply the Riemann Hypothesis. As we shall explain in the next subsection, it has recently been shown how mean values, in typical questions, can be broken as the product of two mean values, one of each of the two types above.

1c. Mean values in the complex plane.

A question of longstanding interest has been to determine, for a given closed convex subset S of the unit circle, the "spectrum", $\Gamma(S)$, of possible mean-values $(1/x)\sum_{n\le x} f(n)$ in the complex plane, where we restrict each $f(p)\in S$. Perhaps due to the fact that so little was known on explicit versions of Halasz's theorem, this sort of problem often came up but there seem to be few results on it in the literature (except if $S=[0,1]$). The "main result" of [GS4] is that mean values can be determined for *all* $f\in\mathcal{F}(S)$ (where $\mathcal{F}(s)$ is the set of multiplicative functions f such that $f(p)\in S$ for all primes p), and asymptotically equal the product of such an Euler product and the value of the solution to such an integral delay equation (essentially we use the Euler product for the "contribution" of the "small" primes, and the delay equation for the contribution of the "large" primes). Such an idea appears implicitly in older works of Wirsing and Hildebrand, but ours seems to be the

first attempt to prove it in such generality. We also proved a converse to the above result: Given an Euler product value and a solution to an integral delay equation we could find a multiplicative function with the above property. Since the values taken by such Euler products are relatively easy to understand, our focus became solutions to integral delay equations. To be precise, above we referred to $\Lambda(S)$, the *integral delay equations spectrum*, the set of values $\sigma(v)$, where $\chi : [0, \infty) \to S$ is any measurable function, with $\chi(t) = 1$ for $t \le 1$, and $\sigma(u)$ is the solution to $u\sigma(u) = \int_0^u \sigma(t)\chi(u-t)dt$ with initial condition $\sigma(u) = 1$ for $u \le 1$. Thus we can now "translate" results and conjectures about mean values of multiplicative functions into results and conjectures about integral delay equations. In general the theory of integral delay equations is cleaner so that it is easier to progress with them. Thus for example we were able to improve on the Halász-Montgomery lemma, and have actually been able to significantly shorten several difficult arguments in the literature (for example Hildebrand's bounds on $\mathcal{F}([0,1])$). Many results and techniques of classical analytic number theory translate into techniques for studying these delay equations (for example the inclusion-exclusion principle and the large sieve). We most desire, though, techniques of analysis which translate back to new number theory results.

Granville and Soundararajan have been discussing with experts in integral delay equations (Volterra equations) what techniques of that field might be applied here. The feeling of Professor L.A. Peletier of Leiden U. is that these are very interesting questions but not quite attackable by familiar results. They are now beginning to explore the area (both above and the next few subsections) with Professor J. Hale of Georgia Tech.

1d. The shape of the "spectrum".

It can be showed that if $1 \notin S$ then $\Gamma(S) = \{0\}$ so we assume that $1 \in S$. If 1 is not isolated in S intersected with the unit circle then one can show that $\Gamma(S)$ is the whole unit circle, so we assume that 1 is isolated. Although we have made several discoveries about the shape and size of $\Gamma(S)$ we have only precisely determined it when S is a subset of the reals (see below).

The spectrum must be a subset of the unit disc, it contains 0 and 1, and is connected. In [GS4] we prove that if S contains a real point other than 1 then its spectrum contains a small disc centered around the origin. In general we show that the spectrum is contained inside a circle, centered at A of radius $1 - A$ for some real number $A \in (0, 1/2)$, so that it touches the unit circle only at 1. We define the *angle* of a set S to be the maximum value of $\arg(1-s)$, $s \in S \setminus \{1\}$. The hypothesis above implies that the angle of S lies in $[0, \pi/2)$. We conjecture that the angle of the spectrum equals the angle of the set; it is easy to show that it is greater than or equal to the angle of the set, and we also show it cannot be much more than the average of $\pi/2$ and the angle of the set. We also are interested in the *projection* of the spectrum onto S, defined as the maximum of $\mathrm{Re}(\overline{s}z)$ over all $s \in S \setminus \{1\}$ and z in the spectrum. We will see below (in section 1e) that for $S = [-1, 1]$ the projection is $1 - 2\delta$ where

$$\delta = 1 - \log(1 + \sqrt{e}) + 2\int_1^{\sqrt{e}} \frac{\log t}{t+1} dt = .1715004930\ldots .$$

We make the risky conjecture that the projection is *always* $1 - 2\delta\cos^2(\mathrm{Angle}(S))$. In fact the projection is always between this and $1 - .1362\cos^2(\mathrm{Angle}(S))$.

1e. When S is a subset of the reals.

If $f(p) = 0$ or 1 for every prime p then the mean value question is the same as a sieve problem; it is easy to show $\Gamma([0,1]) = [0,1]$. More interesting is to "fix" the size of the relevant Euler product and get good upper and lower bounds for the mean value; and Hildebrand showed that the smallest mean value occurs when the primes for which $f(p) = 0$ are the large ones. Hall gave the famous upper bound of twice the Euler product, which was slightly improved by Hildebrand but still the optimal value is not yet known (or even conjectured). We can study this problem in the context of integral delay equations, via our "translation theorem" and hope to improve Hildebrand's result,

The case $S = [-1,1]$ has been of some interest. One application is to the following question: Fix large N and let $m(N)$ be the minimum possible number of quadratic residues (mod p) up to N, as we vary over all primes p. Proving a conjecture of Hall, Heath-Brown and Montgomery we showed [GS4] that $m(N) = \{\delta + o(1)\}N$. Thus if N is sufficiently large then, for any prime p, more than 17.15% of the integers up to N are quadratic residues (mod p). This result is "best possible" since the proportion δ is attained when $(q/p) = 1$ for each prime $q < N^{1/(1+\sqrt{e})}$, and $(q/p) = -1$ when $N^{1/(1+\sqrt{e})} < q < N$, and such p can be found by applying the law of quadratic reciprocity and Dirichlet's Theorem for primes in arithmetic progressions. We also have $\Gamma[-1,1] = [2\delta - 1, 1]$.

In our proof we showed that if, up to $x > x_{\delta_0}$, one has less than a proportion $(1 - \delta_0)$ of the integers being quadratic residues, then the proportion will be $< 1 - \delta/4 + \delta^2/16$ thereafter. It would be nice to get a sharper version of this result. If $\delta_0 = 1$ we got the improved bound $\le 1 - 2\delta$ but would like to know what is the best possible in this case.

Fix $0 \le \alpha \le 1$ and consider the set S_α of real-valued multiplicative functions $f(n)$ with $|f(n)| \le 1$ for all n, for which $\lim_{x\to\infty}(1/x)\sum_{n\le x} f(n) = \alpha$. Then what is

$$\lim_{x\to\infty} \min_{f\in S_\alpha} (1/x) \sum_{n\le x} f(n)?$$

We hope to answer this question by developing the methods used above.

1f. Determining other spectra.

There are several appealing avenues to go down to improve our knowledge of spectra. Perhaps the most appealing is to fix $\chi(t)$ for $t \le u/2$ but to vary the values of $\chi(t) \in S$ for $u/2 < t \le u$. We have already noted that this gives us translated, rotated and shrunken copies of S around certain points, all of which are in the spectrum. We hope other such simple variants will allow us to determine further spectra. We have also shown the "projection conjecture" for $S = \{1, -1, i, -i\}$ and so we wish to put more effort into the spectrum corresponding to the cube roots of unity.

1g. An attack on Vinogradov's conjecture.

Let n_p be the least quadratic non-residue mod p. Vinogradov's conjecture states that $n_p \ll_\epsilon p^\epsilon$. The best result known is Burgess's upper bound $n_p \le p^{1/4\sqrt{e}+o(1)}$ proved in [Bu1], back in 1957. This follows from Burgess's character sum bound (as modified by Hildebrand),

$$\sum_{n\le N} \chi(n) = o(N) \qquad \text{for} \quad N \ge p^{1/4-o(1)}, \tag{1}$$

simply by noting that if $n_p \geq p^{1/4\sqrt{e}+\epsilon}$ then, since significantly more than half of the integers up to $p^{1/4}$ are made up of integers whose prime factors are all $\leq p^{1/4\sqrt{e}+\epsilon}$, we have a contradiction to (1) for $\chi(n) = (n/p)$. The most ambitious plan in this proposal is to try to improve the exponent $1/4\sqrt{e}$ here, by a method motivated in part by our proof of the Hall-Montgomery conjecture. The idea is as follows: Let $z = z_p := p^{1/4\sqrt{e}}$, and suppose that we have an infinite sequence of primes p such that $n_p \geq z_p^{1+o(1)}$. It is easy to show that, in order that (1) holds for $N = p^{1/4}$ we must have $\sum_{n_p \leq q \leq p^{1/4}} \{1+(q/p)\} \log p/p = o(\log p)$; that is, $(q/p) = -1$ for 'most' primes q in the range $n_p \leq q \leq p^{1/4}$. Moreover, if (1) holds for $N > p^{1/4}$, then this forces more such statements about the distribution of (q/p) for larger q. For example, we must have $(q/p) = 1$ for 'most' primes q, $p^{1/4} < q \leq z^2$; and, for 'most' N in the range $z^2 < N < zp^{1/4}$, we must have

$$(1/N) \sum_{q \leq N} (q/p) \log q \sim 1 - 4 \log(\log(N/z)/\log z).$$

We can use our "translation theorem" to study

$$\chi(t) = (1/\theta(z^t)) \sum_{p \leq z^t} (q/p) \log q,$$

since $\sigma(u) = 0$ for all $u \geq \sqrt{e}$ and the delay equation $u\sigma(u) = \int_0^u \chi(t)\sigma(u-t)dt$ is satisfied. With a little work we re-organize this to find that $\chi(u) = \int_{u-1}^u \chi(t)/2(u-t)dt$ for all $u > 1$. It remains to give a good asymptotic for χ. On the other hand $\chi(u)$ can also be obtained from the zeros of the associated Dirichlet L-function, the above should tell us something strange about the distribution of the zeros of the L-function; hopefully something sufficiently strange that we can force a contradiction.

2. Multiplicative Functions in Short Intervals

There are various methods one can use to obtain upper and lower bounds or asymptotics on the mean value of multiplicative functions in short intervals.

2a. The methods of section 1.

One cannot get, in general, a Lipschitz type estimate on mean-values of multiplicative functions, as the example $f(n) = n^{it}$ exhibits. However Elliott [El] showed one can do so for the absolute value of the mean values: Indeed he showed that

$$(1/x)\Big|\sum_{n \leq x} f(n)\Big| - (w/x)\Big|\sum_{n \leq x/w} f(n)\Big| \ll (\log 2w/\log x)^{1/19}.$$

The methods of [GS] allow us to improve "1/19" to $1 - \frac{2}{\pi} = 0.36338\ldots$. It is unclear what the right constant should be; *a priori* there is no reason that it is not 1, and this subject deserves further exploration. One can use the translation theorem to make this into a question about Lipschitz conditions on integral delay equations; in this context it may be easier to make progress on this question.

2b. Applications of differencing techniques.

Classical use of exponential sums have been applied to give a variety of results about the distribution of multiplicative functions in short intervals. Among the contributions to the subject are the works of S. W. Graham and G. Kolesnik [GK], D. R. Heath-Brown [HB2], H. Li [HLi], A. Ivić [Iv], C.-H. Jia [Ji1,Ji2], E. Krätzel [Kr], H. Liu [Liu1,Liu2], M. Nair and G. Tenenbaum [help] R. A. Rankin [Ra], H. E. Richert [Ri], K. F. Roth [Ro], P. G. Schmidt [Sc1,Sc2,Sc3], and P. Shiu [Sh1,Sh2]. These results have seen recent advances through the use of finite difference techniques developed by M. N. Huxley [Hu1-HT], S. Konyagin [Ko], Sargos [HS], and both independently and jointly by the two PI's Filaseta and Trifonov (cf. [Fi1-FT4,Tr1-Tr5]). For example, they have investigated estimates for the sums

$$\sum_{x<n\le x+h} f(n) \tag{2}$$

where h is small ($h = x^\theta$ for some $\theta \in (0,1)$ with the goal of minimizing θ) and $f(n)$ represents one of the three characteristic functions for the set of k-free numbers, for the set of squarefull numbers, and for the set of n for which the number of non-isomorphic abelian groups of order n is a given fixed number k. In fact, each of the papers indicated as applications of exponential sums listed above (from the paper by Graham and Kolesnik [GK] to the papers by Shiu [Sh1,Sh2]) give estimates for (2) for one of these three characteristic functions. In [FT4], Filaseta and Trifonov show how differences can be used in each of these three cases to establish improvements over these known exponential sum estimates.

One problem the Filaseta and Trifonov would pursue is to generalize the applications of finite differences to more general functions $f(n)$. More precisely, we propose that, using the recently developed differencing techniques, we obtain an estimate for (2) for general $f(n)$ (subject to as few constraints as possible). Such $f(n)$ need not necessarily be multiplicative functions, but clearly such a constraint might lead to a better estimate or be advantageous to the approaches. That a general result of some sort should exist is already suggested by the treatment of the non-isomorphic abelian group problem by Filaseta and Trifonov in [FT4]. Further recent evidence includes the observation by Anguel Kumchev [Ku], a current student of Filaseta, that differences can be used to obtain a short interval result when $f(n)$ denotes the number of squarefree divisors of n.

2c. Squarefree and squarefull numbers.

Problems involving short interval results of the type in (2) are closely related to estimating the size of the set

$$S = \{n \in (N, 2N] \cap \mathbb{Z} : \|f(n)\| \le \delta\}, \tag{3}$$

where f is a function satisfying certain conditions on its derivatives, $\delta > 0$, and $\|x\| = \min\{|x - m| : m \in \mathbb{Z}\}$. When δ is small, the finite difference approaches, as in the applications discussed above, produce upper bounds that improve on estimates obtainable by current exponential sum techniques. Different differencing techniques apply to different problems depending on the function f and the size of N. As an example, we consider the

case that $f(n)$ is the characteristic function for the squarefree numbers. One estimates (2) by showing that typically $f(n) = 1$ unless n is divisible by the square of a small prime. This is obvious if one considers a full range of n up to some number x, but treating the case of n in a short interval $(x, x+h]$ is a more difficult problem. This short interval problem for squarefree numbers boils down to establishing that there are $o(h)$ primes $p > h$ such that $p^2|n$ for some $n \in (x, x+h]$. For each $p > h$ such that $p^2|n$, we have $n = p^2m \in (x, x+h]$ for some integer m and, hence, $x/p^2 < m \le x/p^2 + h/p^2$. Thus, if we consider $f(u) = x/u^2$ and $\delta = h/N^2$, then the size of the set S in (3) gives an upper bound for the number of primes $p \in (N, 2N]$ satisfying $p^2|n$ for some $n \in (x, x+h]$. As N varies, the short interval problem for squarefree numbers is reduced to an estimate for $|S|$.

In [G3] Granville showed that the *abc*-conjecture can be used to study the distribution of squarefree numbers, proving several of the outstanding conjectures in the area, under this (big) assumption, including the questions asked above. It would be interesting to know whether this technique can be applied to other problems in this area.

In the case of the characteristic function for squarefull numbers, improvements over the work in [FT4] by further differencing methods have been made by Huxley and Trifonov [HT] and by Konyagin and Trifonov (in progress). The first of these showed how a divided difference approach of H. P. F. Swinnerton-Dyer [Sw] for estimating the number of points on a curve could be extended to an estimate for the number of lattice points close to a curve. In other words, Swinnerton-Dyer obtained estimates in the case $\delta = 0$ in (3) above, and Huxley and Trifonov extended his approach to $\delta > 0$ to give an improvement in the short interval result for squarefull numbers. Swinnerton-Dyer's method relies on the use of a third order divided difference and certain convexity conditions. Extending the approach to divided differences of higher order required a bit of work largely because of issues associated with handling the convexity condition. Making use of some ideas of Huxley [Hu3], Konyagin and Trifonov have bypassed the issues of convexity and extended the work of Swinnerton-Dyer to fourth order divided differences.

2d. Extending this approach to all multiplicative functions.

We would like to generalize the approach of Konyagin and Trifonov to divided differences of an arbitrary order and apply the new estimates to short interval results for multiplicative functions.

One arithmetic problem that arises in the Konyagin-Trifonov approach is to estimate the number of 8-tuples $(D_1, D_2, D_3, D_4, z_1, z_2, z_3, z_4)$ where the D_j are integers satisfying $0 < |D_j| \le B$ and $D_1 + D_3 \ne D_2 + D_4$ and the z_j are integers with $0 < z_1 < z_2 < z_3 < z_4 \le A$ satisfying

$$D_1z_1 - D_2z_2 + D_3z_3 - D_4z_4 = 0$$

and

$$D_1z_1^2 - D_2z_2^2 + D_3z_3^2 - D_4z_4^2 = 0.$$

With a little work one can obtain the bound $O(A^{1+\epsilon}B^4)$, but one expects something closer to $O(AB^2)$. We know how to decrease the exponent on B from 4 to 11/3, but more work is needed on this problem as any improvement on this estimate leads to a sharper estimate for $|S|$ in (3). Such an estimate would in turn lead to an improvement in the application

of differences to the squarefull problem for short intervals. In fact, these results also give improvements to Swinnerton-Dyer's original work where $\delta = 0$. Thus we would like to make further progress on estimates for the number of 8-tuples $(D_1, D_2, D_3, D_4, z_1, z_2, z_3, z_4)$ as described above. More generally, higher order divided differences lead to the problem of estimating the number of $2n$-tuples of integers $D_1, \dots, D_n$ and $z_1, \dots, z_n$ with $0 < |D_j| \le B$ for each j, $0 < z_1 < z_2 < \cdots < z_n \le A$, $\sum_{k=1}^{n} (-1)^k D_k \neq 0$, and $\sum_{k=1}^{n} (-1)^k D_k z_k^j = 0$ for $j = 1, 2, \dots, n-2$. In each of these cases, we are mainly interested in an upper bound when B is "small" compared to A.

2e. Circles, ellipses and hyperbolas.

Suppose $f(n) = 1$ if and only if n is the sum of two squares. Again, f is multiplicative. It would be of particular interest in this case to find a *lower* bound for the sum in (2). A lower bound result would correspond to a short interval result for numbers which are the sum of two squares. In this case, a very simple argument shows that between x and $x + O(x^{1/4})$ there is a number which is the sum of two squares and, although this result dates back to R. P. Bambah and S. Chowla [BC] in 1947, no improvement on the exponent $1/4$ has ever been obtained.

A related question concerning gaps between lattice points on circles and ellipses has been more recently considered by J. Cilleruelo and A. Córdoba [CC1, CC2]. For example if $p_1, p_2, \dots p_k$ are distinct lattice points on $x^2 + y^2 = N^2$ then the arc containing them has length $\gg N^{m/(2m+1)}$ when $k = 2m+1$ or $2m+2$. This is sharp for $k = 3, 4$ and Cilleruelo and Granville have recently shown that it is sharp for $k = 5$ through a complicated construction. This problem corresponds to upper bound estimates for sums of the type given in (2), and Filaseta and Trifonov plan to consider possible applications of the recent differencing approaches to this. One can also consider other curves, some of which lead into classical problems, such as $xy = N$ (divisors close together). A related problem is to look at how many solutions there are of $x^2 \equiv 1 \pmod{n}$ with $x < n^{1/2+\delta}$, which has many applications.

2f. Higher dimension.

Filaseta and Trifonov also plan to lead investigations concerning the use of differences to estimate the size of the set

$$S' = \{(u, v) \in \mathbb{Z}^2 : u \in (N, 2N], v \in (M, 2M], ||f(u, v)|| < \delta\}$$

for some appropriately behaved function $f(u, v)$. In other words, we will consider the possibility of extending the current differencing techniques to obtain multi-dimensional versions of the type already investigated. We wish to find a good upper bound (using differences) for the size of the set S' mentioned above or, more generally, obtain estimates for the number of lattice close to a surface in higher dimensions.

It is anticipated that such estimates would then be applied to obtain new short interval results for multiplicative functions.

2g. Multiplicative functions in short intervals, on average.

Using the large sieve one can get good results for this, in many situations. One application is to prove, via the "translation theorem", a "deviation" theorem for solutions to

integral delay equations, something which seems to be new to that area. In particular, we show that for σ as above $\int_0^u |\sigma(u) - \chi(t)\sigma(u-t)|^2/tdt \le 3/2$, which is best possible up to the constant. It would be interesting to have a direct proof from analytic methods; and if that is possible to see if such methods could be used to give upper bounds for higher moments. This might have extraordinary consequences for understanding of the distribution of multiplicative functions.

3. Multiplicative functions constructed from shifted primes

For fixed nonzero integer a, let P_a denote the set of numbers of the form $p+a$ where p is prime. These are often referred to as sets of "shifted primes". Determining the multiplicative structure of numbers in the sets P_a has been the subject of numerous investigations. In particular, there is a close connection between properties of P_a and properties of certain multiplicative functions, such as Euler's function $\phi(n)$ ($\phi(p) = p-1$ for primes p) and the sum of divisors function $\sigma(n)$ ($\sigma(p) = p+1$ for primes p). The structure of P_{-1} also plays a crucial role in the recent proof that there are infinitely many Carmichael numbers [AGP], and in the work by Gupta and Murty [GM] and Heath-Brown [HB1] on Artin's primitive root conjecture.

Let $P_a(x) = P_a \cap [1, x]$. It is expected that in a multiplicative setting, the sets $P_a(x)$ should behave very much like a "random" set of $\pi(x)$ integers $\le x$, where $\pi(x)$ is the number of primes $\le x$. This heuristic of course has limits, for example P_a will have at most one number in each residue class $-a \pmod p$ for each prime p. But for many arithmetic functions, such as P^+ (the largest prime factor function), the distribution of $P^+(p+a)$ should correspond roughly to the distribution of $P^+(n)$ over all $n \le x$. Current knowledge for this particular function is scant. For instance, Baker and Harman [BHa] have proved that $P^+(p+a) \gg p^{0.677}$ for infinitely many p, and that $P^+(p+a) \ll p^{0.2961}$ for infinitely many p. These statements are expected to be true with exponents $1-\epsilon$ and ϵ, respectively, where $\epsilon > 0$ is arbitrary.

3a. The number of images of a multiplicative function.

Denote by $\Omega(n)$ the number of prime factors of n counted with multiplicity (note that $e^{it\Omega(n)}$ is a multiplicative function). Let f_a be a multiplicative function defined by $f_a(p) = p + a$ and $f_a(p^b) = 0$ if $b \ge 2$. One can show, by sieve methods (e.g. [Er1], [F1,§2]), that the distribution of $\Omega(p+a)$ is similar to the distribution of $\Omega(n)$ over $n \le x$. Applications of this observation are key to bounding the number of positive integers $\le x$ which can be written as a product of numbers of the form $p + a$ (that is, are in the image of f_a); and such bounds, in turn, provide bounds on $\text{Image}_f(x)$, the number of values taken by $f(n)$ that are $\le x$, for various multiplicative functions f such as ϕ and σ. Several authors, including Erdős [Er1] and recently Maier and Pomerance [MP], have developed bounds for $\text{Image}_\phi(x)$ (and the methods work to give identical bounds for $\text{Image}_{f_a}(x)$). Still, a sizeable gap remained between upper and lower bounds until, recently, Ford proved ([F1, Theorems 1,14]) that $\text{Image}_{f_a}(x) \asymp Z(x)$ where

$$Z(x) = \frac{x}{\log x} \exp\{C(\log_3 x - \log_4 x)^2 + D \log_3 x - (D + 1/2 - 2C) \log_4 x\},$$

with $C = 0.817\ldots$ and $D = 2.176\ldots$ being specific constants and $\log_k x$ denoting the k^{th} iterated logarithm of x. Furthermore the same result holds for for a large class of

integer-valued multiplicative functions f with $f(p) = p + a$ for primes p and $f(p^b)$ "not too small" for $b \geq 2$ (in particular for ϕ and σ). One significant improvement to this result would be to find out whether there exists a constant c for which $\text{Image}_{f_a}(x) \sim cZ(x)$, and to determine it if it exists.

3b. The distribution of multiplicities of the pre-images of a multiplicative function.

Let $|f^{-1}(m)|$ denote the number of integers n for which $f(n) = m$, in other words the number of pre-images of m under the map $f : \mathbb{N} \to \mathbb{N}$. Erdős [Er3] showed that (for the same f as above) for any given positive integer k, if there is one integer m with $|f^{-1}(m)| = k$ then there are infinitely many. Using similar methods to those above, Ford [F1,Theorems 2 and 14] showed that if there is one integer m with $|f^{-1}(m)| = k$ then there are $\gg_{f,k} \text{Image}_f(x)$ integers $m \leq x$ with $|f^{-1}(m)| = k$, that is, at least a positive proportion of the integers have exactly k pre-images under the map f. However few integers have many pre-images: To be precise, a proportion $\ll \exp(O(\sqrt{\log N}))/N$ of the images $m \leq x$ have more than N pre-images.

3c. What multiplicities occur?.

Carmichael's famous conjecture [C1,C2] claims that, for $f = \phi$, the multiplicity $k = 1$ is not possible; in other words, for all integers n there exists a different integer N with $\phi(N) = \phi(n)$. This remains open, although large lower bounds on a possible counterexample are easy to obtain, the latest being $10^{10^{10}}$ [F1,Theorem 6]. We can ask for more general f, what multiplicities do in fact occur? One can construct trivial examples of f for which multiplicity 1 is impossible (for example, multiplicative f with $f(p) = 1$ for some prime p, and $f(p^b) = 0$ for all $b \geq 2$), but can we come up with any non-trivial examples other than ϕ?

In the 1950's, Sierpiński conjectured that for $f = \phi$ and $f = \sigma$ that all multiplicities $k \geq 2$ are possible [S1, Er3]; and, in 1961, Schinzel [S2] deduced this conjecture from his well-known Hypothesis H [SS]. Recently, Ford has proven the Sierpiński conjecture for $\phi(n)$ [F3] and, with S. Konyagin [FK], for $\sigma(n)$, the proofs being rather different. In the proof for $\phi(n)$ the proof involves taking an integer m for which $|\phi^{-1}(m)| = k$ and constructing a number m', via Chen's results on almost-primes, with $|\phi^{-1}(mm')| = k+2$. More generally the method gives, for f as above, if $f(p^2) = pf(p)$ for all primes p, and if $|f^{-1}(m)| = k$, then there is a number m' such that $|f^{-1}(mm')| = k+|f^{-1}(1)|$. The proof of the Sierpiński Conjecture for $\sigma(n)$ uses almost primes in a simpler though trickier way; and the proof carries over to other such f provided multiplicity 1 is possible.

3d. Attacking Carmichael's conjecture.

Let $g_f(m)$ be the gcd of the integers n for which $f(n) = m$ if $f^{-1}(m)$ is non-empty. In the proof of the lower bound for $\text{Image}_f(x)$ in [F1, Theorems 2,14], it is proven that if $|f^{-1}(m)| = k \geq 1$ and $f(n_1) = \cdots = f(n_k) = m$ then $f^{-1}(f(u)m) = \{un_1, \ldots, un_k\}$ for $\gg \text{Image}_f(x)$ square-free numbers $u \leq x$ with $(u, m) = 1$. In particular either $k \nmid g_f(m)$ for all m, or $k | g_f(m)$ for $\gg \text{Image}_f(x)$ values of $m \leq x$. Our plan of attack on Carmichael's conjecture is to show that 6 never divides $g_f(m)$ (as appears from computation); this implies Carmichael's conjecture since one can show that if $\phi^{-1}(m) = \{n\}$ then n is divisible

by 6. In general we propose investigating the possible values of $g_f(m)$, in particular for $f = \phi$ and $f = \sigma$.

3e. Constructing counterexamples to primality tests.

Alford, Granville and Pomerance [AGP1] showed recently that there are infinitely many Carmichael numbers, that is numbers n for which $a^n \equiv a \pmod{n}$ for all integers a (which has nothing to do with Carmichael's conjecture!). Another characterization of Carmichael numbers is, squarefree integers n for which $p-1$ divides $n-1$ for all primes p dividing n, and thus we see we are led to understanding the multiplicative structure of $p-1$. Indeed their construction involved $p-1$ divisible only by small primes with special properties. There are many "pseudoprime" tests which "almost certainly" identify prime numbers in random polynomial time; however the problem with these tests is that they don't guarantee that the number is indeed prime. It is hoped that non-random variants will provide deterministic primality tests. For example some people hoped for (and some computer languages implemented) a test based on strong pseudoprimes, though counterexamples to such tests were given in [AGP2] by modifying their earlier methods. There are various other proposed primality tests that are presumably wrong, but have not as yet been proved to be wrong by these same methods. For example, when examining primality tests based on the arithmetic of quadratic fields (or second order linear recurrence sequences) certain substantial difficulties arise from studying the function f_1 as opposed to f_{-1} as before. These difficulties are not technicalities, but really require new ideas, particularly in the applications of group theory in the proof. We propose to look further at this problem.

4. Character sums and L-functions

Most work on character sums $|\sum_{n\le N}\chi(n)|$ has been on obtaining non-trivial upper bounds when N is a small power of the conductor q of χ; there has been little improvement since the work of Burgess [Bu1] forty years ago! In [GS1] Granville and Soundararajan examined the *distribution* of such character sums. One motivation was to discover for what N one might conjecture that the character sum is $o(N)$. Several authors have remarked that it should be so for $N = \log^{2+o(1)} q$, which is now known to be wrong. Indeed Granville and Soundararajan have shown that for all fixed $A > 0$, for all primes q, there are more than $q^{1-o(1)}$ characters $\chi \pmod q$ for which the character sum is $\ge \{1-o(1)\}\rho(A)N$ when $N = \log^A q$. They conjecture though that this is the maximum possible size for such a character sum. Assuming GRH they modified an argument from [MV1] to show that this character sum is $\ll \rho(A/2-\epsilon)N$. Therefore they believe that the character sum is $o(N)$ when $\log N/\log\log q \to \infty$ and that this result is best possible. There are several other main themes in [GS1]. One important one is that if a character sum is large then it must be because $\sum_{n\le N,\ p|N \Longrightarrow p\le \log^2 q}\chi(n)$, the character sum over "smooth numbers", is large. This is "almost always true", and they prove a version of it assuming GRH. They believe that the distribution of character sums can be modeled on the distribution of $\sum_{n\le N} X(n)$ where X is a multiplicative function and each $X(p)$ is an independent random variable equi-distributed on the unit circle; they have shown that the moments of each agree in a wide range of uniformity. This allows to prove various lower bounds for character sums. For example that Paley's lower bound $\gg \sqrt{q}\log\log q$, obtained for a (sparse) sequence of

quadratic character sums, actually holds for more than $q^{1-o(1)}$ characters $\chi \pmod q$.

Littlewood [Li2] showed that

$$\{1/2 + o(1)\}(\pi^2/6)/(e^\gamma \log\log q) \le |L(1,\chi)| \le \{2 + o(1)\}e^\gamma \log\log q,$$

when q is prime assuming GRH. Subsequently, Chowla showed that there are infinitely many q, such that for the primitive quadratic character χ mod q these bounds are almost obtained, though removing the factors '1/2' and '2' from the two sides, respectively. In [GS2] Granville and Soundararajan obtained Chowla's bounds for $q^{1-o(1)}$ characters χ mod q, and then proceeded to obtain distribution results for $|L(1,\chi)|$, showing that $|L(1,\chi)| > \tau$ for a proportion

$$\exp\left(-\left\{2e^\gamma/e^{1+C_1} + o_\tau(1)\right\} e^{e^{-\gamma}\tau}/\tau\right)$$

of the characters $\chi \pmod q$ for any prime q, for

$$1 < \tau < e^\gamma \log\log q - 6\log\log\log q.$$

(A similar result holds for $1/|L(1,\chi)|$.) They obtain such a strong result as a consequence of proving that the mean value of $L(1,\chi)^{z_1}L(1,\overline{\chi})^{z_2}$ as one varies over characters $\chi \pmod q$, equals $\mathbb{E}\left(L(1,X)^{z_1}L(1,\overline{X})^{z_2}\right) + o(1)$, for each $|z_j| \le \log q/(\log\log q)^3$, where X are the random variables above (though with $X(q) = 0$). They obtain similar results for quadratic L-functions, improving results of Erdős and Elliott. They also show that

$$\{(\arg(\chi(2))/2\pi, \arg(\chi(3))/2\pi, \dots, \arg(\chi(p_k))/2\pi) : \ \chi \pmod q\}$$

are equidistributed as vectors in $(\mathbb{R}/\mathbb{Z})^k$, in a reasonable range of uniformity.

4a. Paley's theorem "in all directions".

Paley [Pa] showed that

$$\sum_{n<N} \chi(n) \gg \sqrt{q}\log\log q,$$

for some N, for infinitely many quadratic characters $\chi \pmod q$. Granville and Soundararajan showed that for all primes q there are $> q^{1-o(1)}$ such characters $\chi \pmod q$, with $N = q/2$ and implicit constant e^γ/π in [GS2]. The idea in the proof is that, via a Fourier transform as noted by Polya, this character sum equals the value of the Gauss sum times the value of $L(1,\chi)$, times a small easily controlled factor. Of course the Gauss sum has size $\sqrt{q}$, and as we saw above, we can get $L(1,\chi)$ as big as $e^\gamma \log\log q$. We are now interested in obtaining character sums of this size, with $N = q/2$ but now pointing in any given pre-specified direction. The idea is that Deligne's estimates on Kloosterman sums [De] should allow us to control the arguments of the Gauss sums, while we must control the argument of the $L(1,\chi)$ by moment arguments. Katz [Ka] has already shown that Gauss sums are equi-distributed around the circle of radius $\sqrt{q}$ and results from [GS2] show that the argument of the $L(1,\chi)$ has its own, more complicated, distribution function. The problem here is we have to manage these simultaneously though we have accomplished this in a weak form (see [GS6]). Now we wish to prove this with a stronger error term, and extend the method to $N = cq$ for any rational c with small denominator.

4b. Distribution of Character Sums.

In [GS1] Granville and Soundararajan investigated large values of character sums, and showed that high moments are well-approximated by high moments of the appropriate random variables X, as above. However we have not yet established the desired result that the character sums themselves are distributed in the same way as the sum of the random variables. Proceeding in a similar way to 4a, there is some hope of establishing such a result for character sums with $N = q/2$.

The next step is to actually find the distribution function of $\sum_{n\le N} X(n)$ (which presumably tends to some limiting distribution when correctly normalized). Finally, perhaps by using Poisson summation in a different form from Polya's identity, we can equate this to the more general distribution of character sums.

4c. Distribution of the character sums for a given character.

If $|L(1,\chi)|$ is large with $\chi(-1) = -1$ then $\sum_{n\le N}\chi(n)$ is large for almost all $N \le q$. In fact it stays close to $\sum_{n\le q/2}\chi(n)$. One proves this by computing the second moment. It would be nice to gain a better understanding of the dynamics of this function of N. Computing the fourth moment is generally tough (as it ends up as a function of fourth order Dedekind sums), so we would like to do some computations on this question. There is some old inspiring work of D.H. Lehmer [Le] showing that quadratic character sums have beautiful dynamics on the complex plane.

4d. Distribution of values of Dirichlet L-functions.

In [GS2] Granville and Soundararajan showed that $\{L(1,\chi)\}_{\chi \pmod q}$ behaves in distribution like $L(1,X)$, though without much uniformity. We would like to extend this to a result that is uniform in $|\log|z|| \le \log\log\log q + O(1)$ which is as wide a range as can be true. Given our results in [GS2] on moments with high uniformity, this probably only requires some better complex analysis. The stumbling block to proving this is that, as we saw above, $L(1,\chi)$ decays double exponentially so that simple variants of Perron's formula can't work since the error terms corresponding to the integrand from the innermost edge of the area of the integration, dominate the main term.

4e. Upper bounds on $L(1,\chi)$-values for fixed order characters.

Stephens [St] proved that if χ is a quadratic character of conductor q then

$$L(1,\chi) \le (2 - 2/\sqrt{e} + o(1))\log q.$$

The key tools are Burgess's theorem and then an optimization technique. In fact Stephen's result follows easily from our methods [GS4], and so we have started to look at what kind of bounds one can get for cubic, quartic and higher order characters. The key seems to be that to get pseudo-"inclusion-exclusion" formulas. That is, the inclusion-exclusion formula is based on truncations of the binary expansion for $0 = (1-1)^n$ giving upper and lower bounds for 0. We are trying to develop analogous bounds from the expansion of $(1+\omega+\omega^2)^n$, where ω is a primitive cube root of unity, and have already proved $L(1,\chi) \le \log q$ for χ of order 3 $\pmod q$.

4f. Distribution of values of other L-functions.

Granville and Soundararajan propose investigating many of the problems considered in [GS1] and [GS2] in the context of modular forms. Here are some concrete examples of the problems that arise:

Consider the family $\mathcal{F}_k$ of all Hecke eigenforms forms over $\Gamma = SL(2,\mathbb{Z})$ with weight $2k$. Suppose $f(z) = \sum_{n=1}^{\infty} a(n)e(nz)$ is a typical such form. One question concerns the distribution of the $a(p)$'s. This is expected to be as predicted by Sato-Tate but seems intractable. As evidence to this, Conrey, Duke and Farmer, investigated the distribution of $a(p)$ for fixed p, and varying $f \in \mathcal{F}_k$. They found that the $a(p)$ are uniformly distributed with reference to the p-adic Plancherel measure, which tends to the Sato-Tate distribution as $p \to \infty$. One might extend this by asking how $\{a(p_1), \dots a(p_l)\}$ are distributed, given the primes p_i, and varying once again over $f \in \mathcal{F}_k$. Questions like this for Dirichlet characters are addressed in [GS2], and this seems a natural extension. The key technicality will be to replace our previous use of "orthogonality of character sums" by the appropriate trace formula. If we obtain precise information on this problem (that is, results uniform in k) then we will be able to exhibit modular forms with prescribed eigenvalues on the small primes which should have several applications.

The analogue to the character sum problems considered in [GS1] is to look for large values of $\sum_{n \le N} a(n)$, given N, and varying f over $\mathcal{F}_k$. These sums exhibit a "square-root cancellation" for fixed f, and N sufficiently large. Are there ranges where square-root cancellation fails to hold? Are there ranges where the sum is of size N? We will also consider the distribution of values of $L(1, \mathrm{sym}^2 f)$. This has been investigated recently by Luo [Luo] (in the context of Maass cusp forms), who shows the existence of a distribution function, by computing the (fixed) moments of $L(1, \mathrm{sym}^2 f)$. In the spirit of [GS2], one would like to evaluate the moments as uniformly as possible, so as to gain an understanding of the true maximal, and minimal sizes of $L(1, \mathrm{sym}^2 f)$. At first sight there are no insurmountable technical obstructions, especially given the (known) non-existence of Siegel zeros.

5. Zeros of L-functions and the comparative distribution of primes

Denote by $\pi(x)$ the number of prime numbers $\le x$, and for $q > 2$ and $(a,q) = 1$, let $\pi_{q,a}(x)$ denote the number of primes $\le x$ in the progression $a \pmod q$. Chebyshev [Cheb] observed that there are "more" primes in the progression $3 \mod 4$ than in the progression $1 \mod 4$ (meaning $\pi_{4,3}(x) \ge \pi_{4,1}(x)$ most of the time). As noted by later authors, for many such triples q, a, b there appears to be a bias in the sign of $\Delta_{q,a,b}(x) := \pi_{q,a}(x) - \pi_{q,b}(x)$. In general, if a is a quadratic non-residue modulo q and b is a quadratic residue, then $\Delta_{q,a,b}(x)$ tends to be more often positive than negative. In some cases, the first sign change is quite large, especially if $q|24$, $b = 1$ and $a \ne 1$. For example, computations by Bays and Hudson ([BH1], [BH2]) have shown that the first sign change in $\Delta_{3,1,2}(x)$ occurs at 608981813029. The biases "against" quadratic residues can be explained analytically via the explicit formulae for $\pi_{q,a}(x)$ in terms of zeros of Dirichlet L-functions (e.g. [RS]), or combinatorially ([H2]). These problems are also closely related to the bias in the sign of $\mathrm{Li}(x) - \pi(x)$, where $\mathrm{Li}(x) = \int_2^x dt/\log t$ is the natural smooth approximation to $\pi(x)$.

5a. Sign changes for $\Delta_{q,a,b}(x)$.

On the theoretical side, it is widely believed that for any modulus q and numbers a and b coprime to q, the function $\Delta_{q,a,b}(x)$ changes sign infinitely often. The first such proof was by Littlewood in 1914 [Li1] for the cases $q = 3, a = 1, b = 2$ and $q = 4, a = 1, b = 3$, as well as showing that $\mathrm{Li}(x) - \pi(x)$ also changes sign infinitely often. An extensive program by Knapowski and Turán in the 1960's ([KT1,KT2]) addressed this question. They established infinitely many sign changes for a wide class of q, a, b, some results of which required the hypothesis that the corresponding L-functions have no real non-trivial zeros (easy to verify for a given modulus q), and some which required that the L-functions have no non-trivial zeros off the critical line up to a certain height T (given as cq^{10} for an unspecified c). We would like to make explicit the height T required to prove that for a given fixed q, all functions $\Delta_{q,a,b}(x)$ with $(a, q) = (b, q) = 1$ have infinitely many sign changes, thus reducing the problem for a given q to a finite (and reasonable) computation.

It is also of interest to locate sign changes, or obtain upper bounds on the first sign change. Although Littlewood's proofs provided no particular x for which $\mathrm{Li}(x) - \pi(x)$ is negative, Skewes ([Sk1],[Sk2]) in 1955 showed unconditionally that a sign change occurs before $10^{10^{10^{10^3}}}$. A major breakthrough was made in 1966 by R. S. Lehman [Le], who showed that $\mathrm{Li}(x) - \pi(x)$ is negative somewhere between 1.53×10^{1165} and 1.65×10^{1165}. His method involved approximating a weighted average of $\mathrm{Li}(x) - \pi(x)$ and using the computed values of the first 12,000 zeros of the Riemann zeta function $\zeta(s)$ lying above the real axis. The upper bound has since been lowered twice ([tR], [BH3]) using Lehman's theorem together with more extensive computations of the zeros of $\zeta(s)$.

In joint work with R. Hudson [FH], Ford has successfully generalized Lehman's method to obtain a method of locating sign changes of any $\Delta_{q,a,b}(x)$, provided that sufficiently many small zeros of the corresponding L-functions are known. The zeros ρ with $|\Im\rho| \leq 10000$ for many small q have been computed by R. Rumely [Ru], and with these we have shown that each $\Delta_{8,b,1}(x) < 0$ for some $x < 10^{24}$, each $\Delta_{12,b,1}(x) < 0$ for some $x < 10^{429}$, and each $\Delta_{24,b,1}(x) < 0$ for some $x < 10^{353}$.

5b. Many progressions mod q.

In addition to comparing counts of primes in pairs of arithmetic progressions modulo q, one can compare any $m \leq \phi(q)$ progressions and ask whether all $m!$ possible orderings occur (or occur for arbitrarily large x). Recently Kaczorowski [K1] showed, assuming the Generalized Riemann Hypothesis, that $\pi_{q,1}(x) > \pi_{q,b}(x)$ for all $(b, q) = 1$, for a positive proportion of x, and likewise $\pi_{q,1}(x)$ runs behind all the others for a positive proportion of x. In [K2] and [K3] he extends this to other (but not all) orderings.

Assuming the Generalized Riemann Hypothesis and the Simplicity Hypothesis (that the imaginary parts of the zeros of all Dirichlet L-functions are linearly independent over $\mathbb{Q}$), Rubinstein and Sarnak [RS] have shown that the set of values x for which a certain ordering of the functions $\pi_{q,a_i}(x)$ $(1 \leq i \leq k)$ occurs has a logarithmic density, and this provides numerical values for the biases [RS, p. 188]. They show that this bias is always positive, and give a method of computing it. For example, the logarithmic density of the set of x giving $\mathrm{Li}(x) - \pi(x) > 0$ is about 0.99999973.

For more than two progressions, the procedure becomes quite complex, although G. Martin and A. Feuerverger at the University of Toronto have succeeded in the cases $q =$

$8, a_1 = 3, a_2 = 5, a_3 = 7$ and $q = 12, a_1 = 5, a_2 = 7, a_3 = 11$. Bays and Hudson have developed a less rigorous, but easier to implement, method of approximating the densities by using a truncated version of explicit formulas for $\pi_{q,a}(x)$.

Using this method, Ford has computed biases for the six orderings for triples of progressions of quadratic non-residues modulo $q = 8$, $q = 12$ and $q = 24$. In every case there is a significant deviation from 1/6 for the six bias numbers, although the bias when comparing any two of the progressions is exactly $\frac{1}{2}$. While combinatorial arguments can explain the bias against quadratic residues, we as yet do not have a combinatorial explanation (one not using the specific values of zeros of L-functions) to explain this, and so more work is necessary to understand it.

5c. Computing zeros of L-functions.

For the above subsections it is necessary to compute the zeros of Dirichlet L -functions for small moduli up to various heights. This is a difficult task and needs to be done as a separate project. Moreover due to its wide applicability it is important to produce these results in a very accessible form. To date the PI Rumely has produced almost all of the computations known and does propose to go even further.

In [Ru] Rumely wrote a series of programs to check the Extended Riemann Hypothesis for Dirichlet L-series. For moduli $Q \leq 13$, they were used to compile lists of zeros and check the ERH to height 10000; for moduli in the range $13 < Q \leq 72$, and certain other moduli, this was done to height 2500. These computations were used, as mentioned above, by Sarnak and Rubinstein, by Bays, Ford and Hudson, and more recently by Feueberger and Martin in investigating the Chebyshev bias. An obvious application is to obtain quantitative error bounds in the prime number theorem for arithmetic progressions; this was done by Ramaré and Rumely [RR] for all moduli $q \leq 72$, all composite $q \leq 112$, and certain other moduli.

Recently Rumely has checked the ERH to height 100000 for moduli in the range $1 \leq Q \leq 9$; and, with W. Galway, plans to check the ERH to height 50000 for $11 \leq Q \leq 32$, to height 25000 for $33 \leq Q \leq 72$, and to height 2500 for all moduli up to 500.

Timelines and Dissemination of Material

It is hard to give a precise timeline for the proposed research. The more predictable avenues have more predictable timelines, but we are far more interested in the unpredictable avenues we have described that might have big pay-offs (such as to proving Vinogradov's conjecture or Carmichael's conjecture). Of course we shall disseminate results, as usual, mailing paper preprints to selected interested researchers around the world, by making preprints available electronically on the web, and by submitting completed manuscripts to top quality journals.

Training and Participation

Several of the world's leading researchers in this field, namely Pomerance, Konyagin, Schinzel and Soundararajan, have agreed to participate in this project. We expect that other leading people may get involved out of interest for the material; and we will invite

other young mathematicians, such as Greg Martin, for shorter visits. Other people who have made significant contributions to this area in recent years and would be considered as speakers include Bombieri, Iwaniec, Sarnak, Friedlander, Vaughan, Montgomery, Hall, Tenenbaum, Hildebrand and Elliott. We also expect to train several postdocs and graduate students in this area. Below we give brief biographical sketches of recent Ph. D. students.

Recent and current doctoral students of the PIs

At Georgia.

Jon Grantham (Ph.D.'97) developed the notion of a "Frobenius pseudoprime", of which most known pseudorimes are special cases. This allowed him to combine previous combinations of pseudoprime tests into one test. He now works for the Institute for Defense Analyses, MD.

Kevin James (Ph.D.'97) used Waldspurger's Theorem on Shimura lifts, together with clever computations and results on distribution of class numbers to find modular forms f such that a positive proportion of the quadratic twists of $L(f, s)$ do not vanish at the critical point. He is now a Chowla postdoc at Penn. State and is active in this busy area.

Glenn Fox (Ph.D.'97) created a p-adic L-function in two variables that interpolates values of Bernoulli polynomials. This allowed him to reprove several interesting divisibility properties. He is now at Emory.

Dina Khalil (Ph.D.'00) has constructed families of dihedral extensions of the rationals, of orders $6, 10, 14$ which are subfields of Hilbert class fields. This allows her to prove new results on p-divisibility of class numbers. She also can construct families of quadratic fields with class number divisible by any given prime p.

Pam Cutter (Ph.D.'00) has shown how to find, in practice, consecutive primes with any given difference; and thus was the first to find the long sought after pair of difference 1000. She is now studying the distribution of $\{f(n) \pmod{\mathbb{Q}^2}\}$ for given polynomial f.

Ernie Croot (Ph.D.'00) has improved known bounds for smooth numbers in short intervals, and has proved a ($ 500) conjecture of Erdős and Graham: Every r-coloring of the natural numbers > 1 contains a finite monochromatic subset whose sum of reciprocals is 1.

Mark Watkins (Ph.D.'00) has improved techniques used to determine all imaginary quadratic fields of given class number. In particular he has found all of class number 8. He is now developing an idea of Montgomery and Weinberger on the pair correlation function forced by a small class number.

Gang Yu (Ph.D.'00) has developed the method of Heath-Brown [HB], used for families of quadratic twists, to compute the average size of the 2-Selmer group for elliptic curves with all rational 2-torsion, to more general families of elliptic curves. Surprisingly the average size is bounded, contradicting a conjecture of Brumer, whereas it is unbounded in certain subfamilies.

Stephen Donnelly (Ph.D. '01) is voraciously reading in various areas. For a while he was interested in consequences of Shouwu Zhang's theorem on lower bounds for heights of points on curves. Now he is looking into generalizations of Hilbert's Tenth Problem.

The following have all completed their written prelims: *Milton Nash, Michael Beck, Eric Pine and Jim Blair.*

At South Carolina.

Brian Beasley (Ph.D.,'95) has worked on a generalization of a problem of Erdős concerning moments of gaps between k-free numbers. The generalization is to the moments of gaps between integers m for which $f(m)$ is k-free where $f(x)$ denotes an irreducible polynomial. The case $f(x) = x$ corresponds to the problem of Erdős, and Beasley's approach in this case leads to improvements over the original results of Erdős. He is currently an Associate Professor and Chair of the Mathematics Department at Presbyterian College in Clinton, South Carolina.

Ikhalfani Solan (Ph.D.,'96) has published two joint papers with Filaseta associated with the factorization of polynomials. In one, they establish that if $f(x) \in \mathbb{Z}[x]$ does not have cyclotomic factors and $g(x) \in \mathbb{Z}[x]$ is such that $f(x)g(x)$ has "small" Euclidean norm, then so does $g(x)$. In the second, they establish that the non-reciprocal part of $x^a+x^b+x^c+x^d+1$ is irreducible for arbitrary integers $a > b > c > d$. He is currently an Assistant Professor at the University of the West Indies in Jamaica.

Rich Williams (Ph.D.,'00) is working on irreducibility results associated with the *generalized* Laguerre polynomials. In particular, he is establishing results associated with their Galois groups.

Anguel Kumchev (Ph.D.,'01) already has nine papers published or in press and a tenth joint paper with J. Brudern submitted for publication. He is working on problems in Analytic Number Theory that make use of a variety of exponential sum and sieve techniques. For example, he has recently obtained new estimates associated with primes of the form $[n^c]$ for certain ranges of real $c > 1$.

Martha Allen (Ph.D. '01) is working on generalizations of several irreducibility results of I. Schur that were used by Schur to establish the irreducibility of the classical polynomials of Hermite and Laguerre.