APPLICATIONS OF PROBABILITY: BENFORD'S LAW AND HYPOTHESIS TESTING

FROM *AN INVITATION TO MODERN NUMBER THEORY*

STEVEN J. MILLER AND
RAMIN TAKLOO-BIGHASH

CONTENTS

These notes are from *An Invitation to Modern Number Theory*, by Steven J. Miller and Ramin Takloo-Bighash (Princeton University Press, 2006). PLEASE DO NOT DISTRIBUTE THESE NOTES FURTHER. As this is an excerpt from the book, there are many references to other parts of the book; these appear as ?? in the text below.

1. APPLICATIONS OF PROBABILITY: BENFORD'S LAW AND HYPOTHESIS TESTING

The Gauss-Kuzmin Theorem (Theorem **??**) tells us that the probability that the millionth digit of a randomly chosen continued fraction expansion is k is approximately $q_k = \log_2\left(1 + \frac{1}{k(k+2)}\right)$. What if we choose N algebraic numbers, say the cube roots of N consecutive primes: how often do we expect to observe the millionth digit equal to k? If we believe that algebraic numbers other than rationals and quadratic irrationals satisfy the Gauss-Kuzmin Theorem, we expect to observe $q_k N$ digits equal to k, and probably fluctuations on the order of $\sqrt{N}$. If we observe M digits equal to k, how confident are we (as a function of M and N, of course) that the digits are distributed according to the Gauss-Kuzmin Theorem? This leads us to the subject of **hypothesis testing**: if we assume some process has probability p of success, and we observe M successes in N trials, does this provide support for or against the hypothesis that the probability of success is p?

We develop some of the theory of hypothesis testing by studying a concrete problem, the distribution of the first digit of certain sequences. In many problems (for example, 2^n base 10), the distribution of the first digit is given by Benford's Law, described below. We first investigate situations where we can easily prove the sequences are Benford, and then discuss how to analyze data in harder cases where the proofs are not as clear (such as the famous $3x+1$ problem). The error analysis is, of course, the same as the one we would use to investigate whether or not the digits of the continued fraction expansions of algebraic numbers satisfy the Gauss-Kuzmin Theorem. In the process of investigating Benford's Law, we encounter equidistributed sequences (Chapter **??**), logarithmic probabilities (similar to the Gauss-Kuzmin probabilities in Chapter **??**), and Poisson Summation (Chapter **??**), as well as many of the common problems in statistical testing (such as non-independent events and multiple comparisons).

1.1. **Benford's Law.** While looking through tables of logarithms in the late 1800s, Newcomb noticed a surprising fact: certain pages were significantly more worn out than others. People were looking up numbers whose logarithm started with 1 more frequently than other digits. In 1938 Benford [Ben] observed the same digit bias in a variety of phenomenon. See [Hi1, Rai] for a description and history, [Hi2, BBH, KonMi, LaSo, MN] for recent results, [Knu] for connections between Benford's law and rounding errors in computer calculations and [Nig1, Nig2] for applications of Benford's Law by the IRS to detect corporate tax fraud!

A sequence of positive numbers $\{x_n\}$ is **Benford (base** b**)** if the probability of observing the first digit of x_n in base b is j is $\log_b\left(1+\frac{1}{j}\right)$. More precisely,

$$\lim_{N\to\infty}\frac{\#\{n\leq N : \text{first digit of } x_n \text{ in base } b \text{ is } j\}}{N} \ = \ \log_b\left(1+\frac{1}{j}\right). \tag{1}$$

Note that $j\in\{1,\dots,b-1\}$. This is a probability distribution as one of the $b-1$ events must occur, and the total probability is

$$\sum_{j=1}^{b-1}\log_b\left(1+\frac{1}{j}\right) \ = \ \log_b\prod_{j=1}^{b-1}\left(1+\frac{1}{j}\right) \ = \ \log_b\prod_{j=1}^{b-1}\frac{j+1}{j} \ = \ \log_b b \ = \ 1. \tag{2}$$

It is possible to be Benford to some bases but not others; we show the first digit of 2^n is Benford base 10, but clearly it is not Benford base 2 as the first digit is always 1. For many processes, we obtain a sequence of points, and the distribution of the first digits are Benford. For example, consider the **3x+1 problem**. Let a_0 be any positive integer, and consider the sequence where

$$a_{n+1} \ = \ \begin{cases}3a_n+1 & \text{if } a_n \text{ is odd}\\ a_n/2 & \text{if } a_n \text{ is even.}\end{cases} \tag{3}$$

For example, if $a_0=13$, we have

$$\begin{aligned} 13 \ &\longrightarrow\ 40 \longrightarrow 20 \longrightarrow 10 \longrightarrow 5 \longrightarrow 16 \longrightarrow 8 \longrightarrow 4 \longrightarrow 2 \longrightarrow 1\\ &\longrightarrow\ 4 \longrightarrow 2 \longrightarrow 1 \longrightarrow 4 \longrightarrow 2 \longrightarrow 1 \cdots . \end{aligned} \tag{4}$$

An alternate definition is to remove as many powers of two as possible in one step. Thus

$$a_{n+1} \ = \ \frac{3a_n+1}{2^k}, \tag{5}$$

where k is the largest power of 2 dividing $3a_n+1$. It is conjectured that for *any* a_0, eventually the sequence becomes $4\to2\to1\to4\cdots$ (or in the alternate definition $1\to1\to1\cdots$). While this is known for all $a_0\leq 2^{60}$, the problem has resisted numerous attempts at proofs (Kakutani has described the problem as a conspiracy to slow down mathematical research because of all the time spent on it). See [Lag1, Lag2] for excellent surveys of the problem. How do the first digits behave for a_0 large? Do numerical simulations support the claim that this process is Benford? Does it matter which definition we use?

Exercise 1.1. *Show the Benford probabilities* $\log_{10}\left(1+\frac{1}{j}\right)$ *for* $j \in \{1,\dots,9\}$ *are irrational. What if instead of base ten we work in base* d *for some integer* d*?*

Exercise 1.2. *Below we use the definition of the* $3x+1$ *map from* (5). *Show there are arbitrarily large integers* N *such that if* $a_0 = N$ *then* $a_1 = 1$. *Thus, infinitely often, one iteration is enough to enter the repeating cycle. More generally, for each positive integer* k *does there exist arbitrarily large integers* N *such that if* $a_0 = N$ *then* $a_j > 1$ *for* $j < k$ *and* $a_k = 1$*?*

1.2. **Benford's Law and Equidistributed Sequences.** As we can write any positive x as b^u for some u, the following lemma shows that it suffices to investigate $u \bmod 1$:

Lemma 1.3. *The first digits of* b^u *and* b^v *are the same in base* b *if and only if* $u \equiv v$ *mod* 1.

Proof. We prove one direction as the other is similar. If $u \equiv v \bmod 1$, we may write $v = u + m$, $m \in \mathbb{Z}$. If

$$b^u \ = \ u_k b^k + u_{k-1}b^{k-1} + \cdots + u_0 + u_{-1}b^{-1} + \cdots, \tag{6}$$

then

$$\begin{aligned} b^v &= b^{u+m} \\ &= b^u \cdot b^m \\ &= (u_k b^k + u_{k-1}b^{k-1} + \cdots + u_0 + u_{-1}b^{-1} + \cdots)b^m \\ &= u_k b^{k+m} + \cdots + u_0 b^m + u_{-1}b^{m-1} + \cdots . \end{aligned} \tag{7}$$

Thus the first digits of each are u_k, proving the claim. □

Exercise 1.4. *Prove the other direction of the if and only if.*

Consider the unit interval $[0,1)$. For $j \in \{1,\dots,b\}$, define p_j by

$$b^{p_j} = j \quad \text{or equivalently} \quad p_j \ = \ \log_b j. \tag{8}$$

For $j \in \{1,\dots,b-1\}$, let

$$I_j^{(b)} \ = \ [p_j, p_{j+1}) \ \subset [0,1). \tag{9}$$

Lemma 1.5. *The first digit of* b^y *base* b *is* j *if and only if* y *mod* $1 \in I_j^{(b)}$.

Proof. By Lemma 1.3 we may assume $y \in [0,1)$. Then $y \ \in I_j^{(b)} = [p_j, p_{j+1})$ if and only if $b^{p_j} \le y < b^{p_{j+1}}$, which from the definition of p_j is equivalent to $j \le b^y < j+1$, proving the claim. □

The following theorem shows that the exponentials of equidistributed sequences (see Definition **??**) are Benford.

Theorem 1.6. *If* $y_n = \log_b x_n$ *is equidistributed mod* 1 *then* x_n *is Benford (base* b*).*

Proof. By Lemma 1.5,

$$\begin{aligned} &\{n \le N : y_n \bmod 1 \in [\log_b j, \log_b(j+1))\} \\ &\qquad = \ \{n \le N : \text{first digit of } x_n \text{ in base } b \text{ is } j\}. \end{aligned} \tag{10}$$

Therefore

$$\begin{aligned} &\lim_{N\to\infty} \frac{\#\{n \le N : y_n \bmod 1 \in [\log_b j, \log_b(j+1))\}}{N} \\ &\qquad = \ \lim_{N\to\infty} \frac{\#\{n \le N : \text{first digit of } x_n \text{ in base } b \text{ is } j\}}{N}. \end{aligned} \tag{11}$$

If y_n is equidistributed, then the left side of (11) is $\log_b\left(1+\frac{1}{j}\right)$ which implies x_n is Benford base b. □

Remark 1.7. One can extend the definition of Benford's Law from statements concerning the distribution of the first digit to the distribution of the first k digits. With such an extension, Theorem 1.6 becomes $y_n = \log_b x_n \bmod 1$ is equidistributed if and only if x_n is Benford base b. See [KonMi] for details.

Let $\{x\} = x - [x]$ denote the fractional part of x, where $[x]$ as always is the greatest integer at most x. In Theorem **??** we prove that for $\alpha \notin \mathbb{Q}$ the fractional parts of $n\alpha$ are equidistributed modulo 1. From this and Theorem 1.6, it immediately follows that geometric series are Benford (modulo the irrationality condition):

Theorem 1.8. *Let $x_n = ar^n$ with $\log_b r \notin \mathbb{Q}$. Then x_n is Benford (base b).*

Proof. Let $y_n = \log_b x_n = n \log_b r + \log_b a$. As $\log_b r \notin \mathbb{Q}$, by Theorem **??** the fractional parts of y_n are equidistributed. Exponentiating by b, we obtain that x_n is Benford (base b) by Theorem 1.6. □

Theorem 1.8 implies that 2^n is Benford base 10, but not surprisingly that it is not Benford base 2.

Exercise 1.9. *Do the first digits of e^n follow Benford's Law? What about $e^n + e^{-n}$?*

1.3. **Recurrence Relations and Benford's Law.** We show many sequences defined by recurrence relations are Benford. For more on recurrence relations, see Exercise **??**. The interested reader should see [BrDu, NS] for more on the subject.

1.3.1. *Recurrence Preliminaries.* We consider recurrence relations of length k:

$$a_{n+k} \ = \ c_1 a_{n+k-1} + \cdots + c_k a_n, \tag{12}$$

where $c_1, \dots, c_k$ are fixed real numbers. If the characteristic polynomial

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_{k-1} r - c_k \ = \ 0 \tag{13}$$

has k distinct roots $\lambda_1, \dots, \lambda_k$, there exist k numbers $u_1, \dots, u_k$ such that

$$a_n \ = \ u_1 \lambda_1^n + \cdots + u_k \lambda_k^n, \tag{14}$$

where we have ordered the roots so that $|\lambda_1| \geq \cdots \geq |\lambda_k|$.

For the Fibonacci numbers $k = 2$, $c_1 = c_2 = 1$, $u_1 = -u_2 = \frac{1}{\sqrt{5}}$, and $\lambda_1 = \frac{1+\sqrt{5}}{2}$, $\lambda_2 = \frac{1-\sqrt{5}}{2}$ (see Exercise **??**). If $|\lambda_1| = 1$, we do not expect the first digit of a_n to be Benford (base b). For example, if we consider

$$a_n \ = \ 2a_{n-1} - a_{n-2} \tag{15}$$

with initial values $a_0 = a_1 = 1$, every $a_n = 1$! If we instead take $a_0 = 0$, $a_1 = 1$, we get $a_n = n$. See [Kos] for many interesting occurrences of Fibonacci numbers and recurrence relations.

1.3.2. *Recurrence Relations Are Benford.*

Theorem 1.10. *Let a_n satisfy a recurrence relation of length k with k distinct real roots. Assume $|\lambda_1| \neq 1$ with $|\lambda_1|$ the largest absolute value of the roots. Further, assume the initial conditions are such that the coefficient of λ_1 is non-zero. If $\log_b |\lambda_1| \notin \mathbb{Q}$, then a_n is Benford (base b).*

Proof. By assumption, $u_1 \neq 0$. For simplicity we assume $\lambda_1 > 0$, $\lambda_1 > |\lambda_2|$ and $u_1 > 0$. Again let $y_n = \log_b x_n$. By Theorem 1.6 it suffices to show y_n is equidistributed mod 1. We have

$$\begin{aligned} x_n &= u_1 \lambda_1^n + \cdots + u_n \lambda_k^n \\ x_n &= u_1 \lambda_1^n \left[1 + O\left(\frac{ku\lambda_2^n}{\lambda_1^n} \right) \right], \end{aligned} \tag{16}$$

where $u = \max_i |u_i| + 1$ (so $ku > 1$ and the big-Oh constant is 1). As $\lambda_1 > |\lambda_2|$, we "borrow" some of the growth from λ_1^n; this is a very useful technique. Choose a small ϵ and an n_0 such that

(1) $|\lambda_2| < \lambda_1^{1-\epsilon}$;
(2) for all $n > n_0$, $\frac{(ku)^{1/n}}{\lambda_1^\epsilon} < 1$, which then implies $\frac{ku}{\lambda_1^{n\epsilon}} = \left(\frac{(ku)^{1/n}}{\lambda_1^\epsilon}\right)^n$.

As $ku > 1$, $(ku)^{1/n}$ is decreasing to 1 as n tends to infinity. Note $\epsilon > 0$ if $\lambda_1 > 1$ and $\epsilon < 0$ if $\lambda_1 < 1$. Letting

$$\beta \;=\; \frac{(ku)^{1/n_0}}{\lambda_1^\epsilon}\frac{|\lambda_2|}{\lambda_1^{1-\epsilon}} \;<\; 1, \tag{17}$$

we find that the error term above is bounded by β^n for $n > n_0$, which tends to 0. Therefore

$$\begin{aligned} y_n &= \log_b x_n \\ &= \log_b(u_1\lambda_1^n) + O\left(\log_b(1+\beta^n)\right) \\ &= n\log_b\lambda_1 + \log_b u_1 + O(\beta^n), \end{aligned} \tag{18}$$

where the big-Oh constant is bounded by C say. As $\log_b \lambda_1 \notin \mathbb{Q}$, the fractional parts of $n\log_b\lambda_1$ are equidistributed modulo 1, and hence so are the shifts obtained by adding the fixed constant $\log_b u_1$.

We need only show that the error term $O(\beta^n)$ is negligible. It is possible for the error term to change the first digit; for example, if we had 999999 (or 1000000), then if the error term contributes 2 (or -2), we would change the first digit base 10. However, for n sufficiently large, the error term will change a vanishingly small number of first digits. Say $n\log_b\lambda_1 + \log_b u_1$ exponentiates base b to first digit j, $j \in \{1,\dots,b-1\}$. This means

$$n\log_b\lambda_1 + \log_b u_1 \;\in\; I_j^{(b)} \;=\; [p_{j-1}, p_j). \tag{19}$$

The error term is at most $C\beta^n$ and y_n exponentiates to a different first digit than $n\log_b\lambda_1 + \log_b u_1$ only if one of the following holds:

(1) $n\log_b\lambda_1 + \log_b u_1$ is within $C\beta^n$ of p_j, and adding the error term pushes us to or past p_j;
(2) $n\log_b\lambda_1 + \log_b u_1$ is within $C\beta^n$ of p_{j-1}, and adding the error term pushes us before p_{j-1}.

The first set is contained in $[p_j - C\beta^n, p_j)$, of length $C\beta^n$. The second is contained in $[p_{j-1}, p_{j-1} + C\beta^n)$, also of length $C\beta^n$. Thus the length of the interval where $n\log_b\lambda_1 + \log_b u_1$ and y_n could exponentiate base b to different first digits is of size $2C\beta^n$. If we choose N sufficiently large then for all $n > N$ we can make these lengths arbitrarily small. As $n\log_b\lambda_1 + \log_b u_1$ is equidistributed modulo 1, we can control the size of the subsets of $[0,1)$ where $n\log_b\lambda_1 + \log_b u_1$ and y_n disagree. The Benford behavior (base b) of x_n now follows in the limit. □

Exercise 1.11. *Weaken the conditions of Theorem 1.10 as much as possible. What if several roots equal λ_1? What does a general solution to* (12) *look like now? What if λ_1 is negative? Can anything be said if there are complex roots?*

Exercise(hr) 1.12. *Consider the recurrence relation $a_{n+1} = 5a_n - 8a_{n-1} + 4a_{n-2}$. Show there is a choice of initial conditions such that the coefficient of λ_1 (a largest root of the characteristic polynomial) is non-zero but the sequence does not satisfy Benford's Law.*

Exercise(hr) 1.13. *Assume all the roots of the characteristic polynomial are distinct, and let λ_1 be the largest root in absolute value. Show for almost all initial conditions that the coefficient of λ_1 is non-zero, which implies that our assumption that $u_1 \neq 0$ is true most of the time.*

1.4. **Random Walks and Benford's Law.** Consider the following (colorful) problem: A drunk starts off at time zero at a lamppost. Each minute he stumbles with probability p one unit to the right and with probability $q = 1-p$ one unit to the left. Where do we expect the drunk to be after N tosses? This is known as a **Random Walk**. By the Central Limit Theorem (Theorem **??**), his distribution after N tosses is well approximated by a Gaussian with mean $1\cdot pN + (-1)\cdot(1-p)N = (2p-1)N$ and variance $p(1-p)N$. For more details on Random Walks, see [Re].

For us, a **Geometric Brownian Motion** is a process such that its logarithm is a Random Walk (see [Hu] for complete statements and applications). We show below that the first digits of Geometric

Brownian Motions are Benford. In [KonSi] the $3x + 1$ problem is shown to be an example of Geometric Brownian Motion. For heuristic purposes we use the first definition of the $3x + 1$ map, though the proof is for the alternate definition. We have two operators: T_3 and T_2, with $T_3(x) = 3x + 1$ and $T_2(x) = \frac{x}{2}$. If a_n is odd, $3a_n + 1$ is even, so T_3 must always be followed by T_2. Thus, we have really have two operators T_2 and $T_{3/2}$, with $T_{3/2}(x) = \frac{3x+1}{2}$. If we assume each operator is equally likely, half the time we go from $x \to \frac{3}{2}x + 1$, and half the time to $\frac{1}{2}x$.

If we take logarithms, $\log x$ goes to $\log \frac{3}{2}x = \log x + \log \frac{3}{2}$ half the time and $\log \frac{1}{2}x = \log x + \log \frac{1}{2}$ the other half. Hence on average we send $\log x \to \log x + \frac{1}{2} \log \frac{3}{4}$. As $\log \frac{3}{4} < 0$, on average our sequence is decreasing (which agrees with the conjecture that eventually we reach $4 \to 2 \to 1$). Thus we might expect our sequence to look like $\log x_k = \log x + \frac{k}{2} \log \frac{3}{4}$. As $\log \frac{3}{4} \notin \mathbb{Q}$, its multiples are equidistributed modulo 1, and thus when we exponentiate we expect to see Benford behavior. Note, of course, that this is simply a heuristic, suggesting we might see Benford's Law. A better heuristic is sketched in Exercise 1.14.

While we can consider Random Walks or Brownian Motion with non-zero means, for simplicity below we assume the means are zero. Thus, in the example above, $p = \frac{1}{2}$.

Exercise$^{\text{(hr)}}$ 1.14. *Give a better heuristic for the Geometric Brownian Motion of the* $3x + 1$ *map by considering the alternate definition:* $a_{n+1} = \frac{3a_n+1}{2^k}$, *where* $2^k || 3x + 1$. *In particular, calculate the expected value of* $\log a_{n+1}$. *To do so, we need to estimate the probability* $k = \ell$ *for each* $\ell \in \{1, 2, 3, \dots\}$*; note* $k \neq 0$ *as for* x *odd,* $3x + 1$ *is always even and thus divisible by at least one power of* 2. *Show it is reasonable to assume that* $\text{Prob}(k = \ell) = 2^{-\ell}$.

1.4.1. *Needed Gaussian Integral.* Consider a sequence of Gaussians G_σ with mean 0 and variance σ^2, with $\sigma^2 \to \infty$. The following lemma shows that for any $\delta > 0$ as $\sigma \to \infty$ almost all of the probability is in the interval $[-\sigma^{1+\delta}, \sigma^{1+\delta}]$. We will use this lemma to show that it is enough to investigate Gaussians in the range $[-\sigma^{1+\delta}, \sigma^{1+\delta}]$.

Lemma 1.15.
$$\frac{2}{\sqrt{2\pi\sigma^2}} \int_{\sigma^{1+\delta}}^{\infty} e^{-x^2/2\sigma^2} dx \ \ll\ e^{-\sigma^{2\delta}/2}. \tag{20}$$

Proof. Change the variable of integration to $w = \frac{x}{\sigma\sqrt{2}}$. Denoting the above integral by I, we find
$$I \;=\; \frac{2}{\sqrt{2\pi\sigma^2}} \int_{\sigma^\delta/\sqrt{2}}^{\infty} e^{-w^2} \cdot \sigma\sqrt{2} dw \;=\; \frac{2}{\sqrt{\pi}} \int_{\sigma^\delta/\sqrt{2}}^{\infty} e^{-w^2} dw. \tag{21}$$

The integrand is monotonically decreasing. For $w \in \left[\frac{\sigma^\delta}{\sqrt{2}}, \frac{\sigma^\delta}{\sqrt{2}} + 1\right]$, the integrand is bounded by substituting in the left endpoint, and the region of integration is of length 1. Thus,
$$\begin{aligned}
I &< 1 \cdot \frac{2}{\sqrt{\pi}} e^{-\sigma^{2\delta}/2} + \frac{2}{\sqrt{\pi}} \int_{\frac{\sigma^\delta}{\sqrt{2}}+1}^{\infty} e^{-w^2} dw \\
&= \frac{2}{\sqrt{\pi}} e^{-\sigma^{2\delta}/2} + \frac{2}{\sqrt{\pi}} \int_{\frac{\sigma^\delta}{\sqrt{2}}}^{\infty} e^{-(u+1)^2} du \\
&= \frac{2}{\sqrt{\pi}} e^{-\sigma^{2\delta}/2} + \frac{2}{\sqrt{\pi}} \int_{\frac{\sigma^\delta}{\sqrt{2}}}^{\infty} e^{-u^2} e^{-2u} e^{-1} du \\
&< \frac{2}{\sqrt{\pi}} e^{-\sigma^{2\delta}/2} + \frac{2}{e\sqrt{\pi}} e^{-\sigma^{2\delta}/2} \int_{\frac{\sigma^\delta}{\sqrt{2}}}^{\infty} e^{-2u} du \\
&< \frac{2(e+1)}{\sqrt{\pi}} e^{-\sigma^{2\delta}/2} \\
&< 4e^{-\sigma^{2\delta}/2}.
\end{aligned} \tag{22}$$

□

Exercise 1.16. *Prove a similar result for intervals of the form* $[-\sigma g(\sigma), \sigma g(\sigma)]$ *where* $g(\sigma)$ *is a positive increasing function and* $\lim_{\sigma\to\infty} g(\sigma) = +\infty$.

1.4.2. *Geometric Brownian Motions Are Benford.* We investigate the distribution of digits of processes that are Geometric Brownian Motions. By Theorem 1.6 it suffices to show that the Geometric Brownian Motion converges to being equidistributed modulo 1. Explicitly, we have the following: after N iterations, by the Central Limit Theorem the expected value converges to a Gaussian with mean 0 and variance proportional to $\sqrt{N}$. We must show that the Gaussian with growing variance is equidistributed modulo 1.

For convenience we assume the mean is 0 and the variance is $N/2\pi$. This corresponds to a fair coin where for each head (resp., tail) we move $\frac{1}{\sqrt{4\pi}}$ units to the right (resp., left). By the Central Limit Theorem the probability of being x units to the right of the origin after N tosses is asymptotic to

$$p_N(x) \;=\; \frac{e^{-\pi x^2/N}}{\sqrt{N}}. \tag{23}$$

For ease of exposition, we assume that rather than being asymptotic to a Gaussian, the distribution is a Gaussian. For our example of flipping a coin, this cannot be true. If every minute we flip a coin and record the outcome, after N minutes there are 2^N possible outcomes, a finite number. To each of these we attach a number equal to the excess of heads to tails. There are technical difficulties in working with discrete probability distributions; thus we study instead continuous processes such that at time N the probability of observing x is given by a Gaussian with mean 0 and variance $N/2\pi$. For complete details see [KonMi].

Theorem 1.17. *As* $N \to \infty$, $p_N(x) = \frac{e^{-\pi x^2/N}}{\sqrt{N}}$ *becomes equidistributed modulo* 1.

Proof. For each N we calculate the probability that for $x \in \mathbb{R}$, $x \bmod 1 \in [a,b] \subset [0,1)$. This is

$$\int_{\substack{x=-\infty \\ x \bmod 1 \in [a,b]}}^{\infty} p_N(x)dx \;=\; \frac{1}{\sqrt{N}} \sum_{n\in\mathbb{Z}} \int_{x=a}^{b} e^{-\pi(x+n)^2/N} dx. \tag{24}$$

We need to show the above converges to $b-a$ as $N \to \infty$. For $x \in [a,b]$, standard calculus (Taylor series expansions, see §**??**) gives

$$e^{-\pi(x+n)^2/N} \;=\; e^{-\pi n^2/N} + O\left(\frac{\max(1,|n|)}{N}\, e^{-n^2/N}\right). \tag{25}$$

We claim that in (24) it is sufficient to restrict the summation to $|n| \le N^{5/4}$. The proof is immediate from Lemma 1.15: we increase the integration by expanding to $x \in [0,1]$, and then trivially estimate. Thus, up to negligible terms, all the contribution is from $|n| \le N^{5/4}$.

In §**??** we prove the Poisson Summation formula, which in this case yields

$$\frac{1}{\sqrt{N}} \sum_{n\in\mathbb{Z}} e^{-\pi n^2/N} \;=\; \sum_{n\in\mathbb{Z}} e^{-\pi n^2 N}. \tag{26}$$

The beauty of Poisson Summation is that it converts one infinite sum with *slow* decay to another sum with *rapid* decay; because of this, Poisson Summation is an extremely useful technique for a variety of problems. The exponential terms on the left of (26) are all of size 1 for $n \le \sqrt{N}$, and do not become small until $n \gg \sqrt{N}$ (for instance, once $n > \sqrt{N}\log N$, the exponential terms are small for large N); however, almost all of the contribution on the right comes from $n = 0$. The power of Poisson Summation is it often allows us to approximate well long sums with short sums.

We therefore have

$$\begin{aligned}
&\frac{1}{\sqrt{N}} \sum_{|n|\le N^{5/4}} \int_{x=a}^{b} e^{-\pi(x+n)^2/N} dx \\
&= \frac{1}{\sqrt{N}} \sum_{|n|\le N^{5/4}} \int_{x=a}^{b} \left[e^{-\pi n^2/N} + O\left(\frac{\max(1,|n|)}{N} e^{-n^2/N}\right)\right] dx \\
&= \frac{b-a}{\sqrt{N}} \sum_{|n|\le N^{5/4}} e^{-\pi n^2/N} + O\left(\frac{1}{N}\sum_{n=0}^{N^{5/4}} \frac{n+1}{\sqrt{N}} e^{-\pi(n/\sqrt{N})^2}\right) \\
&= \frac{b-a}{\sqrt{N}} \sum_{|n|\le N^{5/4}} e^{-\pi n^2/N} + O\left(\frac{1}{N}\int_{w=0}^{N^{3/4}} (w+1)e^{-\pi w^2}\sqrt{N} dw\right) \\
&= \frac{b-a}{\sqrt{N}} \sum_{|n|\le N^{5/4}} e^{-\pi n^2/N} + O\left(N^{-1/2}\right). \qquad (27)
\end{aligned}$$

By Lemma 1.15 we can extend all sums to $n \in \mathbb{Z}$ in (27) with negligible error. We now apply Poisson Summation and find that up to lower order terms,

$$\frac{1}{\sqrt{N}} \sum_{n\in\mathbb{Z}} \int_{x=a}^{b} e^{-\pi(x+n)^2/N} dx \ \approx\ (b-a)\cdot \sum_{n\in\mathbb{Z}} e^{-\pi n^2 N}. \qquad (28)$$

For $n = 0$ the right hand side of (28) is $b - a$. For all other n, we trivially estimate the sum:

$$\sum_{n\neq 0} e^{-\pi n^2 N} \ \le\ 2\sum_{n\ge 1} e^{-\pi n N} \ \le\ \frac{2e^{-\pi N}}{1-e^{-\pi N}}, \qquad (29)$$

which is less than $4e^{-\pi N}$ for N sufficiently large. □

We can interpret the above arguments as follows: for each N, consider a Gaussian $p_N(x)$ with mean 0 and variance $N/2\pi$. As $N \to \infty$ for each x (which occurs with probability $p_N(x)$) the first digit of 10^x converges to the Benford base 10 probabilities.

Remark 1.18. The above framework is very general and applicable to a variety of problems. In [KonMi] it is shown that these arguments can be used to prove Benford behavior in discrete systems such as the $3x+1$ problem as well as continuous systems such as the absolute values of the Riemann zeta function (and any "good" L-function) near the critical line! For these number theory results, the crucial ingredients are Selberg's result (near the critical line, $\log|\zeta(s+it)|$ for $t \in [T, 2T]$ converges to a Gaussian with variance tending to infinity in T) and estimates by Hejhal on the rate of convergence. For the $3x + 1$ problem the key ingredients are the structure theorem (see [KonSi]) and the approximation exponent of Definition **??**; see [LaSo] for additional results on Benford behavior of the $3x + 1$ problem.

1.5. **Statistical Inference.** Often we have reason to believe that some process occurs with probability p of success and $q = 1 - p$ of failure. For example, consider the $3x + 1$ problem. Choose a large a_0 and look at the first digit of the a_n's. There is reason to believe the distribution of the first digits is given by Benford's Law for most a_0 as $a_0 \to \infty$. We describe how to test this and similar hypotheses. We content ourselves with describing one simple test; the interested reader should consult a statistics textbook (for example, [BD, CaBe, LF, MoMc]) for the general theory and additional applications.

1.5.1. *Null and Alternative Hypotheses.* Suppose we think some population has a parameter with a certain value. If the population is small, it is possible to investigate every element; in general this is not possible.

For example, say the parameter is how often the millionth decimal or continued fraction digit is 1 in two populations: all rational numbers in $[0,1)$ with denominator at most 5, and all real numbers in $[0,1)$. In the first, there are only 10 numbers, and it is easy to check them all. In the second, as there are infinitely many numbers, it is impossible to numerically investigate each. What we do in practice is we sample a large number of elements (say N elements) in $[0,1)$, and calculate the average value of the parameter for this sample.

We thus have two **populations**, the **underlying population** (in the second case, all numbers in $[0,1)$), and the **sample population** (in this case, the N sampled elements).

Our goal is to test whether or not the underlying population's parameter has a given value, say p. To this end, we want to compare the sample population's value to p. The **null hypothesis**, denoted H_0, is the claim that there is no difference between the sample population's value and the underlying population's value; the **alternative hypothesis**, denoted H_a, is the claim that there is a difference between the sample population's value and the underlying population's value.

When we analyze the data from the sample population, either we reject the null hypothesis, or we fail to reject the null hypothesis. It is important to note that we *never* prove the null or alternative hypothesis is true or false. We are always rejecting or failing to reject the null hypothesis, we are never accepting it. If we flip a coin 100 times and observe all heads, this does not mean the coin is not fair: it is possible the coin is fair but we had a very unusual sample (though, of course, it is extremely unlikely).

We now discuss how to test the null hypothesis. Our main tool is the Central Limit Theorem. This is just one of many possible inference tests; we refer the reader to [BD, CaBe, LF, MoMc] for more details.

1.5.2. *Bernoulli Trials and the Central Limit Theorem.* Assume we have some process where we expect a probability p of observing a given value. For example, if we choose numbers uniformly in $[0,1)$ and look at the millionth decimal digit, we believe that the probability this digit is 1 is $\frac{1}{10}$. If we look at the continued fraction expansion, by Theorem **??** the probability that the millionth digit is 1 is approximately $\log_2 \frac{4}{3}$. What if we restrict to algebraic numbers? What is the probability the millionth digit (decimal or continued fraction expansion) equals 1?

In general, once we formalize our conjecture we test it by choosing N elements from the population independently at random (see §**??**). Consider the claim that a process has probability p of success. We have N independent Bernoulli trials (see §**??**). The null hypothesis is the claim that p percent of the sample are a success. Let S_N be the number of successes; if the null hypothesis is correct, by the Central Limit Theorem (see §**??**) we expect S_N to have a Gaussian distribution with mean pN and variance pqN (see Exercise **??** for the calculations of the mean and variance of a Bernoulli process). This means that if we were to look at many samples with N elements, on average each sample would have $pN \pm O(\sqrt{pqN})$ successes. We calculate the probability of observing a difference $|S_N - pN|$ as large or larger than a. This is given by the area under the Gaussian with mean pN and variance pqN:

$$\frac{1}{\sqrt{2\pi pqN}} \int_{|s-pN|\geq a} e^{-(s-pN)^2/2pqN} ds. \tag{30}$$

If this integral is small, it is extremely unlikely that we choose N independent trials from a process with probability p of success and we reject the null hypothesis; if the integral is large, we do not reject the null hypothesis, and we have support for our claim that the underlying process does have probability p of success.

Unfortunately, the Gaussian is a difficult function to integrate, and we would need to tabulate these integrals for *every* different pair of mean and variance. It is easier, therefore, to renormalize and look at a new statistic which should also be Gaussian, but with mean 0 and variance 1. The advantage is that we need only tabulate *one* special Gaussian, the standard normal.

Let $Z = \frac{S_N - pN}{\sqrt{pqN}}$. This is known as the **z-statistic**. If S_N's distribution is a Gaussian with mean pN and variance pqN, note Z will be a Gaussian with mean 0 and variance 1.

Exercise 1.19. *Prove the above statement about the distribution of z.*

Let

$$I(a) = \frac{1}{\sqrt{2\pi}} \int_{|z| \geq a} e^{-z^2/2} dz, \tag{31}$$

the area under the standard normal (mean 0, standard deviation 1) that is at least a units from the mean. We consider different **confidence intervals**. If we were to randomly choose a number z from such a Gaussian, what is the probability (as a function of a) that z is at most a units from the mean? Approximately 68% of the time $|z| \leq 1$ ($I(1) \approx .32$), approximately 95% of the time $z \leq 1.96$ ($I(1.96) \approx .05$), and approximately 99% of the time $|z| \leq 2.57$ ($I(2.57) = .01$). In other words, there is only about a 1% probability of observing $|z| \geq 2.57$. If $|z| \geq 2.57$, we have strong evidence against the hypothesis that the process occurs with probability p, and we would be reasonably confident in rejecting the null hypothesis; of course, it is possible we were unlucky and obtained an unrepresentative set of data (but it is extremely unlikely that this occurred; in fact, the probability is at most 1%).

Remark 1.20. For a Gaussian with mean μ and standard deviation σ, the probability that $|X - \mu| \leq \sigma$ is approximately .68. Thus if X is drawn from a normal with mean μ and standard deviation σ, then approximately 68% of the time $\mu \in [x - \sigma, x + \sigma]$ (where x is the observed value of the random variable X).

To test the claim that some process occurs with probability p, we observe N independent trials, calculate the z-statistic, and see how likely it is to observe $|Z|$ that large or larger. We give two examples below.

1.5.3. *Digits of the* $3x + 1$ *Problem.* Consider again the $3x + 1$ problem. Choose a large integer a_0, and look at the iterates: $a_1, a_2, a_3, \ldots$. We study how often the first digit of terms in the sequence equal $d \in \{1, \ldots, 9\}$. We can regard the first digit of a term as a Bernoulli trial with a success (or 1) if the first digit is d and a failure (or 0) otherwise. If the distribution of digits is governed by Benford's Law, the theoretical prediction is that the fraction of the first digits that equal d is $p = \log_{10}(\frac{d+1}{d})$. Assume there are N terms in our sequence (before we hit the pattern $4 \to 2 \to 1 \to 4 \cdots$), and say M of them have first digit d. For what M does this experiment provide support that the digits follow Benford's Law?

Exercise 1.21. *The terms in the sequence generated by a_0 are not independent, as a_{n+1} is determined by a_n. Show that if the first digit of a_n is 2 then the first digit of a_{n+1} cannot be a 2.*

The above exercise shows that the first digit of the terms *cannot* be considered independent Bernoulli trials. As the sequence is completely determined by the first term, this is not surprising. If we look at an enormous number of terms, however, these effects "should" average out. Another possible experiment is to look at the first digit of the millionth term for N different a_0's.

Let $a_0 = 333 \ldots 333$ be the integer that is 10,000 threes. There are 177,857 terms in the sequence before we hit $4 \to 2 \to 1$. The following data comparing the number of first digits equal to d to the Benford predictions are from [Min]:

digit	observed	predicted	variance	z-statistic	$I(z)$
1	53425	53540	193.45	-0.596	0.45
2	31256	31310	160.64	-0.393	0.31
3	22257	22220	139.45	0.257	0.21
4	17294	17230	124.76	0.464	0.36
5	14187	14080	113.88	0.914	0.63
6	11957	11900	105.40	0.475	0.36
7	10267	10310	98.57	-0.480	0.37
8	9117	9090	92.91	0.206	0.16
9	8097	8130	88.12	-0.469	0.36

As the values of the z-statistics are all small (well below 1.96 and 2.57), the above table provides evidence that the first digits in the $3x+1$ problem follow Benford's Law, and we would not reject the null hypothesis for any of the digits. If we had obtained large z-statistics, say 4, we would reject the null hypothesis and doubt that the distribution of digits follow Benford's Law.

Remark 1.22 (Important)**.** One must be very careful when analyzing all the digits. Once we know how many digits are in $\{1, \dots, 8\}$, then the number of 9's is forced: these are not nine independent tests, and a different statistical test (a chi-square test with eight degrees of freedom) should be done. Our point here is not to write a treatise on statistical inference, but merely highlight some of the tools and concepts. See [BD, CaBe, LF, MoMc] for more details, and [Mil5] for an amusing analysis of a baseball problem involving chi-square tests.

Additionally, if we have many different experiments, then "unlikely" events should happen. For example, if we have 100 different experiments we would not be surprised to see an outcome which only has a 1% chance of occurring (see Exercise 1.23). Thus, if there are many experiments, the confidence intervals need to be adjusted. One common method is the Bonferroni adjustment method for multiple comparisons. See [BD, MoMc].

Exercise 1.23. *Assume for each trial there is a 95% chance of observing the fraction of first digits equal to 1 is in $[\log_{10} 2 - 1.96\sigma, \log_{10} 2 + 1.96\sigma]$ (for some σ). If we have 10 independent trials, what is the probability that* all *the observed percentages are in this interval? If we have 14 independent trials?*

Remark 1.24. How does one calculate with $10,000$ digit numbers? Such large numbers are greater than the standard number classes (int, long, double) of many computer programming languages. The solution is to represent numbers as arrays. To go from a_n to $3a_n + 1$, we multiply the array by 3, carrying as needed, and then add 1; we leave space-holding zeros at the start of the array. For example,

$$3 \cdot [0, \dots, 0, 0, 5, 6, 7] \ = \ [0, \dots, 0, 1, 7, 0, 1]. \tag{32}$$

We need only do simple operations on the array. For example, $3 \cdot 7 = 21$, so the first entry of the product array is 1 and we carry the 2 for the next multiplication. We must also compute $a_n/2$ if a_n is even. Note this is the same as $5a_n$ divided by 10. The advantage of this approach is that it is easy to calculate $5a_n$, and as a_n is even, the last digit of $5a_n$ is zero, hence array division by 10 is trivial.

Exercise 1.25. *Consider the first digits of the $3x+1$ problem (defined as in (3)) in base 6. Choose a large integer a_0, and look at the iterates $a_1, a_2, a_3, \dots$. As $a_0 \to \infty$, is the distribution of digits Benford base 6?*

Exercise 1.26 (Recommended)**.** *Here is another variant of the $3x+1$ problem:*

$$a_{n+1} \ = \ \begin{cases} 3a_n + 1 & \text{if } a_n \text{ is odd} \\ a_n/2^k & \text{if } a_n \text{ is even and } 2^k || a_n; \end{cases} \tag{33}$$

$2^k||a_n$ means 2^k divides a_n, but 2^{k+1} does not. Consider the distribution of first digits of this sequence for various a_0. What is the null hypothesis? Do the data support the null hypothesis, or the alternative hypothesis? Do you think these numbers also satisfy Benford's Law? What if instead we define

$$a_{n+1} \;=\; \frac{3a_n+1}{2^k}, \quad 2^k||a_n. \tag{34}$$

1.5.4. *Digits of Continued Fractions.* Let us test the hypothesis that the digits of algebraic numbers are given by the Gauss-Kuzmin Theorem (Theorem **??**). Let us look at how often the 1000^{th} digit equals 1. By the Gauss-Kuzmin Theorem this should be approximately $\log_2 \frac{4}{3}$. Let p_n be the n^{th} prime. In the continued fraction expansions of $\sqrt[3]{p_n}$ for $n \in \{100000, 199999\}$, exactly 41565 have the 1000^{th} digit equal to 1. Assuming we have a Bernoulli process with probability of success (a digit of 1) of $p = \log_2 \frac{4}{3}$, the z-statistic is .393. As the z-statistic is small (95% of the time we expect to observe $|z| \leq 1.96$), we do not reject the null hypothesis, and we have obtained evidence supporting the claim that the probability that the 1000^{th} digit is 1 is given by the Gauss-Kuzmin Theorem. See Chapter **??** for more detailed experiments on algebraic numbers and the Gauss-Kuzmin Theorem.

1.6. **Summary.** We have chosen to motivate our presentation of statistical inference by investigating the first digits of the $3x+1$ problem, but of course the methods apply to a variety of problems. Our main tool is the Central Limit Theorem: if we have a process with probability p (resp., $q = 1-p$) of success (resp., failure), then in N independent trials we expect about pN successes, with fluctuations of size $\sqrt{pqN}$. To test whether or not the underlying probability is p we formed the z-statistic: $\frac{S_N - pN}{\sqrt{pqN}}$, where S_N is the number of successes observed in the N trials.

If the process really does have probability p of success, then by the Central Limit Theorem the distribution of S_N is approximately a Gaussian with mean pN and standard deviation $\sqrt{pqN}$, and we then expect the z-statistic to be of size 1. If, however, the underlying process occurs not with probability p but p', then we expect S_N to be approximately a Gaussian with mean $p'N$ and standard deviation $\sqrt{p'q'N}$. We now expect the z-statistic to be of size $\frac{(p'-p)N}{\sqrt{p'q'N}}$. This is of size $\sqrt{N}$, much larger than 1.

We see the z-statistic is very sensitive to $p'-p$: if p' is differs from p, for large N we quickly observe large values of z. Note, of course, that statistical tests can only provide compelling evidence in favor or against a hypothesis, never a proof.

REFERENCES

Links to many of the references below are available online at
http://www.math.princeton.edu/mathlab/book/index.html

[Acz] A. Aczel, *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem*, Four Walls Eight Windows, New York, 1996.

[AKS] R. Adler, M. Keane, and M. Smorodinsky, *A construction of a normal number for the continued fraction transformation*, J. Number Theory **13** (1981), no. 1, 95–105.

[AgKaSa] M. Agrawal, N. Kayal and N. Saxena, *PRIMES is in P*, Ann. of Math. (2) **160** (2004), no. 2, 781–793.

[Al] L. Ahlfors, *Complex Analysis*, 3rd edition, McGraw-Hill, New York, 1979.

[AZ] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, Springer-Verlag, Berlin, 1998.

[AGP] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. Math. **139** (1994), 703–722.

[AMS] AMS MathSciNet, http://www.ams.org/msnmain?screen=Review

[AB] U. Andrews IV and J. Blatz, *Distribution of digits in the continued fraction representations of seventh degree algebraic irrationals*, Junior Thesis, Princeton University, Fall 2002.

[Ap] R. Apéry, *Irrationalité de $\zeta(2)$ et $\zeta(3)$*, Astérisque **61** (1979) 11–13.

[Apo] T. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1998.

[ALM] S. Arms, A. Lozano-Robledo and S. J. Miller, *Constructing One-Parameter Families of Elliptic Curves over $\mathbb{Q}(T)$ with Moderate Rank*, Journal of Number Theory **123** (2007), no. 2, 388–402.

[Art] M. Artin, *Algebra*, Prentice-Hall, Englewood Cliffs, NJ, 1991.

[Ay] R. Ayoub, *Introduction to the Analytic Theory of Numbers*, AMS, Providence, RI, 1963.

[Bai] Z. Bai, *Methodologies in spectral analysis of large-dimensional random matrices, a review*, Statist. Sinica **9** (1999), no. 3, 611–677.

[B] A. Baker, *Transcendental Number Theory*, Cambridge University Press, Cambridge, 1990.

[BM] R. Balasubramanian and C. J. Mozzochi, *Siegel zeros and the Goldbach problem*, J. Number Theory **16** (1983), no. 3, 311–332.

[BR] K. Ball and T. Rivoal, *Irrationalité d'une infinité valeurs de la fonction zeta aux entiers impairs*, Invent. Math. **146** (2001), 193–207.

[BT] V. V. Batyrev and Yu. Tschinkel, *Tamagawa numbers of polarized algebraic varieties*, Nombre et répartition de points de hauteur bornée (Paris, 1996), Astérisque (1998), No. 251, 299–340.

[BL] P. Baxandall and H. Liebeck, *Vector Calculus*, Clarendon Press, Oxford, 1986.

[Be] R. Beals, *Notes on Fourier series*, Lecture Notes, Yale University, 1994.

[Bec] M. Beceanu, *Period of the continued fraction of $\sqrt{n}$*, Junior Thesis, Princeton University, 2003.

[Ben] F. Benford, *The law of anomalous numbers*, Proceedings of the American Philosophical Society **78** (1938) 551–572.

[BBH] A. Berger, Leonid A. Bunimovich, and T. Hill, *One-dimensional dynamical systems and Benford's Law*, Trans. Amer. Math. Soc. **357** (2005), no. 1, 197–219.

[BEW] B. Berndt, R. Evans, and K. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Vol. 21, Wiley-Interscience Publications, John Wiley & Sons, New York, 1998.

[Ber] M. Bernstein, *Games, hats, and codes*, lecture at the SUMS 2005 Conference.

[BD] P. Bickel and K. Doksum, *Mathematical Statistics: Basic Ideas and Selected Topics*, Holden-Day, San Francisco, 1977.

[Bi] P. Billingsley, *Probability and Measure*, 3rd edition, Wiley, New York, 1995.

[Bl1] P. Bleher, *The energy level spacing for two harmonic oscillators with golden mean ratio of frequencies*, J. Stat. Phys. **61** (1990) 869–876.

[Bl2] P. Bleher, *The energy level spacing for two harmonic oscillators with generic ratio of frequencies*, J. Stat. Phys. **63** (1991), 261–283.

[Bob] J. Bober, *On the randomness of modular inverse mappings*, Undergraduate Mathematics Laboratory report, Courant Institute, NYU, 2002.

[Bol] B. Bollobás, *Random Graphs*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2001.

[BoLa] E. Bombieri and J. Lagarias, *Complements to Li's criterion for the Riemann Hypothesis*, J. Number Theory **77** (1999), no. 2, 274–287.

[BG] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, Cambridge, UK, 2006.

[BP] E. Bombieri and A. van der Poorten, *Continued fractions of algebraic numbers*. Pages 137–152 in *Computational Algebra and Number Theory (Sydney, 1992)*, Mathematical Applications, Vol. 325, Kluwer Academic, Dordrecht, 1995.

[Bon] D. Boneh, *Twenty years of attacks on the RSA cryptosystem*, Notices of the American Mathematical Society **46** (1999), no. 2, 203–213.

[BS] Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, New York, 1968.

[BB] J. Borwein and P. Borwein, *Pi and the AGM: A Study in Analytic Number Theory and Computational Complexity*, John Wiley and Sons, New York, 1987.

[BK] A. Boutet de Monvel and A. Khorunzhy, *Some elementary results around the Wigner semicircle law*, lecture notes.

[BoDi] W. Boyce and R. DiPrima, *Elementary differential equations and boundary value problems*, 7th edition, John Wiley & Sons, New York, 2000.

[Bre1] R. Brent, *The distribution of small gaps between successive primes*, Math. Comp. **28** (1974), 315–324.

[Bre2] R. Brent, *Irregularities in the distribution of primes and twin primes*, Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday, Math. Comp. **29** (1975), 43–56.

[BPR] R. Brent, A. van der Poorten, and H. te Riele, *A comparative study of algorithms for computing continued fractions of algebraic numbers*. Pages 35–47 in *Algorithmic number theory (Talence, 1996)*, Lecture Notes in Computer Science, Vol. 1122, Springer, Berlin, 1996.

[deBr] R. de la Bretèche, *Sur le nombre de points de hauteur bornée d'une certaine surface cubique singulière*. Pages 51–77 in *Nombre et répartition de points de hauteur bornée (Paris, 1996)*, Astérisque, (1998) no. 251, 51–77.

[BBD] R. de la Bretèche, T. D. Browning, and U. Derenthal, *On Manin's conjecture for a certain singular cubic surface*, preprint.

[BPPW] B. Brindza, A. Pintér, A. van der Poorten, and M. Waldschmidt, *On the distribution of solutions of Thue's equation*. Pages 35–46 in *Number theory in progress (Zakopane-Koscielisko, 1997)*, Vol. 1, de Gruyter, Berlin, 1999.

[BFFMPW] T. Brody, J. Flores, J. French, P. Mello, A. Pandey, and S. Wong, *Random-matrix physics: spectrum and strength fluctuations*, Rev. Mod. Phys. **53** (1981), no. 3, 385–479.

[BrDu] J. Brown and R. Duncan, *Modulo one uniform distribution of the sequence of logarithms of certain recursive sequences*, Fibonacci Quarterly **8** (1970) 482–486.

[Bro] T. Browning, *The density of rational points on a certain singular cubic surface*, preprint.

[BDJ] W. Bryc, A. Dembo, T. Jiang, *Spectral measure of large random Hankel, Markov and Toeplitz matrices*, Ann. Probab. **34** (2006), no. 1, 1–38.

[Bry] A. Bryuno, *Continued frations of some algebraic numbers*, U.S.S.R. Comput. Math. & Math. Phys. **4** (1972), 1–15.

[Bur] E. Burger, *Exploring the Number Jungle: A Journey into Diophantine Analysis*, AMS, Providence, RI, 2000.

[BuP] E. Burger and A. van der Poorten, *On periods of elements from real quadratic number fields*. Pages 35–43 in *Constructive, Experimental, and Nonlinear Analysis (Limoges, 1999)*, CMS Conf. Proc., **27**, AMS, Providence, RI, 2000.

[CaBe] G. Casella and R. Berger, *Statistical Inference*, 2nd edition, Duxbury Advanced Series, Pacific Grove, CA, 2002.

[CGI] G. Casati, I. Guarneri, and F. M. Izrailev, *Statistical properties of the quasi-energy spectrum of a simple integrable system*, Phys. Lett. A **124** (1987), 263–266.

[Car] L. Carleson, *On the convergence and growth of partial sums of Fourier series*, Acta Math. **116** (1966), 135–157.

[Ca] J. W. S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge University Press, London 1957.

[Ch] D. Champernowne, *The construction of decimals normal in the scale of ten*, J. London Math. Soc. 8 (1933), 254–260.

[Cha] K. Chang, *An experimental approach to understanding Ramanujan graphs*, Junior Thesis, Princeton University, Spring 2001.

[ChWa] J. R. Chen and T. Z. Wang, *On the Goldbach problem*, Acta Math. Sinica **32** (1989), 702–718.

[Chr] J. Christiansen, *An introduction to the moment problem*, lecture notes.

[Ci] J. Cisneros, *Waring's problem*, Junior Thesis, Princeton University, Spring 2001.

[CW] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnterton-Dyer*, Invent. Math. **39** (1977), 43–67.

[CB] S. Chatterjee and A. Bose, *A new method for bounding rates of convergence of empirical spectral distributions*, J. Theoret. Probab. **17** (2004), no. 4, 1003–1019.

[Cof1] M. Coffey, *Toward verification of the Riemann hypothesis: Application of the Li criterion*, to appear in Math. Physics, Analysis and Geometry. http://arxiv.org/pdf/math-ph/0505052.

[Cof2] M. Coffey, *On the coefficients of the Baez-Duarte criterion for the Riemann hypothesis and their extensions*, preprint. http://arxiv.org/pdf/math-ph/0608050.

[CL1] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*. Pages 33–62 in *Number Theory*, Lecture Notes in Mathematics, Vol. 1068, Springer-Verlag, Berlin, 33–62.

[CL2] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups*, in *Number Theory*, Lecture Notes in Mathematics, Vol. 1052, Springer-Verlag, Berlin, 26–36.

[Coh] P. Cohen, *The independence of the continuum hypothesis*, Proc. Nat. Acad. Sci. U.S.A, **50** (1963), 1143–1148; **51** (1964), 105–110.

[Cohn] J. Cohn, *The length of the period of simple continued fractions*, Pacific Journal of Mathematics, **71** (1977), no. 1, 21–32.

[Con1] J. B. Conrey, *L-Functions and random matrices*. Pages 331–352 in *Mathematics unlimited — 2001 and Beyond*, Springer-Verlag, Berlin, 2001.

[Con2] J. B. Conrey, *The Riemann hypothesis*, Notices of the AMS, **50** (2003), no. 3, 341–353.

[CFKRS] B. Conrey, D. Farmer, P. Keating, M. Rubinstein and N. Snaith, *Integral moments of L-functions*, Proc. London Math. Soc. (3) **91** (2005), no. 1, 33–104.

[Conw] J. H. Conway, *The weird and wonderful chemistry of audioactive decay*. Pages 173–178 in *Open Problems in Communications and Computation*, ed. T. M. Cover and B. Gopinath, Springer-Verlag, New York, 1987.

[CG] J. H. Conway and R. Guy, *The Book of Numbers*, Springer-Verlag, Berlin, 1996.

[CS] J. H. Conway and N. J. A. Sloane, *Lexicographic Codes: Error-Correcting Codes from Game Theory*, IEEE Trans. Inform. Theory, **32** (1986), no. 3, 219–235.

[Corl] R. M. Corless,*Continued fractions and chaos*. Amer. Math. Monthly **99** (1992), no. 3, 203–215.

[Cor1] Cornell University, *arXiv*, http://arxiv.org

[Cor2] Cornell University, *Project Euclid*, http://projecteuclid.org/

[CFS] I. P. Cornfeld, S. V. Fomin, and I. G. Sinai, *Ergodic Theory*, Grundlehren Der Mathematischen Wissenschaften, Springer-Verlag, Berlin, 1982.

[Da1] H. Davenport, *The Higher Arithmetic: An Introduction to the Theory of Numbers*, 7th edition, Cambridge University Press, Cambridge, 1999.

[Da2] H. Davenport, *Multiplicative Number Theory*, 2nd edition, revised by H. Montgomery, Graduate Texts in Mathematics, Vol. 74, Springer-Verlag, New York, 1980.

[Da3] H. Davenport, *On the distribution of quadratic residues (mod p)*, London Math. Soc. **6** (1931), 49–54.

[Da4] H. Davenport, *On character sums in finite fields*, Acta Math. **71** (1939), 99–121.

[DN] H. A. David and H. N. Nagaraja, *Order Statistics*, 3rd edition, Wiley Interscience, Hoboken, NJ, 2003.

[DSV] G. Davidoff, P. Sarnak, and A. Valette, *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, London Mathematical Society, Student Texts, Vol. 55, Cambridge University Press, Cambridge 2003.

[Dev] R. Devaney, *An Introduction to Chaotic Dynamical Systems*, 2nd edition, Westview Press, Cambridge, MA, 2003.

[Dia] P. Diaconis, *Patterns in eigenvalues: the* 70^{th} *Josiah Williard Gibbs lecture*, Bulletin of the American Mathematical Society **40** (2003), no. 2, 155–178.

[Di] T. Dimofte, *Rational shifts of linearly periodic continued fractions*, Junior Thesis, Princeton University, 2003.

[DM] E. Dueñez and S. J. Miller, *The Low Lying Zeros of a* $\mathrm{GL}(4)$ *and a* $\mathrm{GL}(6)$ *family of L-functions*, to appear in Compositio Mathematica.

[Du] R. Durrett, *Probability: Theory and Examples*, 2nd edition, Duxbury Press, 1996.

[Dy1] F. Dyson, *Statistical theory of the energy levels of complex systems: I, II, III*, J. Mathematical Phys. **3** (1962) 140–156, 157–165, 166–175.

[Dy2] F. Dyson, *The threefold way. Algebraic structure of symmetry groups and ensembles in quantum mechanics*, J. Mathematical Phys., **3** (1962) 1199–1215.

[Edg] G. Edgar, *Measure, Topology, and Fractal Geometry*, 2nd edition, Springer-Verlag, 1990.

[Ed] H. M. Edwards, *Riemann's Zeta Function*, Academic Press, New York, 1974.

[EST] B. Elias, L. Silberman and R. Takloo-Bighash, *On Cayley's theorem*, preprint.

[EE] W. J. Ellison and F. Ellison, *Prime Numbers*, John Wiley & Sons, New York, 1985.

[Est1] T. Estermann, *On Goldbach's problem: Proof that almost all even positive integers are sums of two primes*, Proc. London Math. Soc. Ser. 2 **44** (1938) 307–314.

[Est2] T. Estermann, *Introduction to Modern Prime Number Theory*, Cambridge University Press, Cambridge, 1961.

[Fal] K. Falconer, *Fractal Geometry: Mathematical Foundations and Applications*, 2nd edition, John Wiley & Sons, New York, 2003.

[Fef] C. Fefferman, *Pointwise convergence of Fourier series*, Ann. of Math. Ser. 2 **98** (1973), 551–571.

[Fe] W. Feller, *An Introduction to Probability Theory and Its Applications*, 2nd edition, Vol. II, John Wiley & Sons, New York, 1971.

[Fi] D. Fishman, *Closed form continued fraction expansions of special quadratic irrationals*, Junior Thesis, Princeton University, 2003.

[Fol] G. Folland, *Real Analysis: Modern Techniques and Their Applications*, 2nd edition, Pure and Applied Mathematics, Wiley-Interscience, New York, 1999.

[For] P. Forrester, *Log-gases and random matrices*, book in progress.

[Fou] E. Fouvry, *Sur la hauteur des points d'une certaine surface cubique singulière*. In *Nombre et répartition de points de hauteur bornée (Paris, 1996)*, Astérisque, (1999) no. 251, 31–49.

[FSV] P. J. Forrester, N. C. Snaith, and J. J. M. Verbaarschot, *Developments in Random Matrix Theory*. In *Random matrix theory*, J. Phys. A **36** (2003), no. 12, R1–R10.

[Fr] J. Franklin, *Mathematical Methods of Economics: Linear and Nonlinear Programming, Fixed-Point Theorem*, Springer-Verlag, New York, 1980.

[GP1] H. G. Gadiyar and R. Padma, *Ramanujan-Fourier series and the density of Sophie Germain primes*, 2005. `http://arxiv.org/abs/math/0508639`

[GP2] H. G. Gadiyar and R. Padma, *Linking the Circle and the Sieve: Ramanujan - Fourier Series*, 2006. `http://arxiv.org/abs/math/0601574`

[Ga] P. Garrett, *Making, Breaking Codes: An Introduction to Cryptography*, Prentice-Hall, Englewood Cliffs, NJ, 2000.

[Gau] M. Gaudin, *Sur la loi limite de l'espacement des valeurs propres d'une matrice aléatoire*, Nucl. Phys. **25** (1961) 447–458.

[Gel] A. O. Gelfond, *Transcendental and Algebraic Numbers*, Dover, New York, 1960.

[Gl] A. Gliga, *On continued fractions of the square root of prime numbers*, Junior Thesis, Princeton University, 2003.

[Gö] K. Gödel, *On Formally Undecidable Propositions of Principia Mathematica and Related Systems*, Dover, New York, 1992.

[Gol1] D. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. 3, **4** (1976), 624–663.

[Gol2] D. Goldfeld, *The Elementary proof of the Prime Number Theorem, An Historical Perspective*. Pages 179–192 in *Number Theory, New York Seminar 2003*, eds. D. and G. Chudnovsky, M. Nathanson, Springer-Verlag, New York, 2004.

[Gold] L. Goldmakher, *On the limiting distribution of eigenvalues of large random regular graphs with weighted edges*, American Institute of Mathematics Summer REU, 2003.

[GV] D. A. Goldston and R. C. Vaughan, *On the Montgomery-Hooley asymptotic formula*. Pages 117–142 in *Sieve Methods, Exponential Sums and their Applications in Number Theory*, ed. G. R. H. Greaves, G. Harman, and M. N. Huxley, Cambridge University Press, Cambridge, 1996.

[GG] M. Golubitsky and V. Guillemin, *Stable Mappings and Their Singularities*, Graduate Texts in Mathematics, Vol. 14, Springer-Verlag, New York, 1973.

[Gou] X. Gourdon, *The* 10^{13} *first zeros of the Riemann zeta function, and zeros computation at very large height,* preprint. http://numbers.computation.free.fr/Constants/Miscellaneous/zetazeros1e13-1e24.pdf

[GKP] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, Addison-Wesley, Reading, MA, 1988.

[GK] A. Granville and P. Kurlberg, *Poisson statistics via the Chinese remainder theorem*, preprint.

[GT] A. Granville and T. Tucker, *It's as easy as abc*, Notices of the AMS **49** (2002), no. 10, 224–1231.

[GZ] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[Guy] R. Guy, *Unsolved Problems in Number Theory (Problem Books in Mathematics)*, 2nd edition, Springer-Verlag, New York, 1994.

[HM] C. Hammond and S. J. Miller, *Eigenvalue spacing distribution for the ensemble of real symmetric Toeplitz matrices*, Journal of Theoretical Probability **18** (2005), no. 3, 537–566.

[HL1] G. H. Hardy and J. E. Littlewood, *A new solution of Waring's problem*, Q. J. Math. **48** (1919), 272–293.

[HL2] G. H. Hardy and J. E. Littlewood, *Some problems of "Partitio Numerorum." A new solution of Waring's problem*, Göttingen Nach. (1920), 33–54.

[HL3] 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.

[HL4] G. H. Hardy and J. E. Littlewood, *Some problems of "Partitio Numerorum." IV. Further researches in Waring's problem*, Math. Z. **23** (1925) 1–37.

[HR] G. H. Hardy and S. Ramanujan, *Asymptotic formulae in combinatorial analysis*, Proc. London Math. Soc. **17** (1918), 75–115.

[HW] G. H. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Oxford Science Publications, Clarendon Press, Oxford, 1995.

[Hata] R. Hata, *Improvement in the irrationality measures of* π *and* π^2, Proc. Japan. Acad. Ser. A Math. Sci. **68** (1992), 283–286.

[Ha1] B. Hayes, *Third Base: Three cheers for base 3!*, American Scientist **89** (2001), no. 6, 490–494.

[Ha2] B. Hayes, *The spectrum of Riemannium*, American Scientist **91** (2003), no. 4, 296–300.

[He] R. Heath-Brown, *The density of rational points on Cayley's cubic surface*, preprint.

[Hei] H. Heillbronn, *On the average length of a class of finite continued fractions*. In *Number Theory and Analysis (A collection of papers in honor of E. Landau)*, VEB Deutscher Verlag, Berlin, 1968.

[Hej] D. Hejhal, *On the triple correlation of zeros of the zeta function*, Internat. Math. Res. Notices (1994), no. 7, 294–302.

[Hil] D. Hilbert, *Beweis für die Darstellbarkeit der ganzen zahlen durch eine feste Anzahl* n^{ter} *Potenzen (Waringsches Problem)*, Mat. Annalen **67** (1909), 281–300.

[Hi1] T. Hill, *The first-digit phenomenon*, American Scientist **86** (1996), 358–363.

[Hi2] T. Hill, *A statistical derivation of the significant-digit law*, Statistical Science **10** (1996), 354–363.

[HS] M. Hindry and J. Silverman, *Diophantine Geometry: An Introduction*, Graduate Texts in Mathematics, Vol. 201, Springer-Verlag, New York, 2000.

[HSP] J. Hoffstein, J. H. Silverman and J. Pipher, *An Introduction to Mathematical Cryptography*.

[HJ] K. Hrbacek and T. Jech, *Introduction to Set Theory*, Pure and Applied Mathematics, Marcel Dekker, New York, 1984.

[Hua] Hua Loo Keng, *Introduction to Number Theory*, Springer-Verlag, New York, 1982.

[HuRu] C. Hughes and Z. Rudnick, *Mock Gaussian behaviour for linear statistics of classical compact groups*, J. Phys. A **36** (2003) 2919–2932.

[Hu] J. Hull, *Options, Futures, and Other Derivatives*, 5th edition, Prentice-Hall, Englewood Cliffs, NJ, 2002.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, Vol. 84, Springer-Verlag, New York, 1990.

[Iw] H. Iwaniec, *Topics in Classical Automorphic Forms*, Graduate Studies in Mathematics, Vol. 17, AMS, Providence, RI, 1997.

[IK] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, AMS Colloquium Publications, Vol. 53, AMS, Providence, RI, 2004.

[ILS] H. Iwaniec, W. Luo, and P. Sarnak, *Low lying zeros of families of L-functions*, Inst. Hautes Études Sci. Publ. Math. **91** (2000), 55–131.

[IS1] H. Iwaniec and P. Sarnak, *Dirichlet L-functions at the central point*. Pages 941–952 in *Number Theory in Progress, (Zakopane-Kościelisko, 1997)*, Vol. 2, de Gruyter, Berlin, 1999.

[IS2] H. Iwaniec and P. Sarnak, *The non-vanishing of central values of automorphic L-functions and Landau-Siegel zeros*, Israel J. Math. **120** (2000), 155–177.

[JMRR] D. Jakobson, S. D. Miller, I. Rivin, and Z. Rudnick, *Eigenvalue spacings for regular graphs*. Pages 317–327 in *Emerging Applications of Number Theory (Minneapolis, 1996)*, The IMA Volumes in Mathematics and its Applications, Vol. 109, Springer, New York, 1999.

[J] N. Jacobson, *Basic Algebra I*, 2nd edition, W H Freeman & Co, San Francisco, 1985.

[Je] R. Jeffrey, *Formal Logic: Its Scope and Limits*, McGraw-Hill, New York, 1989.

[Ka] S. Kapnick, *Continued fraction of cubed roots of primes*, Junior Thesis, Princeton University, Fall 2002.

[Kar] A. Karlsson, *Applications of heat kernels on Abelian groups: $\zeta(2n)$, quadratic reciprocity, Bessel integral*, preprint.

[KS1] N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, AMS Colloquium Publications, Vol. 45, AMS, Providence, RI, 1999.

[KS2] N. Katz and P. Sarnak, *Zeros of zeta functions and symmetries*, Bull. AMS **36** (1999), 1–26.

[KeSn] J. P. Keating and N. C. Snaith, *Random matrices and L-functions*. In *Random Matrix Theory*, J. Phys. A **36** (2003), no. 12, 2859–2881.

[Kei] J. B. Keiper, *Power series expansions of Riemann's ξ function*, Math. Comp. **58**(1992), 765-773.

[Kel] D. Kelley, *Introduction to Probability*, Macmillan Publishing Company, London, 1994.

[Kh] A. Y. Khinchin, *Continued Fractions*, 3rd edition, University of Chicago Press, Chicago, 1964.

[KSS] D. Kleinbock, N. Shah, and A. Starkov,*Dynamics of subgroup actions on homogeneous spaces of Lie groups and applications to number theory*. Pages 813–930 in *Handbook of Dynamical Systems*, Vol. 1A, North-Holland, Amsterdam, 2002.

[Kn] A. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, NJ, 1992.

[Knu] D. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd edition, Addison-Wesley, MA, 1997.

[Kob1] N. Koblitz, *Why study equations over finite fields?*, Math. Mag. **55** (1982), no. 3, 144–149.

[Kob2] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), no. 177, 203–209.

[Kob3] N. Koblitz, *A survey of number theory and cryptography*. Pages 217-239 in *Number Theory*, Trends in Mathematics, Birkhäuser, Basel, 2000.

[Ko] V. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*. Pages 429-436 in *Proceedings of the International Congress of Mathematicians (Kyoto, 1990)*, vols. I and II, Math. Soc. Japan, Tokyo, 1991.

[KonMi] A. Kontorovich and S. J. Miller, *Benford's law, values of L-functions and the $3x + 1$ problem*, Acta Arith. **120** (2005), 269–297.

[KonSi] A. Kontorovich and Ya. G. Sinai, *Structure theorem for (d, g, h)-maps*, Bull. Braz. Math. Soc. (N.S.) 33 (2002), no. 2, 213–224.

[Kor] A. Korselt, *Probléme chinois*, L'intermédiaire math. **6** (1899), 143–143.

[Kos] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, Wiley-Interscience, New York, 2001

[Kua] F. Kuan, *Digit distribution in the continued fraction of $\zeta(n)$*, Junior Thesis, Princeton University, Fall 2002.

[KN] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, John Wiley & Sons, New York, 1974.

[KR] P. Kurlberg and Z. Rudnick, *The distribution of spacings between quadratic residues*, Duke Math. J. **100** (1999), no. 2, 211–242.

[Ku] R. Kuzmin, *Ob odnoi zadache Gaussa*, Doklady Akad. Nauk, Ser. A (1928), 375–380.

[Lag1] J. Lagarias, *The $3x + 1$ problem and its generalizations*. Pages 305-334 in *Organic mathematics (Burnaby, BC, 1995)*, CMS Conf. Proc., vol. 20, AMS, Providence, RI, 1997.

[Lag2] J. Lagarias, *The 3x+1 problem: An annotated bibliography*, preprint.

[LaSo] J. Lagarias and K. Soundararajan, *Benford's Law for the $3x + 1$ function*, J. London Math. Soc. (2) **74** (2006), no. 2, 289–303.

[La1] S. Lang, *Diophantine Geometry*, Interscience Publishers, New York, 1962.

[La2] S. Lang, *Introduction to Diophantine Approximations*, Addison-Wesley, Reading, MA, 1966.

[La3] S. Lang, *Undergraduate Algebra*, 2nd edition, Springer-Verlag, New York, 1986.

[La4] S. Lang, *Calculus of Several Variables*, Springer-Verlag, New York, 1987.

[La5] S. Lang, *Undergraduate Analysis*, 2nd edition, Springer-Verlag, New York, 1997.

[La6] S. Lang, *Complex Analysis*, Graduate Texts in Mathematics, Vol. 103, Springer-Verlag, New York, 1999.

[LT] S. Lang and H. Trotter, *Continued fractions for some algebraic numbers*, J. Reine Angew. Math. **255** (1972), 112–134.

[LF] R. Larson and B. Farber, *Elementary Statistics: Picturing the World*, Prentice-Hall, Englewood Cliffs, NJ, 2003.

[LP] R. Laubenbacher and D. Pengelley, *Gauss, Eisenstein, and the "third" proof of the quadratic reciprocity theorem: Ein kleines Schauspiel*, Math. Intelligencer 16 (1994), no. 2, 67–72.

[Law1] J. Law, *Kuzmin's theorem on algebraic numbers*, Junior Thesis, Princeton University, Fall 2002.

[Law2] J. Law, *The circle method on the binary Goldbach conjecture*, Junior Thesis, Princeton University, Spring 2003.

[Leh] R. Lehman, *First order spacings of random matrix eigenvalues*, Junior Thesis, Princeton University, Spring 2000.

[LS] H. Lenstra and G. Seroussi, *On hats and other covers*, 2002, preprint.

[Le] P. Lévy, *Sur les lois de probabilité dont dependent les quotients complets et incomplets d'une fraction continue*, Bull. Soc. Math. **57** (1929), 178–194.

[XLi] X.-J. Li, *The positivity of a sequence of numbers and Riemann hypothesis*, J. Number Theory **65** (1997), 325-333.

[LU] C. Liaw and H. Úlfarsson, *Transcendence of e and π*, class notes for Math 252 (Graduate Algebra), Brown University, Spring 2006.

[Lidl] R. Lidl, *Mathematical aspects of cryptanalysis*. Pages 86–97 in *Number Theory and Cryptography (Sydney, 1989)*, London Mathematical Society Lecture Note Series, vol. 154, Cambridge University Press, Cambridge, 1990.

[Li] R. Lipshitz, *Numerical results concerning the distribution of $\{n^2\alpha\}$*, Junior Thesis, Princeton University, Spring 2000.

[Liu] Y. Liu, *Statistical behavior of the eigenvalues of random matrices*, Junior Thesis, Princeton University, Spring 2000.

[Mah] K. Mahler, *Arithmetische Eigenschaften einer Klasse von Dezimalbrüchen*, Amsterdam Proc. Konin. Neder. Akad. Wet. **40** (1937), 421–428.

[Ma] E. S. Mahmoodian, *Mathematical Olympiads in Iran*, Vol. I, Sharif University Press, Tehran, Iran, 2002.

[Man] B. Mandelbrot, *The Fractal Geometry of Nature*, W. H. Freeman, New York, 1982.

[Mar] J. Marklof, *Almost modular functions and the distribution of n^2x modulo one*, Int. Math. Res. Not. (2003), no. 39, 2131–2151.

[MaMc] R. Martin and W. McMillen, *An elliptic curve over $\mathbb{Q}$ with rank at least* 24, Number Theory Listserver, May 2000.

[MMS] A. Massey, S. J. Miller, and J. Sinsheimer, *Eigenvalue spacing distribution for the ensemble of real symmetric palindromic Toeplitz matrices*, Journal of Theoretical Probability 20 (2007), no. 3, 637–662.

[Maz1] B. Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math. **47** (1977), 33–186.

[Maz2] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[Maz3] B. Mazur, *Number Theory as Gadfly*, Amer. Math. Monthly, **98** (1991), 593–610.

[McK] B. McKay, *The expected eigenvalue distribution of a large regular graph*, Linear Algebra Appl. **40** (1981), 203–216.

[McW] B. McKay and N. Wormald, *The degree sequence of a random graph. I. The models*, Random Structures Algorithms **11** (1997), no. 2, 97–117.

[Meh1] M. Mehta, *On the statistical properties of level spacings in nuclear spectra*, Nucl. Phys. **18** (1960), 395–419.

[Meh2] M. Mehta, *Random Matrices*, 2nd edition, Academic Press, Boston, 1991.

[Met] N. Metropolis, *The beginning of the Monte Carlo method*, Los Alamos Science, No. 15, Special Issue (1987), 125–130.

[MU] N. Metropolis and S. Ulam, *The Monte Carlo method*, J. Amer. Statist. Assoc. **44** (1949), 335–341.

[Mic1] M. Michelini, *Independence of the digits of continued fractions*, Junior Thesis, Princeton University, Fall 2002.

[Mic2] M. Michelini, *Kuzmin's extraordinaty zero measure set*, Senior Thesis, Princeton University, Spring 2004.

[Mi1] N. Miller, *Various tendencies of non-Poissonian distributions along subsequences of certain transcendental numbers*, Junior Thesis, Princeton University, Fall 2002.

[Mi2] N. Miller, *Distribution of eigenvalue spacings for band-diagonal matrices*, Junior Thesis, Princeton University, Spring 2003.

[Mill] S. D. Miller, *A simpler way to show $\zeta(3)$ is irrational*, preprint.

[Mil1] S. J. Miller, 1- *and* 2-*level densities for families of elliptic curves: Evidence for the underlying group symmetries*, Compositio Mathematica **104** (2004), no. 4, 952–992.

[Mil2] S. J. Miller, *Density functions for families of Dirichlet characters*, preprint.

[Mil3] S. J. Miller, *The arithmetic mean and geometric inequality*, Class Notes from Math 187/487, The Ohio State University, Fall 2003.

[Mil4] S. J. Miller, *Differentiating identities*, Class Notes from Math 162: Statistics, Brown University, Spring 2005.

[Mil5] S. J. Miller, *The Pythagorean won-loss formula in baseball*, Chance Magazine **20** (2007), no. 1, 40–48 (an abridged version appeared in The Newsletter of the SABR Statistical Analysis Committee **16** (February 2006), no. 1, 17–22).

[Mil6] S. J. Miller, *Investigations of zeros near the central point of elliptic curve L-functions*, Experimental Mathematics **15** (2006), no. 3, 257–279.

[Mil7] S. J. Miller, *Die battles and order statistics*, Class Notes from Math 162: Statistics, Brown University, Spring 2006.

[Mil8] S. J. Miller, *Beyond the Pigeon-Hole Principle: Many pigeons in the same box*, Class Notes from Math 162: Statistics, Brown University, Spring 2006.

[MN] S. J. Miller and M. Nigrini, *Order Statistics and Shifted Almost Benford Behavior*, preprint.

[M] V. Miller, *Use of elliptic curves in cryptography*. Pages 417–426 in *Advances in cryptology – CRYPTO '85 (Santa Barbara, CA, 1985)*, Lecture Notes in Computer Science, Vol. 218, Springer-Verlag, Berlin, 1986.

[Milne] J. S. Milne, *Elliptic Curves*, course notes.

[Min] S. Minteer, *Analysis of Benford's law applied to the* $3x+1$ *problem*, Number Theory Working Group, The Ohio State University, 2004.

[Mon1] H. Montgomery, *Primes in arithmetic progression*, Michigan Math. J. **17** (1970), 33–39.

[Mon2] H. Montgomery, *The pair correlation of zeros of the zeta function*. Pages 181–193 in *Analytic Number Theory*, Proceedings of Symposia in Pure Mathematics, vol. 24, AMS, Providence, RI, 1973.

[MoMc] D. Moore and G. McCabe, *Introduction to the Practice of Statistics*, W. H. Freeman and Co., London, 2003.

[MS] H. Montgomery and K. Soundararajan, *Beyond pair correlation*. Pages 507–514 in *Paul Erdös and His Mathematics, I (Budapest, 1999)*, Bolyai Society Mathematical Studies, Vol. 11, János Bolyai Math. Soc., Budapest, 2002.

[MW] C. J. Moreno and S. S. Wagstaff, Jr., *Sums of Squares of Integers*, Chapman and Hall, 2006.

[Moz1] C. J. Mozzochi, *An analytic sufficiency condition for Goldbach's conjecture with minimal redundancy*, Kyungpook Math. J. **20** (1980), no. 1, 1–9.

[Moz2] C. J. Mozzochi, *The Fermat Diary*, AMS, Providence, RI, 2000.

[Moz3] C. J. Mozzochi, *The Fermat Proof*, Trafford Publishing, Victoria, 2004.

[Mu1] R. Murty, *Primes in certain arithmetic progressions*, Journal of the Madras University, (1988), 161–169.

[Mu2] R. Murty, *Problems in Analytic Number Theory*, Springer-Verlag, New York, 2001.

[MM] M. R. Murty and V. K. Murty, *Non-Vanishing of L-Functions and Applications*, Progress in Mathematics, vol. 157, Birkhäuser, Basel, 1997.

[NS] K. Nagasaka and J. S. Shiue, *Benford's law for linear recurrence sequences*, Tsukuba J. Math. **11** (1987), 341–351.

[Nar] W. Narkiewicz, *The Development of Prime Number Theory*, Springer Monographs in Mathematics, Springer-Verlag, New York, 2000.

[Na] M. Nathanson, *Additive Number Theory: The Classical Bases*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1996.

[NT] J. von Neumann and B. Tuckerman, *Continued fraction expansion of* $2^{1/3}$, Math. Tables Aids Comput. **9** (1955), 23–24.

[Ni1] T. Nicely, *The pentium bug*, http://www.trnicely.net/pentbug/pentbug.html

[Ni2] T. Nicely, *Enumeration to* 10^{14} *of the Twin Primes and Brun's Constant*, Virginia J. Sci. **46** (1996), 195–204.

[Nig1] M. Nigrini, *Digital Analysis and the Reduction of Auditor Litigation Risk*. Pages 69–81 in *Proceedings of the 1996 Deloitte & Touche / University of Kansas Symposium on Auditing Problems*, ed. M. Ettredge, University of Kansas, Lawrence, KS, 1996.

[Nig2] M. Nigrini, *The Use of Benford's Law as an Aid in Analytical Procedures*, Auditing: A Journal of Practice & Theory, **16** (1997), no. 2, 52–67.

[NZM] I. Niven, H. Zuckerman, and H. Montgomery, *An Introduction to the Theory of Numbers*, 5th edition, John Wiley & Sons, New York, 1991.

[Nov] T. Novikoff, *Asymptotic behavior of the random* 3-*regular bipartite graph*, Undergraduate Mathematics Laboratory report, Courant Institute, NYU, 2002.

[Ny] J. E. Nymann, *An Application of Diophantine Approximation*, The American Mathematical Monthly **76** (1969), no. 6, 668–671.

[Od1] A. Odlyzko, *On the distribution of spacings between zeros of the zeta function*, Math. Comp. **48** (1987), no. 177, 273–308.

[Od2] A. Odlyzko, *The* 10^{22}*-nd zero of the Riemann zeta function*. Pages 139–144 in *Proceedings of the Conference on Dynamical, Spectral and Arithmetic Zeta Functions*, ed. M. van Frankenhuysen and M. L. Lapidus, Contemporary Mathematics Series, AMS, Providence, RI, 2001.

[Ok] T. Okano, *A note on the transcendental continued fractions*, Tokyo J. Math **10** (1987), no. 1, 151–156.

[Ol] T. Oliveira e Silva, *Verification of the Goldbach conjecture up to* $6 \cdot 10^{16}$, NMBRTHRY@listserv.nodak.edu mailing list, Oct. 3, 2003, http://listserv.nodak.edu/scripts/wa.exe?A2=ind0310&L=nmbrthry&P=168 and http://www.ieeta.pt/∼tos/goldbach.html

[Ols] L. Olsen, *Extremely non-normal continued fractions*, Acta Arith. **108** (2003), no. 2, 191–202.

[Pi] R. G. E. Pinch, *The Carmichael numbers up to* 10^{18}, preprint, http://arxiv.org/abs/math.NT/0604376.

[Pol] G. Polya, *Heuristic reasoning in the theory of numbers*, Amer. Math. Monthly **66** (1959) 375–384.

[vdP1] A. van der Poorten, *An introduction to continued fractions*. Pages 99-138 in *Diophantine Analysis (Kensington, 1985)*, London Mathematical Society Lecture Note Series, Vol. 109, Cambridge University Press, Cambridge, 1986.

[vdP2] A. van der Poorten, *Notes on continued fractions and recurrence sequences*. Pages 86–97 in *Number theory and cryptography (Sydney, 1989)*, London Mathematical Society Lecture Note Series, Vol. 154, Cambridge University Press, Cambridge, 1990.

[vdP3] A. van der Poorten, *Continued fractions of formal power series*. Pages 453–466 in *Advances in Number Theory (Kingston, ON, 1991)*, Oxford Science Publications, Oxford University Press, New York, 1993.

[vdP4] A. van der Poorten, *Fractions of the period of the continued fraction expansion of quadratic integers*, Bull. Austral. Math. Soc. **44** (1991), no. 1, 155–169.

[vdP5] A. van der Poorten, *Continued fraction expansions of values of the exponential function and related fun with continued fractions*, Nieuw Arch. Wisk. (4) **14** (1996), no. 2, 221–230.

[vdP6] A. van der Poorten, *Notes on Fermat's Last Theorem*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Wiley-Interscience, New York, 1996.

[PS1] A. van der Poorten and J. Shallit, *Folded continued fractions*, J. Number Theory **40** (1992), no. 2, 237–250.

[PS2] A. van der Poorten and J. Shallit, *A specialised continued fraction*, Canad. J. Math. **45** (1993), no. 5, 1067–1079.

[Po] C. Porter (editor), *Statistical Theories of Spectra: Fluctuations*, Academic Press, New York, 1965.

[Py] R. Pyke, *Spacings*, J. Roy. Statist. Soc. Ser. B **27** (1965), 395–449.

[QS1] R. Qian and D. Steinhauer, *Rational relation conjectures*, Junior Thesis, Princeton University, Fall 2003.

[QS2] R. Qian and D. Steinhauer, *Eigenvalues of weighted random graphs*, Junior Thesis, Princeton University, Spring 2003.

[Rai] R. A. Raimi, *The first digit problem*, Amer. Math. Monthly **83** (1976), no. 7, 521–538.

[Ra] K. Ramachandra, *Lectures on Transcendental Numbers*, Ramanujan Institute, Madras, 1969.

[Re] F. Reif, *Fundamentals of Statistical and Thermal Physics*, McGraw-Hill, New York, 1965.

[Ric] P. Richter, *An investigation of expanders and ramanujan graphs along random walks of cubic bipartite graphs*, Junior Thesis, Princeton University, Spring 2001.

[RDM] R. D. Richtmyer, M. Devaney, and N. Metropolis, *Continued fraction of algebraic numbers*, Numer. Math. **4** (1962), 68–84.

[Rie] H. J. J. te Riele, *On the sign of the difference* $\pi(x) - \mathrm{Li}(x)$, Mathematics of Computation **48** (1987), no. 177, 323–328.

[Ri] G. F. B. Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, Monatsber. Königl. Preuss. Akad. Wiss. Berlin, Nov. 1859, 671–680 (see [Ed] for an English translation).

[RSA] R. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Comm. ACM **21** (1978), 120–126.

[Roc] D. Rockmore, *Stalking the Riemann Hypothesis: The Quest to Find the Hidden Law of Prime Numbers*, Pantheon, New York, 2005.

[Ro] K. Roth, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 1–20.

[Rub1] M. Rubinstein, *A simple heuristic proof of Hardy and Littlewood's conjecture B*, Amer. Math. Monthly **100** (1993), no. 5, 456–460.

[Rub2] M. Rubinstein, *Low-lying zeros of* L*-functions and random matrix theory*, Duke Math. J. **109** (2001), no. 1, 147–181.

[RubSa] M. Rubinstein and P. Sarnak, *Chebyshev's bias*, Experiment. Math. **3** (1994), no. 3, 173–197.

[Rud] W. Rudin, *Principles of Mathematical Analysis*, 3rd edition, International Series in Pure and Applied Mathematics, McGraw-Hill, New York, 1976.

[RS] Z. Rudnick and P. Sarnak, *Zeros of principal* L*-functions and random matrix theory*, Duke J. of Math. **81** (1996), 269–322.

[RS2] Z. Rudnick and P. Sarnak, *The pair correlation function of fractional parts of polynomials*, Comm. Math. Phys. **194** (1998), no. 1, 61–70.

[RSZ] Z. Rudnick, P. Sarnak, and A. Zaharescu, *The distribution of spacings between the fractional parts of $n^2\alpha$*, Invent. Math. **145** (2001), no. 1, 37–57.

[RZ1] Z. Rudnick and A. Zaharescu, *A metric result on the pair correlation of fractional parts of sequences*, Acta Arith. **89** (1999), no. 3, 283–293.

[RZ2] Z. Rudnick and A. Zaharescu, *The distribution of spacings between fractional parts of lacunary sequences*, Forum Math. **14** (2002), no. 5, 691–712.

[Sai] F. Saidak, *A new proof of Euclid's theorem*, Amer. Math. Monthly **113** (2006), no. 10, 937–938.

[Sar] P. Sarnak *Some applications of modular forms*, Cambridge Trusts in Mathemetics, Vol. 99, Cambridge University Press, Cambridge, 1990.

[Sch] D. Schmidt, *Prime Spacing and the Hardy-Littlewood Conjecture B*, Junior Thesis, Princeton University, Spring 2001.

[Sc] P. Schumer, *Mathematical Journeys*, Wiley-Interscience, John Wiley & Sons, New York, 2004.

[Se] J. P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1996.

[Sh] A. Shidlovskii, *Transcendental Numbers*, Walter de Gruyter & Co., New York, 1989.

[ShTa] J. A. Shohat and J. D. Tamarkin, *The Problem of Moments*, AMS, Providence, RI, 1943.

[Sil1] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Vol. 106, Springer-Verlag, New York, 1986.

[Sil2] J. Silverman, *A Friendly Introduction to Number Theory*, 2nd edition, Prentice-Hall, Englewood Cliffs, NJ, 2001.

[ST] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

[Si] B. Simon, *The classical moment problem as a self-adjoint finite difference operator*, Adv. Math. **137** (1998), no. 1, 82–203.

[SM] S. Simon and A. Moustakas, *Eigenvalue density of correlated complex random Wishart matrices*, Bell Labs Technical Memo, 2004.

[Sk] S. Skewes, *On the difference $\pi(x) - \mathrm{Li}(x)$*, J. London Math. Soc. **8** (1933), 277–283.

[Sl] N. Sloane, *On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/∼njas/sequences/Seis.html

[Sn] N. Snaith, *Derivatives of random matrix characteristic polynomials with applications to elliptic curves*, J. Phys. A **38** (2005), no. 48, 10345–10360.

[So] K. Soundararajan, *Small gaps between prime numbers: The work of Goldston-Pintz-Yildirim*, Bull. of the AMS **44** (2007), no. 1, 1–18.

[SS1] E. Stein and R. Shakarchi, *Fourier Analysis: An Introduction*, Princeton University Press, Princeton, NJ, 2003.

[SS2] E. Stein and R. Shakarchi, *Complex Analysis*, Princeton University Press, Princeton, NJ, 2003.

[SS3] E. Stein and R. Shakarchi, *Real Analysis: Measure Theory, Integration, and Hilbert Spaces*, Princeton University Press, Princeton, NJ, 2005.

[StTa] I. Stewart and D. Tall, *Algebraic Number Theory*, 2nd edition, Chapman & Hall, London, 1987.

[St] Strang, *Linear Algebra and Its Applications*, 3rd edition, Wellesley-Cambridge Press, Wellesley, MA 1998.

[Str] K. Stromberg, *The Banach-Tarski paradox*, Amer. Math. Monthly **86** (1979), no. 3, 151–161.

[Sz] P. Szüsz, *On the length of continued fractions representing a rational number with given denominator*, Acta Arithmetica **37** (1980), 55–59.

[Ta] C. Taylor, *The Gamma function and Kuzmin's theorem*, Junior Thesis, Princeton University, Fall 2002.

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141** (1995), 553–572.

[TrWi] C. Tracy and H. Widom, *Correlation functions, cluster functions, and spacing distributions for random matrices*, J. Statist. Phys. **92** (1998), no. 5–6, 809–835.

[Te] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge University Press, Cambridge, 1995.

[Ti] E. C. Titchmarsh, *The Theory of the Riemann Zeta-function*, revised by D. R. Heath-Brown, Oxford University Press, Oxford, 1986.

[Va] R. C. Vaughan, *On a variance associated with the distribution of primes in arithmetic progression*, Proc. London Math. Soc. (3) **82** (2001), 533–553.

[VW] R. C. Vaughan and T. D. Wooley, *Waring's problem: a survey*. Pages 301–340 in *Number Theory for the Millennium, III (Urbana, IL, 2000)*, A. K. Peters, Natick, MA, 2002.

[Vin1] I. Vinogradov, *Representation of an odd number as the sum of three primes*, Doklady Akad. Nauk SSSR **15** (1937), no. 6–7, 291–294.

[Vin2] I. Vinogradov, *Some theorems concerning the theory of primes*, Mat. Sbornik **2** (1937), no. 44, 179–195.

[Vo] A. Voros, *A sharpening of Li's criterion for the Riemann hypothesis*, preprint.

[VG] W. Voxman and R. Goetschel, Jr., *Advanced Calculus*, Mercer Dekker, New York, 1981.

[Wa] L. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman & Hall / CRC, New York, 2003.

[Wed] S. Wedeniwski, *ZetaGrid*, http://www.zetagrid.net

[Wei1] A. Weil, *Numbers of Solutions of Equations in Finite Fields*, Bull. Amer. Math. Soc. **14** (1949), 497–508.

[Wei2] A. Weil, *Prehistory of the zeta-function*. Pages 1–9 in *Number Theory, Trace Formulas and Discrete Groups (Oslo, 1987)*, Academic Press, Boston, 1989.

[Weir] B. Weir, *The local behavior of Germain primes*, Undergraduate Mathematics Laboratory report, Courant Institute, NYU, 2002.

[We] E. Weisstein, *MathWorld — A Wolfram Web Resource*, http://mathworld.wolfram.com

[Weyl] H. Weyl, *The Classical Groups: Their Invariants and Representations*, Princeton University Press, Princeton, NJ, 1946.

[Wh] E. Whittaker, *A Treatise on the Analytical Dynamics of Particles and Rigid Bodies: With an Introduction to the Problem of Three Bodies*, Dover, New York, 1944.

[WW] E. Whittaker and G. Watson, *A Course of Modern Analysis*, 4th edition, Cambridge University Press, Cambridge, 1996.

[Wig1] E. Wigner, *On the statistical distribution of the widths and spacings of nuclear resonance levels*, Proc. Cambridge Philo. Soc. **47** (1951), 790–798.

[Wig2] E. Wigner, *Characteristic vectors of bordered matrices with infinite dimensions*, Ann. of Math. **2** (1955), no. 62, 548–564.

[Wig3] E. Wigner, *Statistical Properties of real symmetric matrices*. Pages 174–184 in *Canadian Mathematical Congress Proceedings*, University of Toronto Press, Toronto, 1957.

[Wig4] E. Wigner, *Characteristic vectors of bordered matrices with infinite dimensions. II*, Ann. of Math. Ser. 2 **65** (1957), 203–207.

[Wig5] E. Wigner, *On the distribution of the roots of certain symmetric matrices*, Ann. of Math. Ser. 2 **67** (1958), 325–327.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **141** (1995), 443–551.

[Wilf] H. Wilf, *Algorithms and Complexity*, 2nd edition, A. K. Peters, Natick, MA, 2002.

[Wir] E. Wirsing, *On the theorem of Gauss-Kuzmin-Lévy and a Frobenius-type theorem for function spaces*, Acta Arith. **24** (1974) 507–528.

[Wis] J. Wishart, *The generalized product moment distribution in samples from a normal multivariate population*, Biometrika **20 A** (1928), 32–52.

[Wor] N. C. Wormald, *Models of random regular graphs*. Pages 239–298 in *Surveys in combinatorics, 1999 (Canterbury)* London Mathematical Society Lecture Note Series, vol. 267, Cambridge University Press, Cambridge, 1999.

[Wo] T. Wooley, *Large improvements in Waring's problem*, Ann. of Math. (2), **135** (1992), no. 1, 131–164.

[Za] I. Zakharevich, *A generalization of Wigner's law*, Comm. Math. Phys. **268** (2006), no. 2, 403–414.

[Zu] W. Zudilin, *One of the numbers* $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ *is irrational*, Uspekhi Mat. Nauk **56** (2001), 149-150.

[Zy] A. Zygmund, *Trigonometrical Series*, vols. I and II, Cambridge University Press, Cambridge, 1968.

INDEX