Project summary

The PI has worked on a wide range of topics in number theory. He proposes here to continue these investigations. The proposed projects are from four distinct areas, all belonging to analytic number theory broadly construed: Prime-splitting statistics in abelian extensions, the value-distribution of the Euler ϕ-function, a statistical study of perfect numbers and their generalizations, and the distribution of irreducible polynomials over finite fields.

Intellectual merit

The PI's work on prime-splitting statistics has the potential to offer new insight into abelian cases of the Chebotarev density theorem, a theorem whose applications are nearly ubiquitous in number theory. Moreover, the PI's work in this area has close ties with two recently developing schools of number theory, *arithmetic statistics* (in the spirit of Bhargava, Thorne, Wood, and others) and the *pretentious perspective* (championed by Granville and Soundararajan).

Problems about perfect numbers are some of the most famous in all of mathematics; many of the open questions are known to the larger scientifically literate public. Work in this area is therefore good PR for mathematics! Moreover, because several related problems are easy to state and can be attacked without excessive prerequisites, there is a lot of room for undergraduate research.

The reviewer's proposed work on the Euler function aims to answer natural questions about the values assumed by ϕ and the corresponding preimages. Why ϕ in particular? The ϕ-function arises in nearly any investigation connected with multiplicative orders; moreover, its nature as a multiplicative function with well-understood behavior on prime powers makes it a simple model for its more ornery relatives (such as the sum-of-divisors function σ and the Carmichael λ-function).

Finally, the work of the PI on the distribution of irreducibles should be viewed as part of an ongoing project of the mathematical community to compare and contrast number fields and function fields. Investigations of this sort have already paid rich dividends (e.g., the spectacular resolution of the Riemann Hypothesis for function fields by Weil).

Broader impacts

The PI is a strong believer in recognizing and nurturing junior talent. He was one of the coauthors of this year's UGA High School Math Tournament, which attracts competitors from Georgia and neighboring states; he expects his involvement to continue over the next several years. He is also running the Putnam seminar this year at UGA (a 1-credit hour course). As part of a separate grant, he has applied to run a number theory REU at UGA in the near future.

The PI is also interested in pursuing writing projects that result in work accessible to undergraduates. He has published three papers in the *Monthly* (all of which could be read by talented undergraduates), as well as an expository paper in *Elemente der Mathematik* offering a new proof of the infinitude of primes. He has also written a textbook suitable for advanced undergraduates (*Not always buried deep*), published by the AMS in late 2009.

The PI has agreed to give a week-long course at a 2013 CIMPA/ICTP summer school in the Philippines. CIMPA (International Centre for Pure and Applied Mathematics) and ICTP (the Abdus Salam International Centre for Theoretical Physics) are organizations aiming to promote scientific education and research in developing countries.

Project description

1 Introduction

Broader impacts

The PI has a strong interest in recognizing and nurturing young mathematical talent. He was one of the coauthors of this year's University of Georgia High School Math Tournament, which attracts competitors from the state of Georgia and beyond; he expects his involvement with this tournament to continue for the next several years. This year, he is running the Putnam training seminar at UGA (a 1-credit hour course). The PI has also been a frequent guest lecturer at the Ross Summer Mathematics Program, a residential summer program for high school students held annually at Ohio State University. He last visited the program in 2009 to give a week-long minicourse on analytic number theory; he intends to maintain strong ties to the program going forward.

During the summer of 2009 (while an NSF postdoctoral fellow), the PI served as a REGS mentor at the University of Illinois, working with graduate students Joseph Vandehey and Paul Spiegelhalter. (REGS = **R**esearch **E**xperiences for **G**raduate **S**tudents.) This was a wonderful learning experience for everyone involved. The PI is proud of the resulting paper [VS] and expects that it will be accepted soon at a research journal.

The PI is interested in producing mathematical writing that can be read profitably by undergraduates. He has three papers in the *Monthly*: two on sociable numbers (a topic discussed later in this proposal), and another on Goldbach's conjecture for polynomial rings. He also has a paper in *Elemente der Mathematik* offering a new proof of the infinitude of the primes. All of these papers are accessible to undergraduates and could be the basis of possible undergraduate research projects. Indeed, possible REU projects along these lines have been described in a separate grant proposal of the reviewer. In 2009, the American Mathematical Society published the PI's book *Not always buried deep.* This text is suitable for study by advanced undergraduates.

Next summer, the PI will give a mini-course at a summer school in Manila. This summer school is being organized through CIMPA (International Centre for Pure and Applied Mathematics) and ICTP (the Abdus Salam International Centre for Theoretical Physics), both of which are organizations promoting the dissemination of scientific research findings in developing countries.

Overview

In the next four sections, four proposed research areas and associated research projects are discussed in turn. In the final section of this project description, the papers resulting from the PI's previous NSF support are summarized.

2 Prime splitting in abelian extensions

In 1880, Kronecker showed that for each Galois extension $L/\mathbf{Q}$ of degree n, the proportion of rational primes that split completely in L is $1/n$. A substantial generalization of Kronecker's result was proved by Chebotarev in 1922:

Chebotarev Density Theorem. *Suppose that L/K is a Galois extension of number fields, with $[L:K]=n$. Let $\mathscr{C}$ be any conjugacy class of the group $\mathrm{Gal}(L/K)$. The proportion of prime ideals*

$\mathfrak{p}$ *of* K *whose Frobenius conjugacy class* $\left(\frac{L/K}{\mathfrak{p}}\right)$ *coincides with* $\mathscr{C}$ *is* $|\mathscr{C}|/n$.

To see that Chebotarev's theorem generalizes Kronecker's, one should recall that when $\mathfrak{p}$ is a prime ideal of K that is unramified in L, its Frobenius determines the *splitting type of* $\mathfrak{p}$ *in* L. Here and below, we use the term *splitting type* to refer to the number of prime ideals lying above $\mathfrak{p}$ and their (common) residue degree. The Frobenius conjugacy class is trivial (consists only of the identity) precisely when $\mathfrak{p}$ splits completely, and so Kronecker's theorem follows.

From the theorem of Chebotarev, one knows that the set of unramified primes with a given splitting type is either empty or of positive density. (In fact, this much can be deduced from a special case of Chebotarev's theorem, proved earlier by Frobenius.) Oftentimes, it is important to know how far one has to go to get ones hands on the smallest member of this set:

Problem. Let L/K be a Galois extension of number fields. Give an upper bound for the norm of the least unramified prime ideal $\mathfrak{p}$ of K possessing a prescribed splitting type in L (assuming at least one such prime ideal exists).

One answer is provided by a theorem of Lagarias, Montgomery, and Odlyzko [LMO79], who investigate the norm of the smallest prime ideal $\mathfrak{p}$ of L/K with a prescribed Frobenius conjugacy class. Their main result is that for a certain absolute constant A, this prime ideal $\mathfrak{p}$ satisfies

$$\mathbf{N}_{K/\mathbf{Q}}(\mathfrak{p}) \ll |D_L|^A, \tag{1}$$

where D_L is the discriminant of $L/\mathbf{Q}$ and both the exponent A and the implied constant are absolute. This is a deep and powerful result, but it has the unfortunate feature that the exponent A, while effectively computable, has never been computed. Moreover, it is an answer to a somewhat different question than the one that was asked; the Frobenius conjugacy class not only determines the splitting type of a prime ideal but usually overdetermines it! Said differently, many different Frobenius classes yield the same splitting type. So one might hope for a sharper result if one specifies only the splitting type.

In recent work, the PI has investigated the situation when $K = \mathbf{Q}$ and $L/\mathbf{Q}$ is abelian. In the split-completely case, he was able to show the following [Polc]:

Theorem 1. *If* $L/\mathbf{Q}$ *is an abelian extension of degree* n*, then the least split completely prime* p *satisfies*

$$p \ll_{n,\epsilon} |D_L|^{\frac{1}{4}+\epsilon}.$$

That is, (1) *holds with any* $A > \frac{1}{4}$*, if we allow the implied constant to depend on* n *and* A.

Theorem 1 had been known earlier for cyclic extensions of prime conductor by work of Elliott [Ell71], who in turn was generalizing results of Vinogradov and Linnik [VL66] for quadratic extensions. In [Pola], the PI proved a somewhat sharper result in the non-split-completely case:

Theorem 2. *Let* $L/\mathbf{Q}$ *be an abelian extension of degree* n*. Take a divisor* g *of* n *with* $g < n$*. If there is any unramified rational prime that splits into* g *distinct prime ideals in* L*, then the least such* p *satisfies*

$$p \ll_{n,\epsilon} f^{\frac{n}{8}+\epsilon}.$$

Here f *is the conductor of* $L/\mathbf{Q}$*, in other words, the least natural number for which* $L \subset \mathbf{Q}(e^{2\pi i/f})$.

It is elementary that $|D_L| \geq f^{n/2}$, so that the bound given in Theorem 2 is, in the worst-case, of the same quality as (1) for $A = \frac{1}{4} + \epsilon$.

The method of proof, which is an outgrowth of that used by Vinogradov–Linnik and Elliott (op. cit.), is substantially different than that of Lagarias et al. Most strikingly, it is essentially elementary (cf. Pintz [Pin77]), making almost no reference to zeros of L-functions and no essential use of contour integration. Theorems 1 and 2 can therefore be viewed as a victory for the "pretentious perspective" on analytic number theory that has been championed recently by Granville and Soundararajan (see, for example, [Gra09] and [Gra10]).

Research problem (Analogues for abelian extensions L/K). The PI proposes obtaining analogues of Theorems 1 and 2 for abelian extensions of number fields L/K with $K \neq \mathbf{Q}$. In the proofs of Theorems 1 and 2, one of the major technical devices is Burgess's bound on partial sums of Dirichlet characters [Bur63, Bur86]. Handling those cases when K is a nontrivial extension of $\mathbf{Q}$ will require estimates for partial sums of certain Hecke characters. Using Landau's generalization [Lan18] of the Pólya–Vinogradov inequality to characters of strict ray class groups, the PI expects to be able to show that for any represented splitting type, there is a corresponding prime ideal $\mathfrak{p}$ of K satisfying (1) once $A > \frac{1}{2}$, where now the implied constant may depend on both A and the degree of $L/\mathbf{Q}$. It seems plausible that recent subconvexity estimates for Hecke L-functions, as investigated (e.g.) by Venkatesh (see [Ven10, Theorem 6.1]), would allow one to break the $\frac{1}{2}$-barrier.

Research problem (Prime splitting averages across families of number fields). One can also ask statistical questions where instead of varying primes in an individual number field, one varies the number field across a family. A prototype is a mean-value theorem of Erdős [Erd61], who showed that the smallest inert prime, considereds over all quadratic fields of prime conductor, has average value $\sum_{k=1}^{\infty} p_k/2^k = 3.674643966\ldots$. Here p_k denotes the kth prime in increasing order. Elliott [Ell70] later showed that Erdős's result also holds with "inert" replace by "split-completely".

The proposer suggests investigating such averages taken over *all* number fields with a prescribed abelian Galois group. Fix a finite abelian group G, and fix a splitting type compatible with the structure of G. Now ask for the average value of the smallest rational prime with the given splitting type, where the average is taken over all abelian extensions $K/\mathbf{Q}$ with Galois group G, ordered by conductor. (One could also order the fields K by discriminant, but the results would be messier.) If $\alpha(p)$ denotes the proportion of those extensions $K/\mathbf{Q}$ in which the particular rational prime p splits in the desired fashion, a naive prediction for the average is

$$\sum_{p} p \cdot \alpha(p) \prod_{q<p} (1 - \alpha(q)), \tag{2}$$

where both p and q run over primes. Recent work of Wood [Woo10] shows how to describe these proportions $\alpha(p)$ for any given abelian group G and any given splitting type (and in particular ensures that these proportions are always well-defined). So in principle, the sum (2) can be explicitly computed.

Here two questions suggest themselves:

- For which groups G can it be proved that the average is really given by (2)? The proposer has proved this prediction when $G = \mathbf{Z}/2\mathbf{Z}$ or $G = \mathbf{Z}/3\mathbf{Z}$, and for all choices of splitting type. For $G = \mathbf{Z}/\ell\mathbf{Z}$, with prime $\ell \geq 5$, he has the same results but now conditional on the Generalized Riemann Hypothesis. (For all of this, see [Pol12a, Polb].) It would be very interesting to know if, assuming GRH, one could prove that the heuristic prediction is valid for *all* choices of G and all corresponding splitting types.

- How does the size of the expected average (2) vary as a function of the structure of G and the structure of the splitting type? Is there an asymptotic formula lurking somewhere in the background? It would be useful to collect some computational data on this question.

Several related questions could be asked and deserve to be studied. For example, what do the statistics look like if one averages over all fields of a fixed degree d, where the fields are now ordered by (the absolute value of their) discriminant? When $d = 3$, Martin and the PI [MP12] computed, conditional on the GRH, the average values of the least split-completely prime, the least-partially split prime, and the least inert prime. They made use of recent work of Taniguchi and Thorne [TT] counting cubic fields with prescribed splitting conditions (but earlier estimates of Belabas, Bhargava, and Pomerance might have sufficed [BBP10]). For arbitrary d, we do not even know how to count how many number fields there are of degree d and bounded discriminant, although there has been spectacular recent progress due to Bhargava. It would be interesting to investigate whether the known results are strong enough to compute, conditional on GRH, the corresponding averages for $d = 4$.

3 Value-distribution of the Euler function

Let $\phi(n) = \#(\mathbf{Z}/n\mathbf{Z})^\times$ denote Euler's totient function. Call an integer belonging to the range of ϕ a *totient*. In the 1920s, Pillai succeeded in showing that almost all numbers are not totients. His quantitative estimates were substantially improved by Erdős [Erd35b], who proved that if $V(x)$ denotes the count of totients in $[1, x]$, then

$$V(x) = x/(\log x)^{1+o(1)}, \quad \text{as } x \to \infty. \tag{3}$$

(The lower bound here follows immediately from the prime number theorem, since $\phi(p) = p - 1$, so the substance of the result is the upper bound.) Owing to the presence of the $o(1)$-term in an exponent, there is quite a bit of room to strengthen (3) in the direction of a true asymptotic formula. The best result to date is due to Kevin Ford [For98] who, majorizing a substantial amount of earlier work (see [EH73, EH76, Pom86, MP88]), gave the exact order of magnitude of $V(x)$: For constants $C = 0.817814\ldots$ and $D = 2.176968\ldots$, we have

$$V(x) \asymp \frac{x}{\log x} \exp(C(\log_3 x - \log_4 x)^2 + D\log_3 x - (D + 1/2 - 2C)\log_4 x) \tag{4}$$

for large x. Here $\log_k$ denotes the k-fold iterated logarithm.

In fact, Ford's determination of $V(x)$ is only one consequence of a substantial and intricate theory describing the multiplicative structure of totients and their preimages. The roots of this theory can be traced back to the work of Maier and Pomerance [MP88]. Let $\varrho = 0.542598586\ldots$ be the unique solution in $(0, 1)$ to the equation

$$\sum_{n=1}^{\infty} a_n \varrho^n = 1, \quad \text{where} \quad a_n = (n+1)\log(n+1) - n\log n - 1.$$

To establish their lower bound on $V(x)$, Maier and Pomerance considered numbers m whose jth largest prime factor (starting the numbering with $j = 0$) has size roughly $\exp((\log x)^{\varrho^j})$. They show that for this set of m, the set of corresponding totients $\phi(m)$ is rather large. Ford's proof of (4) depends on a much stronger assertion, namely that for *almost every* totient (asymptotically 100%), every one of its preimages has its prime factors constrained in a similar (but somewhat more complicated) manner.

The proposer was exposed to this theory while working with Ford on a conjecture of Erdős. More than fifty years ago, Erdős [Erd59] asked for a proof that there are infinitely many integers common to the range of the ϕ-function and the sum-of-divisors function σ. As Erdős's conjectures go, this one was fairly low-risk: If $p, p+2$ is a twin prime pair, then $\phi(p+2) = p+1 = \sigma(p)$. Similarly, if $2^p - 1$ is a Mersenne prime, then $\sigma(2^p - 1) = 2^p = \phi(2^{p+1})$. So if there are infinitely many twin prime pairs or infinitely many Mersenne primes, then Erdős's conjecture follows. So the truth of Erdős's conjecture is not so surprising. Perhaps more surprising is that it was not settled until 2010, in work of Ford, Luca, and Pomerance [FLP10]; their methods are very different from those used in the study of $V(x)$.

Let $V_{\phi,\sigma}(x)$ denote the number of integers in $[1, x]$ common to the range of ϕ and σ. The argument of Ford, Luca, and Pomerance (op. cit.) leads to a lower bound of the form $V_{\phi,\sigma}(x) \geq \exp((\log\log x)^c)$ for some $c > 0$ and all large x. How good is this? As we remarked above, Erdős proved that the number of ϕ-values in $[1, x]$ is of size $x/(\log x)^{1+o(1)}$, and his argument applies also for σ-values. So if being a ϕ-value and being a σ-value were independent, we might expect that $V_{\phi,\sigma}(x) \approx x/(\log x)^2$. This is much larger than the lower bound obtained Ford et al. Conditional on a suitable generalization of the twin prime conjecture, Ford and the proposer [FP11] have shown that the count of common values is much larger still;

$$V_{\phi,\sigma}(x) = x/(\log x)^{1+o(1)} \quad (x \to \infty).$$

Thus (conditionally) there is a very strong correlation between being a ϕ-value and being a σ-value. In a separate paper [FP], we have shown (unconditionally) limits to this correlation; almost all values of the ϕ-function are not values of the σ-function, and vice-versa. For both results, the insights of Ford's structure theory are essential.

Research problem (Further consequences of Ford's structure theory). The PI suggests investigating other consequences of Ford's structure theory. For example, by modifying the proof of the upper bound on $V_{\phi,\sigma}(x)$ in [FP], the proposer believes the following result can be proved: *For almost all (asymptotically 100%) totients v, the elements of the preimage set $\phi^{-1}(v)$ all share the same largest prime factor.* In fact, not only should the largest prime factors agree, but so should the k largest prime factors for any fixed k; one should even be able to take k as a function of x, and perhaps even large enough that it accounts for almost all of the prime factors of every preimage. This project would be joint work with Kevin Ford.

Research problem (Square totients). How often is a ϕ-value a square? There are at least two ways of hearing this question. On one interpretation, we are asking for an estimate of the count of $n \leq x$ for which $\phi(n)$ is a square. This problem was investigated by Banks et al. [BFPS04], who showed that this count exceeds $x^{0.7038}$ for large x; moreover, under reasonable conjectures, the exponent 0.7038 can be taken arbitrarily close to 1. The PI proposes researching the question from another angle: If we start with the set of totients, how frequently do we run into square values? So the object now is now is to count numbers in the image of ϕ that are square values, not their preimages.

It seems quite likely, in analogy with (3), that the number of square totients in $[1, x]$ has the form $x^{1/2}/(\log x)^{c+o(1)}$ as $x \to \infty$, for some positive constant c. What can be proved? From work of Freiberg [Fre] or independent work of Banks and Luca [BL11], one can deduce a lower bound of $x^{1/2}/(\log x)^C$ for some constant C. In fact, this lower bound holds already for square totients of the form $\phi(pq)$, for distinct primes p and q.

What about the upper bound? It is surely true that almost all squares are not totients, but even this modest result has so far eluded us! Carl Pomerance suggests that techniques from recent joint work of his with Florian Luca (concerning the range of the Carmichael function $\lambda(n)$) might be helpful in attacking this problem. More speculatively, one wonders if there is a structure theory of square totients, analogous to that developed by Ford for all totients.

This project brings with it the possibility of joint work with Florian Luca and Carl Pomerance.

4 The distribution of perfect numbers, amicable pairs, and their relatives

Let $s(n) = \sigma(n) - n$, so that $s(n)$ gives the sum of the proper divisors of the natural number n. The function $s(n)$ is perhaps the first arithmetic function to attract serious attention from research mathematicians, dating back to work of the Pythagorean school five centuries B.C.E. Despite the long history of this subject, a wealth of unsolved problems remain.

Recall that a natural number n is said to be *perfect* if $s(n) = n$ (for example, $n = 6$ or $n = 28$). We do not know if there are infinitely many perfect numbers (though we strongly suspect that there are), nor do we know if there are any odd perfect numbers (it is suspected, maybe a little less strongly, that there are not). Similarly, we do not know whether there are infinitely many *amicable pairs*, pairs of distinct natural numbers m and n where $s(m) = n$ and $s(n) = m$. The smallest amicable pair, known already to the Pythagoreans, is 220 and 284. We know more than 10 million examples of amicable pairs, but there is no proof in sight that there are infinitely many. (For a survey of known results, see [GPtR04].)

From a dynamical systems standpoint, the *sociable numbers* are a natural generalization of both perfect numbers and amicable pairs. A number n is called *sociable* if the sequence n, $s(n)$, $s(s(n))$, $s(s(s(n))), \dots$ is purely periodic; if the period length is k, then n is called *k-sociable* and the set $\{n, s(n), s(s(n)), \dots\}$ is called a *sociable k-cycle*. Note that the perfect numbers are precisely the 1-sociable integers, while a number n is 2-sociable exactly when it is a member of an amicable pair (with other member $s(n)$). For $k \geq 3$, the k-sociable numbers began to be studied at the end of the 19th century, by mathematicians such as Dickson, Catalan, and Perrott. Currently there are 217 known sociable cycles (see [Moe]): 206 of these have length 4, one has length 5, five have length 6, three have length 8, one has length 9, and one has length 28.

Our ignorance about sociable numbers is truly impressive (or depressing). We do not even know if there are infinitely many sociable cycles in total (making no restrictions on the length)!

In the face of such ignorance, what is one to do? Erdős's idea was to take a statistical perspective. Perhaps one doesn't know how to show, for example, that there are infinitely many amicable pairs. But maybe one can prove a result in the opposite direction, that amicable pairs are not too frequent. This new perspective was responsible for the first progress on these problems in two thousand years. In 1955, Erdős showed that the set of numbers belonging to an amicable pair has asymptotic density zero. Twenty years later, he used a more sophisticated version of the same method to show that for each fixed k, the set of k-sociable numbers has density zero [Erd76].

The PI believes it would be interesting to further investigate the distribution of the k-sociable numbers. Let $N_k(x)$ denote the count of k-sociable numbers in $[1, x]$. (So from the just-mentioned work of Erdős, we know that $N_k(x) = o(x)$, as $x \to \infty$.)

Research problem (Improved upper bounds for perfect numbers). For the count of perfect numbers in $[1, x]$, one knows from work of Hornfeck and Wirsing [HW57] that $N_1(x) \ll_\epsilon x^\epsilon$ for each fixed $\epsilon > 0$. The sharpest quantitative form of this result was given by Wirsing two years later [Wir59]: *For a certain absolute constant $W > 0$ and all $x > 3$, we have $N_1(x) \le x^{W/\log\log x}$.* The challenge of improving this 50-year old bound resurfaces regularly in the thoughts of the proposer. The difficulty of this task belies the fact that the true order of $N_1(x)$ is undoubtedly minuscule in comparison to Wirsing's bound; heuristic arguments suggest convincingly that $N_1(x) < \log x$ for large x.

What is stopping us from improving Wirsing's upper bound? It seems that the primary obstacle is the possible existence of perfect numbers n for which $\omega(n)$ (the number of distinct prime factors of n) is extraordinarily large. It is a well-known consequence of the prime number theorem that an arbitrary natural number in $[1, x]$ has at most $(1 + o(1)) \log x/ \log\log x$ distinct prime factors, as $x \to \infty$. Moreover, very few natural numbers come close to having this many prime divisors; most of the time, $\omega(n)$ hovers closely around $\log\log x$ (the substance of a celebrated theorem of Hardy and Ramanujan). A careful analysis of Wirsing's argument shows that his upper bound could be improved if one could show that each perfect number $n \le x$ satisfies $\omega(n) = o(\log x/ \log\log x)$, as $x \to \infty$. However, this does not seem easy. As a step in this direction, the PI proposes investigating the multiplicative structure of hypothetical perfect numbers $n \le x$ for which $\omega(n) \gg \log x/ \log\log x$.

It might be noted that the above thoughts on Wirsing's method inspired the work [Pol11c] of the proposer improving the known explicit upper bounds on the number of odd perfect numbers with a prescribed number of distinct prime factors.

Research problem (Improved upper bounds on sociable numbers of odd order). It is probably true for every k, one has $N_k(x) \ll_{k,A} x/(\log x)^A$ for any fixed A. Pomerance [Pom81] has proved this – and in fact a bit more – when $k = 2$. For $k > 2$, the situation is much less rosy. The sharpest upper bounds are due to Kobayashi, Pomerance and the proposer [KPP09], who showed that for every fixed k,

$$N_k(x) \ll x/ \exp((1 + o(1))\sqrt{\log_3 x \log_4 x}),$$

as $x \to \infty$. (As above, $\log_j$ denotes the j-fold iterated logarithm.) Note that the denominator here does not even grow as fast as $\log\log x$. For odd k, Kobayashi et al. obtained a somewhat stronger bound; their result was further improved by the proposer [Pol10b], who showed that in these cases,

$$N_k(x) \le x/(\log x)^{1+o(1)}, \quad \text{as } x \to \infty. \tag{5}$$

Almost any improvement of (5) would have interesting consequences: Enlarging the exponent from $1+o(1)$ in (5) to $1+\delta$ would give that the sum of the reciprocals of the k-sociable numbers converges (for odd k). It seems we may be just one idea away from this goal. It would be interesting to find that idea!

Research problem (Solitary numbers). There are many sequences related to the sociable numbers whose behavior merits further study. Here we focus on one particular example where it seems a theorem might be waiting in the wings. Say that the two natural numbers m and n are *friends* if $\sigma(m)/m = \sigma(n)/n$, and call a number *solitary* if it has no friends. What can be proved about the distribution of solitary numbers?

There is a very easily-described family of solitary numbers, those natural numbers n relatively prime to $\sigma(n)$. Indeed, suppose $\gcd(n, \sigma(n)) = 1$ but that $\sigma(m)/m = \sigma(n)/n$. Since the latter fraction is in lowest-terms (by assumption), we must have

$$m = kn \tag{6}$$

and

$$\sigma(m) = k\sigma(n) \tag{7}$$

for some positive integer k. Supposing $m \neq n$, we have $k > 1$. From (6), we see that the list of divisors of m includes 1 as well as all integers of the form kd where $d \mid n$. Thus,

$$\sigma(m) \geq 1 + k \sum_{d|n} d > k\sigma(n),$$

contradicting (7). So $k = 1$ and $m = n$, proving that n is solitary.

A result of Erdős (cf. [Erd48]) asserts that the number of $n \leq x$ for which n and $\sigma(n)$ are coprime is $(e^{-\gamma} + o(1))x/\log\log\log x$, as $x \to \infty$. So this same expression holds as a lower bound on the count of solitary numbers. Now on the one hand, this lower bound is small; since the denominator tends to infinity, we are capturing a vanishingly small proportion of the integers (as $x \to \infty$). However, as Dan Shanks quipped, "$\log\log\log x$ tends to infinity with great dignity". So as vanishingly small proportions go, it's on the large end of the scale – just a stone's throw away from a positive proportion.

The PI suggests investigating other families of solitary numbers, with one possible goal being a proof that a positive proportion of natural numbers are solitary. This problem was suggested by Carl Pomerance and may constitute joint work.

5 The distribution of irreducible polynomials over finite fields

Like so many stories in mathematics, this one begins with Gauss. In 1792 or 1793, when Gauss was 15 or 16, he made the following conjecture based on a careful study of the existing tables: *As $x \to \infty$, the count $\pi(x)$ of primes not exceeding x is asymptotic to $x/\log x$.* It would be another century before Gauss's guess could be confirmed; we know this result now as the *prime number theorem.*

Fast forwarding five years in Gauss's life, we find him writing his masterwork, the *Disquisitiones Arithmeticae*. For this work, Gauss prepared a chapter (cut from the final manuscript) discussing what modern mathematicians recognize as the rudiments of the theory of finite fields (see [Fre07]). Among the many results obtained by Gauss is a formula for $\pi(q; n)$, the number of monic irreducible polynomials of degree n over the field with q elements. After discarding less significant terms, one deduces from his formula that $\pi(q; n) \sim q^n/n$, whenever $q^n \to \infty$. The analogy with the prime number theorem is striking once we make the substitution $X = q^n$: Gauss's theorem then becomes the asymptotic formula $\pi(q; n) \sim X/\log X$ as $X \to \infty$, where the log must now be read as a base q logarithm.

This analogy between prime polynomials and prime numbers has been carried much further since the time of Gauss. In the early twentieth century, Landau's student Heinrich Kornblum proved an $\mathbf{F}_q[T]$-analogue of Dirichlet's theorem on primes in progressions (published posthumously as [Kor19]). A decade or so later, Emil Artin gave a version of the prime number theorem for these progressions, as part of his doctoral dissertation on quadratic function fields [Art24]. Even techniques of more modern vintage, such as sieve methods and the Hardy–Littlewood circle method, have now been generalized and applied to problems about polynomials. (For sieves, see [Che78, Web83, Car84a, Car84b, Hsu96]; for the circle method, see [Hay66, EH91b, EH91a, LW07, LW10, Pol11a].) And last year, Lê published a polynomial analogue of Green and Tao's pathbreaking theorem concerning arithmetic progressions in the primes [Lê11].

The PI proposes continuing his investigations (begun in his Ph.D. thesis [Pol08a]) into analogies between the distribution of irreducible polynomials and the distribution of prime numbers.

Research problem (weights of irreducible polynomials over $\mathbf{F}_2$). The weight of a polynomial in $\mathbf{F}_2[T]$ is defined as its number of nonzero coefficients. The proposer suggests investigating the parallels between the weight-distribution of irreducible polynomials and the distribution of the sum-of-binary-digits of rational primes.

From work of Kátai [Kát86], we know that the binary digits of the rational primes satisfy a central limit theorem: Let $s_2(n)$ denote the sum of the binary digits of n, and let $\operatorname{lb} x$ denote the binary (base 2) logarithm of x. Finally, let

$$\Phi(y) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} e^{-u^2/2}\, du$$

be the Gaussian cumulative distribution function. Then Kátai showed that $s_2(p)$ is normally distributed with mean $\frac{1}{2} \operatorname{lb} p$ and variance $\frac{1}{4} \operatorname{lb} p$; more precisely,

$$\frac{1}{\pi(x)} \#\{p \le x : s_2(p) \le \frac{1}{2} \operatorname{lb} x + y \frac{\sqrt{\operatorname{lb} x}}{2}\} \to \Phi(y), \quad \text{as } x \to \infty.$$

This is a direct analogue of the conjecture of Hicks, Mullen, and Sato (compare with [HMS02, Conjecture 2]) that the weights of irreducible polynomials of degree n over $\mathbf{F}_2$ are normally distributed with mean $n/2$ and variance $n/4$ (as $n \to \infty$). It would be very interesting to determine whether a suitable adaptation of Kátai's argument could prove this conjecture. Estimates for exponential sums over irreducibles, as developed by Hayes [Hay66] to study additive problems about primes in the polynomial context (cf. the present author's paper [Pol08b]), may be useful here.

If this project is successful, a further goal would be to investigate the existence of a local central limit law, providing an asymptotic formula for the number of irreducibles of degree n and weight k, for all values $k \approx n/2$. This would be analogous to a recent deep result of Drmota, Mauduit, and Rivat for rational primes [DMR09].

Research problem (twin primes with nonconstant difference). In his Ph.D. thesis, Chris Hall [Hal03, Hal06] proved an analogue of the twin prime conjecture for polynomials over finite fields. He showed that if $q > 3$, then there are infinitely many pairs of monic irreducible polynomials $A, A+1$ in $\mathbf{F}_q[T]$. The proof fits easily within a page; the key ingredient is Capelli's irreducibility criterion, which (in the needed form) goes back at least to the beginnings of the twentieth century. Extensions of Hall's results were given by the proposer [Pol08b]. He showed that Hall's twin prime result also holds when $q = 3$ and proves a corresponding theorem about "prime triples". More importantly, he showed that Hall's theorem is (at least for large q) a corollary of a very general theorem:

Theorem 3. *If $F_1(T), \dots, F_r(T)$ are irreducible polynomials over $\mathbf{F}_q$, and if q is sufficiently large in terms of the degrees of $F_1, \dots, F_r$, then there are infinitely many monic polynomials $G(T)$ for which all of $F_1(G(T)), \dots, F_r(G(T))$ are irreducible.*

To get Hall's result for large q, it suffices to choose $F_1(T) = T$ and $F_2(T) = T + 1$. In addition to Capelli's theorem, the proof of this last result used character sum bounds shown by Lenstra to follow from the Riemann Hypothesis for function fields.

Unfortunately, these methods are not robust enough to study twin prime pairs $P, P + D$, where D is *nonconstant*. The PI suggests further investigations in this area. The simplest problem of this type is to prove that there are infinitely many twin prime pairs over $\mathbf{F}_2$, where now a twin prime pair means a pair of irreducibles which differ by $T^2 + T$. A possible starting point is an intriguing observation of Effinger [Eff08] that $P = T^n + T^3 + T^2 + T + 1$ starts such a pair whenever P is irreducible.

Results from prior NSF support

The proposer was the recipient of an NSF Mathematical Sciences Postdoctoral Research Fellowship, award number DMS-0802970, from August 2008–July 2011. During his visit to the Institute for Advanced Study during the Fall 2009 term, he was also supported by NSF award DMS-0635607. What follows is a list of publications written while the author enjoyed the support of the MSPRF. Brief summaries are given for each paper. For full bibliographical details, please consult the list of "References cited."

- *Hypothesis H and an impossibility theorem of Ram Murty* [Pol10a]
  It is well-known that for certain arithmetic progressions, one can verify the conclusion of Dirichlet's theorem by elementary reasoning paralleling Euclid's argument for the infinitude of the primes. For example, it is an exercise in many undergraduate elementary number theory courses to prove Dirichlet's theorem for all coprime progressions modulo 4. In 1912, Schur [Sch12] showed that there is such an elementary proof for every progression $a \bmod m$ satisfying $a^2 \equiv 1 \pmod{m}$. Ram Murty [Mur88] showed that for a certain formal definition of "elementary proof", these are the only progressions for which Dirichlet's theorem admits an elementary proof. Here the PI considers a more lenient-seeming definition of "elementary proof" (suggested to him by N. Snyder) and shows, conditional on Schinzel's Hypothesis H, that the progressions identified by Schur remain the only ones for which an elementary proof exists.

- *A remark on sociable numbers of odd order* [Pol10b]
  This paper was discussed in §4 above. Here the proposer shows that for each fixed k, the count of k-sociable numbers in $[1, x]$ is at most $x/(\log x)^{1+o(1)}$, as $x \to \infty$. This improves on an earlier estimate of Kobyashi et al. [KPP09].

- *Revisiting Gauss's analogue of the prime number theorem for polynomials over a finite field* [Pol10c]
  Let p be a rational prime. Each polynomial $A \in \mathbf{F}_p[T]$ can be written in the form $\bar{a_0} + \bar{a_1}T + \cdots + \bar{a_n}T^n$, where each $a_0, \dots, a_n \in [0, p)$, and the bar denotes reduction modulo p. We assign to $A \in \mathbf{F}_p[T]$ the *norm* $\|A\| := \sum_{i \ge 0} a_i p^i \in \mathbf{N}$, and we let $\pi_p(X)$ be the counting function of

irreducible polynomials P over $\mathbf{F}_p$ with $\|P\| < X$. The main result of this paper is a formula for $\pi_p(X)$ with a square root error term. Specifically, if we set

$$\mathrm{ls}_p(X) := \sum_{\substack{\|A\|<X \\ \deg A>0}} \frac{1}{\deg A},$$

then for all $X \geq p$,

$$\pi_p(X) = \mathrm{ls}_p(X) + O(np^{n/2+1}),$$

where n is chosen as the unique integer with $p^n \leq X < p^{n+1}$. This should be seen as an analogue of the RH-conditional estimate $\pi(x) = \sum_{1<n\leq x} \frac{1}{\log n} + O(\sqrt{x}\log x)$ proved by von Koch in 1901.

- *On polynomial rings with a Goldbach property* [Pol11b]
  In 1965, David Hayes gave an elementary proof that the ring $R = \mathbf{Z}$ has the following *Goldbach property*: Every element of $R[T]$ of degree $n \geq 1$ can be written as a sum of two irreducible elements of $R[T]$ of degree n. Here the PI shows that this result holds in a fair amount of generality: One can take R as any Noetherian domain possessing infinitely many maximal ideals.

- *On Dickson's theorem concerning odd perfect numbers* [Pol11c]
  This paper was alluded to in §4. A 1913 theorem of Dickson [Dic13] asserts that for any fixed k, there are only finitely many odd perfect numbers n for which $\omega(n) \leq k$. The first explicit upper bound on n in terms of k was given by Pomerance [Pom77]; he showed that

  $$n < (4k)^{(4k)^{2^{k^2}}}.$$

  This was improved by Heath-Brown [HB94], Cook [Coo99], and finally Nielsen [Nie03], who gave the upper bound $n < 2^{4^k}$. In this paper, the PI takes a somewhat different perspective from these earlier works and asks for a bound on the number of possible such n, instead of a bound on the size of all such n. He obtains that the number of odd perfect n with $\omega(n) \leq k$ is bounded by 4^{k^2}. The proof uses the Heath-Brown–Cook–Nielsen work and a method of Wirsing [Wir59].

  This paper has inspired extensions by Chen and Luo [CL11], and Dai, Pan, and Tang [DPT].

- *Perfect numbers with identical digits* [Pol11d]
  A *repdigit* is a number with all of its digits identical in a given base. For example, 666 is a repdigit in base 10. The PI shows that in any given base, there are only finitely many perfect numbers which are repdigits; moreover, all such numbers are effectively bounded. In base 10, the only example is shown to be the (trivial) example $n = 6$.

- *Multiperfect numbers with identical digits* (joint w/ F. Luca) [LP11a]
  This paper extends most of the results of the just-mentioned paper to *multiply-perfect numbers*, numbers n for which $\sigma(n)$ is a proper multiple of n. (For example, $n = 120$ is multiply perfect, since $\sigma(120) = 3 \cdot 120$.) It is shown that in any given base, there are only finitely many multiply-perfect repdigits, and that when the base is 10, the number $n = 6$ is the only example.

The preceding two papers have inspired additional research by Kevin Broughan and collaborators [BZ12, Bro12, BGSF].

- *Long gaps between deficient numbers* [Pol11e]
  Call a number *deficient* whenever $s(n) < n$; e.g., $n = 10$ is deficient, since $s(10) = 1+2+5 = 8$. It is an elementary exercise to prove that there are arbitrarily large gaps between consecutive deficient numbers: It suffices to find a long string of numbers, each of which is divisible by "many" small primes, which can be accomplished by a straightforward application of the Chinese remainder theorem. Let $G(x)$ be the largest gap between two consecutive deficient numbers both belonging to the interval $[1, x]$. Erdős [Erd35a] showed that $G(x)/\log\log\log x$ is bounded between two positive constants, for all sufficiently large x. In this paper, the PI shows that $G(x)/\log\log\log x$ tends to a finite limit which is about 3.5.

- *On Hilbert's solution of Waring's problem* [Pol11f]
  A classical problem of Waring asks for the least integer $g(k)$ with the property that every nonnegative integer can be expressed as a sum of $g(k)$ nonnegative kth powers. For example, $g(4) = 4$, since every natural number is a sum of four squares and some (e.g., 7) cannot be written as a sum of fewer than four squares. Hilbert was the first to prove the existence of $g(k)$ for every k in 1909. Hilbert's method of proof fell out of favor after the realization of Hardy and Littlewood that much stronger results could be obtained by their "circle method." Here we show that a variant of Hilbert's original method is capable of establishing the upper bound $g(k) < (2k + 1)^{1808k^5}$.

- *Powerful amicable numbers* [Pol11g]
  A positive integer n is said to be *k-powerful* (or more simply *k-full*) if every prime dividing n appears to the kth power or greater. It is elementary to show that that the count of k-full numbers up to x has the same order of magnitude as the count of kth powers up to x, namely $x^{1/k}$. In this paper, the PI shows that for each fixed k, zero percent of the k-powerful numbers (in the limit) are members of an amicable pair. That is, the number of amicable k-powerful numbers in $[1, x]$ is $o(x^{1/k})$, as $x \to \infty$.

- *Values of the Euler and Carmichael functions which are sums of three squares* [Pol11h]
  It is shown that (asymptotically) 7/8 of positive integers n have the property that $\phi(n)$ is expressible as a sum of three squares. This should be compared with the classical result that 5/6 of all positive integers are so expressible. For Carmichael's function $\lambda(n)$, defined as the exponent of the group $(\mathbf{Z}/n\mathbf{Z})^\times$, it is shown that the set of n with $\lambda(n)$ expressible as a sum of three squares has positive lower density and upper density less than 1.

- *On some friends of the sociable numbers* [Pol10d]
  Fix an integer $k \geq 1$. Let $s_k(n)$ be the kth iterate of the sum-of-proper divisors function $s(n)$. Recall from §4 that a number is said to be k-sociable if $s_k(n) = n$. In this paper, it is shown that the set of positive integers n for which $s_k(n) \mid n$ has asymptotic density zero, and the same for the set of positive integers n for which $n \mid s_k(n)$.

- *The greatest common divisor of a number and its sum of divisors*[Pol11i]
  If a number is perfect or multiply perfect, then the greatest common divisor of n and $\sigma(n)$ is n itself, which is as large as possible. In this paper, the PI investigates the function

$G(x, A)$, defined as the number of $n \leq x$ for which $\gcd(n, \sigma(n)) > A$. (So if A is large, we are counting "near-multiperfect" numbers.) Along the way, he corrects some erroneous assertions of Erdős in this direction [Erd56]. A new result is that for fixed $\alpha \in (0, 1)$, we have $G(x, x^{\alpha}) = x^{1-\alpha+o(1)}$, as $x \to \infty$. The proof of the upper bound implicit in this assertion uses an adaptation of the method of Wirsing [Wir59], while the proof of the lower bound uses some ideas of Luca and Pomerance [LP07] used to study iterates of the Euler ϕ-function.

- *Quasi-amicable numbers are rare* [Pol11j]
  Let $s^{-}(n)$ denote the sum of the nontrivial divisors of n, where *nontrivial* excludes both 1 and n itself. A *quasi-amicable pair* is a pair of distinct positive integers n and m for which $s^{-}(n) = m$ and $s^{-}(m) = n$. Equivalently, n is a member of a quasi-amicable pair precisely when $s^{-}(s^{-}(n)) = n$. (See [Gar68, LF71, HL77] for empirical investigations into these pairs.) Borrowing ideas of Erdős, Granville, Pomerance, and Spiro [EGPS90] employed to study iterates of $s(\cdot)$, it is shown that the set of numbers which are members of a quasi-amicable pair has asymptotic density zero.

- *The exceptional set in the polynomial Goldbach problem* [Pol11a]
  This paper was mentioned in §5 above. Hardy and Littlewood's work in the 1920s on the circle method constitutes, together with the nearly concurrent work of Viggo Brun on sieves, one of the first serious attacks on the Goldbach conjecture. In [HL23], they showed that the Riemann Hypothesis for Dirichlet L-functions implies that every large odd integer can be written as a sum of three-primes. (This "three primes theorem" was later later proved unconditionally by Vinogradov.) They also showed, under the same hypothesis, that nearly all positive even integers are expressible as a sum of *two* primes: More precisely, the number of exceptions in $[1, x]$ to Goldbach's conjecture is $O_{\epsilon}(x^{1/2+\epsilon})$ for each $\epsilon > 0$. In this paper, the PI proves a corresponding result for sums of two irreducibles over a finite field. The results are unconditional, owing to Weil's Riemann Hypothesis for function fields.

- *The Möbius transform and the infinitude of primes* [Pol11k]
  The infinitude of primes is deduced from the following "uncertainty principle": If f and g are two arithmetic functions satisfying $g(n) = \sum_{d|n} f(d)$ (for all positive integers n) and both f and g have finite support, then both f and g are identically zero.

- *Remarks on a paper of Ballot and Luca concerning prime divisors of $a^{f(n)} - 1$* [Pol11l]
  Let $f(T) \in \mathbf{Q}[T]$ be a nonconstant, integer-valued polynomial with positive leading term. Suppose that there are infinitely many primes p for which f does not possess a root modulo p, and let r_f be the density of such primes. By the Chebotarev density theorem, $r_f > 0$. Assuming the GRH for Dedekind zeta functions, is proved that the number of primes $p \leq x$ which do not divide any number of the form $a^{f(n)} - 1$ is (as $x \to \infty$) bounded above by $x/(\log x)^{1+r_f+o(1)}$. Ballot and Luca [BL06] had this result with $\log \log x$ in the denominator instead of $\log x$. The method draws heavily on the techniques introduced by Hooley [Hoo67] in his GRH-conditional resolution of Artin's primitive root conjecture.

- *On common values of $\varphi(n)$ and $\sigma(m)$, I and II* (joint w/ K. Ford) [FP11, FP]
  The results of these papers were discussed in detail in §3 above.

- *Two remarks on iterates of Euler's totient function* [Pol11m]
  Let ϕ_k denote the kth iterate of Euler's ϕ-function. The first section of this paper presents

asymptotic formulas for the sums of $\phi_k(n)$ and $1/\phi_k(n)$, taken over $n \leq x$. In the second section, it is shown that for all but $x^{o(1)}$ primes $p \leq x$, the number of distinct primes dividing the infinite product $\prod_{k=1}^{\infty} \phi_k(p)$ at least $(\log p)^{\frac{1}{2}-\epsilon}$. This second result connects with recent deep work of Ford, Konyagin, and Luca [FKL10], who study a natural tree-structure on this set of primes [FKL10].

- *An arithmetic function arising from Carmichael's conjecture* (joint w/ F. Luca) [LP11b]
For every n, can one always find an $m \neq n$ for which $\phi(m) = \phi(n)$? In other words, is it true that a ϕ-value never has a single preimage? Carmichael claimed a proof of this assertion in 1907 [Car07]; he later retracted this claim [Car22] and proposed it as a conjecture. The conjecture is still open, but there have been interesting partial results. For example, using his detailed structure theory of totients, Ford [For98] showed that if there is a single ϕ-value that is a counterexample to Carmichael's conjecture, then a positive proportion of all ϕ-values are counterexamples. In this paper, Luca and the PI investigate the typical number of solutions m to the equation $\phi(m) = \phi(n)$. Call this number $F(n)$. Then Luca and the PI show that for any fixed $\epsilon > 0$, all but $o(x)$ natural numbers $n \leq x$ (as $x \to \infty$) satisfy
$$\exp\left((\frac{1}{2}-\epsilon)(\log\log x)^2(\log\log\log x)\right) < F(n) < \exp\left((\frac{3}{2}+\epsilon)(\log\log x)^2(\log\log\log x)\right).$$

- *On the parity of the number of multiplicative partitions and related problems* [Pol12b]
For each natural number n, let $f(n)$ denote the number of ways of writing n as a product of natural numbers, where the order of the factors is not taken into account. For example, $f(30) = 5$, corresponding to the five factorizations $2 \cdot 3 \cdot 5, 5 \cdot 6, 3 \cdot 10, 2 \cdot 15$, and 30. The function $f(n)$ is a multiplicative analogue of the "additive partition" function $p(n)$. The arithmetic properties of $p(n)$ have been the subject of many researches since the pioneering work of Ramanujan (see [AO01] for a survey). In this paper, congruence properties of $f(n)$ are investigated. It is proved that for any a and m, the density of integers n for which $f(n) \equiv a \pmod{m}$ exists. In the case $m = 2$, and $a = 1$, it is shown that that this density is about 57%. These results sharpen earlier work of Zaharescu and Zaki [ZZ10].

- *Prime-perfect numbers* (w/ C. Pomerance) [PP]
Call the natural number n *prime-perfect* if $\sigma(n)$ and n share the same set of distinct prime divisors. It is proved that the set of prime-perfect numbers is infinite, but that the counting function of prime-perfect numbers in $[1, x]$ is bounded by $x^{\frac{1}{3}+o(1)}$, as $x \to \infty$. It is conjectured that the $\frac{1}{3}$ in the exponent can be removed; this is an attractive target for future research.

- *How many primes can divide the values of a polynomial?* (w/ F. Luca) [LP]
Let $\Omega(n)$ denote the number of primes dividing n, counted with multiplicity. So, for example, $\Omega(18) = 3$, since $18 = 2 \cdot 3^2$. Let $F(T) \in \mathbf{Z}[T]$ be a nonconstant polynomial. In this paper, the proposer and Luca study both the minimal and maximal orders of $\Omega(F(n))$. For the minimal order, they propose a conjecture for $\liminf_{n\to\infty} \Omega(F(n))$ which is shown to be equivalent to Schinzel's Hypothesis H concerning simultaneous prime values of polynomials. For the maximal order, they prove that $\limsup_{n\to\infty} \Omega(F(n))/\log n = 1/\log \ell$, where ℓ is the least prime for which F has a zero in the ℓ-adic integers $\mathbf{Z}_\ell$. The proof of the upper bound depends on Schmidt's powerful subspace theorem from Diophantine analysis. The upper-bound result

generalizes earlier work of Erdős and Nicolas [EN80], who treated the case $F(T) = T(T+1)$ using a version of Roth's theorem.

References cited

[AO01] S. Ahlgren and K. Ono, *Congruences and conjectures for the partition function*, q-series with applications to combinatorics, number theory, and physics (Urbana, IL, 2000), Contemp. Math., vol. 291, Amer. Math. Soc., Providence, RI, 2001, pp. 1–10.

[Art24] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen. I and II*, Math. Z. **19** (1924), 153–246.

[BBP10] K. Belabas, M. Bhargava, and C. Pomerance, Error estimates for the Davenport-Heilbronn theorems, Duke Math. J. **153** (2010), 173–201.

[BFPS04] W. D. Banks, J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, *Multiplicative structure of values of the Euler function*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 29–47.

[BL06] C. Ballot and F. Luca, *Prime factors of $a^{f(n)}-1$ with an irreducible polynomial $f(x)$*, New York J. Math. **12** (2006), 39–45. Available electronically at `http://nyjm.albany.edu`.

[BL11] W. D. Banks and F. Luca, *Power totients with almost primes*, Integers **11A** (2011), 7 pp.; available electronically at `http://www.integers-ejcnt.org`.

[BGSF] K. A. Broughan, S. Guzman, S. Sanchez, and F. Luca, *Perfect repdigits*, Math. Comp. (to appear).

[BZ12] K. A. Broughan and Q. Zhou, *Odd Repdigits to Small Bases are Not Perfect*, Integers **12** (2012), 16 pp.; available electronically at `http://www.integers-ejcnt.org`.

[Bro12] K. A. Broughan, *An explicit bound for aliquot cycles of repdigits*, Integers **12** (2012), 14 pp.; available electronically at `http://www.integers-ejcnt.org`.

[Bur63] D. A. Burgess, *On character sums and L-series. II*, Proc. London Math. Soc. (3) **13** (1963), 524–536.

[Bur86] ———, *The character sum estimate with $r = 3$*, J. London Math. Soc. (2) **33** (1986), 219–226.

[Car07] R. D. Carmichael, *On Euler's φ-function*, Bull. Amer. Math. Soc. **13** (1907), 241–243.

[Car22] ———, *Note on Euler's φ-function*, Bull. Amer. Math. Soc. **28** (1922), 109–110.

[Car84a] M. Car, *Le théorème de Chen pour $\mathbf{F}_q[X]$*, Dissertationes Math. (Rozprawy Mat.) **223** (1984), 54.

[Car84b] ———, *Polynômes irréductibles de $F_q[X]$ de la forme $M + N$ où N est norme d'un polynôme de $F_{q^2}[X]$*, Dissertationes Math. (Rozprawy Mat.) **238** (1984), 50.

[Che78] J. Cherly, *A lower bound theorem in $F_q[x]$*, J. Reine Angew. Math. **303/304** (1978), 253–264.

[CL11] S.-C. Chen and H. Luo, *Bounds for odd k-perfect numbers*, Bull. Aust. Math. Soc. **84** (2011), 475–480.

[Coo99] R. J. Cook, *Bounds for odd perfect numbers*, Number theory (Ottawa, ON, 1996), CRM Proc. Lecture Notes, vol. 19, Amer. Math. Soc., Providence, RI, 1999, pp. 67–71.

[Dic13] L. E. Dickson, *Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors*, Amer. J. Math. **35** (1913), 413–422.

[DMR09] M. Drmota, C. Mauduit, and J. Rivat, *Primes with an average sum of digits*, Compos. Math. **145** (2009), 271–292.

[DPT] L.-X. Dai, H. Pan, and C.-E. Tang, *Note on odd multiperfect numbers*, Bull. Aust. Math. Soc. (to appear).

[Eff08] G. Effinger, *Toward a complete twin primes theorem for polynomials over finite fields*, Finite fields and applications, Contemp. Math., vol. 461, Amer. Math. Soc., Providence, RI, 2008, pp. 103–110.

[EH73] P. Erdős and R. R. Hall, *On the values of Euler's ϕ-function*, Acta Arith. **22** (1973), 201–206.

[EH76] ———, *Distinct values of Euler's ϕ-function*, Mathematika **23** (1976), 1–3.

[EH91a] G. W. Effinger and D. R. Hayes, *Additive number theory of polynomials over a finite field*, Oxford Mathematical Monographs, Oxford University Press, New York, 1991.

[EH91b] ———, *A complete solution to the polynomial 3-primes problem*, Bull. Amer. Math. Soc. (N.S.) **24** (1991), 363–369.

[Ell70] P. D. T. A. Elliott, *On the mean value of $f(p)$*, Proc. London Math. Soc. (3) **21** (1970), 28–96.

[Ell71] ———, *The least prime k-th-power residue*, J. London Math. Soc. (2) **3** (1971), 205–210.

[EGPS90] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions*, Analytic number theory (Allerton Park, IL, 1989), Progr. Math., vol. 85, Birkhäuser, Boston, 1990, pp. 165–204.

[EN80] P. Erdős and J.-L. Nicolas, *Sur la fonction "nombre de facteurs premiers de n"*, Séminaire Delange-Pisot-Poitou, 20e année: 1978/1979. Théorie des nombres, Fasc. 2 (French), Secrétariat Math., Paris, 1980, Exp. No. 32, 19 pp.

[Erd35a] P. Erdős, *Note on consecutive abundant numbers*, J. London Math. Soc. **10** (1935), 128–131.

[Erd35b] ———, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ-function*, Quart. J. Math. **6** (1935), 205–213.

[Erd48] ———, *Some asymptotic formulas in number theory*, J. Indian Math. Soc. **12** (1948).

[Erd55] ———, *On amicable numbers*, Publ. Math. Debrecen **4** (1955), 108–111.

[Erd56] ———, *On perfect and multiply perfect numbers*, Ann. Mat. Pura Appl. **42** (1956), 253–258.

[Erd59] ———, *Remarks on number theory. II. Some problems on the σ function*, Acta Arith. **5** (1959), 171–177.

[Erd61] ———, *Remarks on number theory. I*, Mat. Lapok **12** (1961), 10–17 (Hungarian).

[Erd76] ———, *On asymptotic properties of aliquot sequences*, Math. Comp. **30** (1976), 641–645.

[FKL10] K. Ford, S. V. Konyagin, F. Luca, *Prime chains and Pratt trees*, Geom. Funct. Anal. **20** (2010), 1231–1258.

[FLP10] K. Ford, F. Luca, and C. Pomerance, *Common values of the arithmetic functions ϕ and σ*, Bull. Lond. Math. Soc. **42** (2010), 478–488.

[For98] K. Ford, *The distribution of totients*, Ramanujan J. **2** (1998), no. 1-2, 67–151; corrected electronic version available as `arXiv:1104.3264`.

[FP11] K. Ford and P. Pollack, *On common values of $\phi(n)$ and $\sigma(m)$. I*, Acta Math. Hungar. **133** (2011), 251–271.

[FP] ———, *Common values of $\phi(n)$ and $\sigma(m)$, II*, Algebra Number Theory, to appear.

[Fre] T. Freiberg, *Products of shifted primes simultaneously taking perfect power values*, e-print available as `arXiv:1008.1978`.

[Fre07] G. Frei, *The unpublished section eight: on the way to function fields over a finite field*, The shaping of arithmetic after C. F. Gauss's *Disquisitiones arithmeticae*, Springer, Berlin, 2007, pp. 159–198.

[Gar68] M. García, *Números casi amigos y casi sociables*, Revista Annal (1968).

[GPtR04] M. García, J. M. Pedersen, and H. te Riele, *Amicable pairs, a survey*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 179–196.

[Gra09] A. Granville, *Pretentiousness in analytic number theory*, Journal de Théorie de nombres de Bordeaux **21** (2009), 159–173.

[Gra10] ———, *Different approaches to the distribution of primes*, Milan J. Math. **78** (2010), 65–84.

[Hal03] C. J. Hall, *L-functions of twisted Legendre curves*, Ph.D. thesis, Princeton University, 2003.

[Hal06] ———, *L-functions of twisted Legendre curves*, J. Number Theory **119** (2006), 128–147.

[Hay66] D. R. Hayes, *The expression of a polynomial as a sum of three irreducibles*, Acta Arith. **11** (1966), 461–488.

[HB94] D. R. Heath-Brown, *Odd perfect numbers*, Math. Proc. Cambridge Philos. Soc. **115** (1994), 191–196.

[HL23] G. H. Hardy and J. E. Littlewood, *Some problems of Partitio Numerorum III: on the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.

[HL77] P. Hagis, Jr. and G. Lord, *Quasi-amicable numbers*, Math. Comp. **31** (1977), 608–611.

[Hoo67] C. Hooley, *On Artins conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[HMS02] K. H. Hicks, G. L. Mullen, and I. Sato, *Distribution of irreducible polynomials over* $\mathbf{F}_2$, Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), Springer, Berlin, 2002, pp. 177–186.

[Hsu96] C.-N. Hsu, *A large sieve inequality for rational function fields*, J. Number Theory **58** (1996), 267–287.

[HW57] B. Hornfeck and E. Wirsing, *Über die Häufigkeit vollkommener Zahlen*, Math. Ann. **133** (1957), 431–438.

[Kát86] I. Kátai, *Distribution of digits of primes in q-ary canonical form*, Acta Math. Hungar. **47** (1986), 341–359.

[Kor19] H. Kornblum, *Über die Primfunktionen in einer arithmetischen Progression*, Math. Zeitschrift **5** (1919), 100–111.

[KPP09] M. Kobayashi, P. Pollack, and C. Pomerance, *On the distribution of sociable numbers*, J. Number Theory **129** (2009), 1990–2009.

[Lan18] E. Landau, *Verallgemeinerung eines Pólyaschen Satzes auf algebraische Zahlkörper*, Göttinger Nachr. (1918), 478–488.

[Lê11] T. H. Lê, *Green-Tao theorem in function fields*, Acta Arith. **147** (2011), 129–152.

[LF71] M. Lal and A. Forbes, *A note on Chowla's function*, Math. Comp. **25** (1971), 923–925.

[LMO79] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), 271–296.

[LP07] F. Luca and C. Pomerance, *Irreducible radical extensions and Euler-function chains*, Combinatorial number theory, de Gruyter, Berlin, 2007, pp. 351–361.

[LP11a] F. Luca and P. Pollack, *Multiperfect numbers with identical digits*, J. Number Theory **131** (2011), 260–284.

[LP11b] ———, *An arithmetic function arising from Carmichael's conjecture*, J. Théor. Nombres Bordeaux **23** (2011), 697–714.

[LP] ———, *How many primes can divide the values of a polynomial?*, Acta Arith. (to appear).

[LW07] Y.-R. Liu and T. D. Wooley, *The unrestricted variant of Waring's problem in function fields*, Funct. Approx. Comment. Math. **37** (2007), 285–291.

[LW10] ———, *Waring's problem in function fields*, J. Reine Angew. Math. **638** (2010), 1–67.

[Moe] D. Moews, *A list of aliquot cycles of length greater than* 2, online resource; `http://djm.cc/sociable.txt`.

[MP12] G. Martin and P. Pollack, *The average least character nonresidue and further variations on a theme of Erdős*, J. London Math. Soc. (to appear).

[MP88] H. Maier and C. Pomerance, *On the number of distinct values of Euler's ϕ-function*, Acta Arith. **49** (1988), 263–275.

[Mur88] M. R. Murty, *Primes in certain arithmetic progressions*, Journal of the Madras University (1988), 161–169.

[Nie03] P. P. Nielsen, *An upper bound for odd perfect numbers*, Integers **3** (2003), 9 pp.; available electronically at `http://www.integers-ejcnt.org`.

[Pin77] J. Pintz, *Elementary methods in the theory of L-functions. VI. On the least prime quadratic residue* (mod p), Acta Arith. **32** (1977), 173–178.

[Pola] P. Pollack, *A problem on linear combinations of Dirichlet characters*, submitted; e-print available from `http://www.math.uga.edu/~pollack/work.html`.

[Polb] ———, *The smallest inert prime in a cyclic number field of prime degree*, submitted; e-print available from `http://www.math.uga.edu/~pollack/work.html`.

[Polc] ———, *The smallest prime that splits completely in an abelian number field*, submitted; e-print available from `http://www.math.uga.edu/~pollack/work.html`.

[Pol08a] ———, *Prime polynomials over finite fields*, Ph.D. thesis, Dartmouth College, 2008.

[Pol08b] ———, *An explicit approach to Hypothesis H for polynomials over a finite field*, The anatomy of integers: Proceedings of the Anatomy of Integers Conference, Montréal, March 2006 (J. M. de Koninck, A. Granville, and F. Luca, eds.), 2008, pp. 259–273.

[Pol10a] ———, *Hypothesis H and an impossibility theorem of Ram Murty*, Rend. Sem. Mat. Univ. Pol. Torino **68** (2010), 183–197.

[Pol10b] ———, *A remark on sociable numbers of odd order*, J. Number Theory **130** (2010), 1732–1736.

[Pol10c] ———, *Revisiting Gauss's analogue of the prime number theorem for polynomials over a finite field*, Finite Fields and their Applications **16** (2010), 290–299.

[Pol10d] ———, *On some friends of the sociable numbers*, Montash. Math. **162** (2010), 321–327.

[Pol11a] ———, *The exceptional set in the polynomial Goldbach problem*, Int. J. Number Theory **7** (2011), 579–591.

[Pol11b] ______, *On polynomial rings with a Goldbach property*, American Math. Monthly **118** (2011), 71–77.

[Pol11c] ______, *On Dickson's theorem concerning odd perfect numbers*, American Math. Monthly **118** (2011), 161–164, errata in **118** (2011), 953.

[Pol11d] ______, *Perfect numbers with identical digits*, Integers **11A** (2011), 11 pp; available electronically at `http://www.integers-ejcnt.org`.

[Pol11e] ______, *Long gaps between deficient numbers*, Acta Arith. **146** (2011), 33–42.

[Pol11f] ______, *On Hilbert's solution of Waring's problem*, Cent. Eur. J. Math **9** (2011), 294–301.

[Pol11g] ______, *Powerful amicable numbers*, Colloq. Math **122** (2011), 103–123.

[Pol11h] ______, *Values of the Euler and Carmichael functions which are sums of three squares*, Integers **11** (2011), 16 pp; available electronically at `http://www.integers-ejcnt.org`.

[Pol11i] ______, *The greatest common divisor of a number and its sum of divisors*, Michigan Math. J. **60** (2011), 199–214.

[Pol11j] ______, *Quasi-amicable numbers are rare*, J. Integer Sequences **14** (2011), article 11.5.2, 13 pp.; available online at `https://cs.uwaterloo.ca/journals/JIS/`.

[Pol11k] ______, *The Möbius transform and the infinitude of primes*, Elem. Math. **66** (2011), 118–120.

[Pol11l] ______, *Remarks on a paper of Ballot and Luca concerning prime divisors of* $a^{f(n)} - 1$, New York J. Math **17** (2011), 553-567. Available electronically at `http://nyjm.albany.edu`.

[Pol11m] ______, *Two remarks on iterates of Euler's totient function*, Arch. Math **97** (2011), 443–452.

[Pol12a] ______, *The average least quadratic nonresidue modulo* m *and other variations on a theme of Erdős*, J. Number Theory **132** (2012), 1185–1201.

[Pol12b] ______, *On the parity of the number of multiplicative partitions and related problems*, Proc. Amer. Math. Soc. **140** (2012), 3793–3803.

[Pom77] C. Pomerance, *Multiply perfect numbers, Mersenne primes, and effective computability*, Math. Ann. **226** (1977), 195–206.

[Pom81] ______, *On the distribution of amicable numbers. II*, J. Reine Angew. Math. **325** (1981), 183–188.

[Pom86] ______, *On the distribution of the values of Euler's function*, Acta Arith. **47** (1986), 63–70.

[PP] P. Pollack and C. Pomerance, *Prime-perfect numbers*, Integers, special issue in memory of J. L. Selfridge (to appear). Available online from `http://www.math.uga.edu/~pollack12BMack/work.html`.

[Sch12] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, Sitzungsber. Berl. Math. Ges. **11** (1912), 40–50.

[TT] T. Taniguchi and F. Thorne, *Secondary terms in counting functions for cubic fields*, submitted, e-print at `arXiv:1102.2914`.

[Ven10] A. Venkatesh, *Sparse equidistribution problems, period bounds and subconvexity*, Ann. of Math. (2) **172** (2010), 989–1094.

[VL66] A. I. Vinogradov and U. V. Linnik, *Hypoelliptic curves and the least prime quadratic residue*, Dokl. Akad. Nauk SSSR **168** (1966), 259–261 (Russian).

[VS] J. Vandehey and P. Spiegelhalter, *Squares in polynomial product sequences*, e-print available as `arXiv:1107.1730`.

[Web83] W. A. Webb, *Sieve methods for polynomial rings over finite fields*, J. Number Theory **16** (1983), 343–355.

[Wir59] E. Wirsing, *Bemerkung zu der Arbeit über vollkommene Zahlen*, Math. Ann. **137** (1959), 316–318.

[Woo10] M. M. Wood, *On the probabilities of local behaviors in abelian field extensions*, Compos. Math. **146** (2010), 102–128.

[ZZ10] A. Zaharescu and M. Zaki, *On the parity of the number of multiplicative partitions*, Acta Arith. **145** (2010), 221–232.

Biographical sketch: Paul Pollack

Education

University of Georgia	B.S., Mathematics	2003
Dartmouth College	M.A, Mathematics	2007
Dartmouth College	Ph.D., Mathematics	2008

Positions held

2012–	Assistant Professor, University of Georgia
2011-12	Postdoctoral Fellow, Department of Mathematics, joint appointment at University of British Columbia/Simon Fraser University
2008-11	J.L. Doob Research Assistant Professor and NSF Postdoctoral Fellow, University of Illinois at Urbana
2010	(Spring only) Visiting research scholar, Dartmouth College
2009	(Fall only) Member of the School of Mathematics, Institute for Advanced Study

Most relevant publications

E-prints of the proposer's unpublished papers are available from `http://www.math.uga.edu/~pollack/work.html`.

(1) P. Pollack, *A problem on linear combinations of Dirichlet characters*, submitted.
(2) G. Martin and P. Pollack, *The average least character nonresidue and further variations on a theme of Erdős*, J. London Math. Soc. (to appear).
(3) K. Ford and P. Pollack, *On common values of $\phi(n)$ and $\sigma(m)$, II*, Algebra and Number Theory (to appear).
(4) P. Pollack, *The exceptional set in the polynomial Goldbach problem*, Int. J. Number Theory **7** (2011), 579–591.
(5) M. Kobayashi, P. Pollack, and C. Pomerance, *On the distribution of sociable numbers*, J. Number Theory **129** (2009), 1990–2009.

Additional selected publications

(1) P. Pollack, *The smallest inert prime in a cyclic number field of prime degree*, submitted.
(2) P. Pollack, C. Pomerance, and E. Treviño, *Sets of monotonicity for Euler's totient function*, Ramanujan J. (to appear).
(3) P. Pollack, *The greatest common divisor of a number and its sum of divisors*, Michigan Math. J. **60** (2011), 199–214.
(4) P. Pollack, *Simultaneous prime specializations of polynomials over finite fields*, Proc. London Math. Soc. **97** (2008), 545–567.
(5) P. Pollack, *An explicit approach to Hypothesis H for polynomials over finite fields.* Anatomy of integers. Proceedings of a conference on the anatomy of integers, Montreal, March 13th-17th, 2006. Edited by J.M. de Koninck, A. Granville and F. Luca, pp. 259–273.

Synergistic activities

- **Refereeing:** Have refereed for Integers, the Amer. Math. Monthly, Bull. Aust. Math. Soc., Math. Comp., J. Integer Sequences, Algebra and Number Theory, Canad. Math. Bull., J. Number Theory, J. Combinatorics and Number Theory, Int. J. Number Theory, and the Handbook of Finite Fields.
- **Special session organizer** (with L. Goldmakher, M. Milinovich, J. Kish): Co-organized the special session at the 2012 AMS/MAA Joint Meetings titled "New perspectives on multiplicative number theory." This was a special session following up on an NSF-sponsored Mathematics Research Communities workshop ("The pretentious view of analytic number theory").
- **Work with high school students:** Since 2001, the University of Georgia has organized a high school math tournament for students in Georgia and neighboring states. For the 2012 contest, the proposer was one of the primary test writers; he co-wrote the written round (joint with Ted Shifrin and Mo Hendon) and the team round (joint with Boris and Valery Alexeev). The PI has also been a frequent guest lecturer (most recently in 2009) at the Ross Summer Mathematics Program, a mathcamp for high school students held annually at Ohio State University.
- **Graduate mentoring:** During the summer of 2009, the PI served as a REGS mentor at the University of Illinois (REGS = **R**esearch **E**xperiences for **G**raduate **S**tudents.) He advised Joseph Vandehey and Paul Spiegelhalter. Their project resulted in a paper which the PI expects to see accepted soon at a research journal.
- **CIMPA/ICTP summer school:** During the summer of 2013, the PI will teach a one-week course in Manila as part of a summer school on algebraic curves. The summer school is sponsored by CIMPA (International Centre for Pure and Applied Mathematics) and ICTP (the Abdus Salam International Centre for Theoretical Physics); both of these are organizations aiming to promote scientific education in the developing world.

Other affiliations

Collaborators: Kevin Ford, University of Illinois; Luis Gallardo, Université de Bretagne Occidentale; Mitsuo Kobayashi, Cal Poly Pomona; Florian Luca, Universidad Nacional Autónoma de México; Greg Martin, University of British Columbia; Carl Pomerance, Dartmouth College; Olivier Rahavandrainy, Université de Bretagne Occidentale; Vladimir Shevelev, Ben-Gurion University of the Negev; Ethan Smith, Liberty University; Lola Thompson, University of Georgia; Enrique Treviño, Swarthmore College.

Graduate and postdoctoral advisors: Carl Pomerance, Dartmouth College (graduate); Kevin Ford, University of Illinois at Urbana-Champaign (postdoctoral); Greg Martin, University of British Columbia (postdoctoral).

Thesis committees served on: 1, Lola Thompson (Dartmouth College, 2012)

Total number of graduate students advised: 0

Total number of postdoctoral scholars sponsored: 1, Lola Thompson (UGA, current)