ON THE NORMALITY OF NUMBERS

by

Adrian Belshaw

B. Sc., University of British Columbia, 1973
M. A., Princeton University, 1976

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in the Department
of
Mathematics

SIMON FRASER UNIVERSITY
Fall 2005

APPROVAL

Name: Adrian Belshaw

Degree: Master of Science

Title of Thesis: On the Normality of Numbers

Examining Committee:

Dr. Ladislav Stacho
Chair

Dr. Peter Borwein
Senior Supervisor
Professor of Mathematics
Simon Fraser University

Dr. Stephen Choi
Supervisor
Assistant Professor of Mathematics
Simon Fraser University

Dr. Jason Bell
Internal Examiner
Assistant Professor of Mathematics
Simon Fraser University

Date Approved: December 5, 2005

Abstract

A number is normal to the base r if, in its expansion to that base, all possible digit strings of length t are equally frequent for each t. While it is generally believed that many familiar irrational constants are normal, normality has only been proven for numbers expressly invented for the purpose of proving their normality.

In this study we give an overview of the main results to date.

We then define a new normality criterion, strong normality, to exclude certain normal but clearly non-random artificial numbers. We show that strongly normal numbers are normal but that Champernowne's number, the best-known example of a normal number, fails to be strongly normal.

We also re-frame the question of normality as a question about the frequency of modular residue classes of a sequence of integers. This leads to the beginning of a detailed examination of the digits of square roots.

Acknowledgements

I thank Peter Borwein for his excellent advice and his patient encouragement, and for introducing me to the warmth and humanity of the mathematical community. His great wisdom was to keep asking questions until the fire kindled.

I thank Stephen Choi, Imin Chen, and Nils Bruin, for their gentle teaching. They guided me into the first details of the mystery.

I thank my Capilano College teaching colleagues John Field and John Pass for generously adjusting their schedules to make my flight in the SFU starship possible.

I thank the Department of Mathematics at Simon Fraser University, and every staff person, fellow student, and faculty member who has helped me along the way. What a rich environment this is for the exchange of ideas and the expression of mathematical creativity.

I thank my dear friend Beverly Tanchak, and many other friends, for their kind interest when I tried to explain what I was thinking about. Beverly humoured me on more than one occasion when I thought I had proven the normality of $\sqrt{2}$.

I thank my beloved daughter Juniper Belshaw for cheering me on at every step of the way. She will never know the strength of the emotional foundation she gave.

Lastly, I give thanks to Providence that I could set Sundays aside to look into the figurative mind of God.

Contents

Chapter 1

Introduction

Émile Borel introduced normal numbers in a 1909 paper addressing the question of probability on a countably infinite sequence of trials [11]. He defined normality, noted that rational numbers are not normal, and proved that almost all numbers are normal.

A number is normal if, in its decimal expansion, all possible digit strings of length t are equally frequent for each t; below we give more precise and general definitons.

While the question of normality has found a place in a number of elementary texts on number theory (see, for example, Hardy and Wright [21] or Niven [31]), there has been very little progress beyond Borel's original work.

Progress has been limited to the discovery, or perhaps it would be better to say the invention, of new classes of normal numbers. The work of Champernowne [16], Stoneham [37] [38], and others is discussed below.

But nothing is known about the normality of any algebraic irrational number nor of any well-known irrational constant. The only numbers known to be normal have been designed expressly for the purpose of proving their normality.

Yet experimental evidence strongly suggests that many, if not all of the familiar irrationals are indeed normal (see for example, Berggren, Borwein and Borwein [7] or Borwein and Bailey [13]).

Chapter 2

Normality

2.1 Representation of a Real Number in an Integer Base

Any non-negative real number α may be written as a sum of digits expressed in terms of any integer base r, with $r \geq 2$:

$$\alpha = \sum_{j=-d}^{\infty} a_j r^{-j}.$$

We call this series the *expansion* or the *representation* of α to the base r, or (more archaically) in the base r, and for specified r and irrational α it is unique. When α is rational, then its representation in the base r may be given by a terminating or a repeating sequence of coefficients $\{a_j\}$. If α has a terminating representation in the base r, then it also has a representation ending in a repeating sequence in which all digits are equal to $r-1$; apart from this, the representation of a rational number is also unique in each base.

To recover the familiar "decimal" representation of α from the above series, we write

$$\alpha = a_{-d}a_{-(d-1)}\cdots a_0 \cdot a_1 a_2 \cdots$$

The term "decimal" properly refers to expansions to the base 10, but we will use the term loosely to refer to any base. In particular, we will call the point in this expansion the "decimal point" and not the "r-ary point."

We will use the term *string* to denote a sequence $\{a_j\}$ of digits. The string may be finite or infinite; we will call a finite string of t digits a t-string.

A finite string of digits beginning in some specified position we will refer to as a *block*. An infinite string beginning in a specified position we will call a *tail*.

Since we are interested in the asymptotic frequencies of digit strings, we will work in $\mathbb{R}/\mathbb{Z}$ by discarding all digits to the left of the decimal point in the representation of α. If the real numbers α and β have the same fractional part, we write

$$\alpha \equiv \beta \pmod 1.$$

Some of the difficulties in working in $\mathbb{R}/\mathbb{Z}$ arise from the fact that the natural map taking a real number to its fractional part is not a ring homomorphism. In particular, multiplication is not preserved by the map.

2.2 Normal Numbers

The definitions given here are as given by Borel [11] in 1909.

Definition 1 *A number α is* simply normal *to the base r if every 1-string in its expansion to the base r occurs with a frequency approaching $1/r$. That is, given the expansion $\{a_j\}$ of α to the base r, and letting $m_k(n)$ be the number of times that $a_j = k$ for $j \leq n$, we have*

$$\lim_{n\to\infty} \frac{m_k(n)}{n} = \frac{1}{r}$$

for each $k \in \{0, 1, \ldots, r-1\}$.

(It has no impact on the definition if we include the digits to the left of the decimal point, but following Borel they are understood to be excluded, that is, $j, n > 0$.)

Many numbers are simply normal but have highly ordered digital representations. The simplest example is given by $\alpha = 1/3$. In base 2,

$$\alpha = .010101\ldots$$

The strings 0 and 1 each occur with frequency $1/2$. To exclude these simply normal rational numbers from consideration, Borel made a further definition:

Definition 2 *A number α is* normal *to the base r if the number $r^k\alpha$ is simply normal to the base r^j, for every pair of integers j, $k \geq 1$.*

It is clear that no rational number is normal to any base. In any base r, the number will end in some repeating t-string, and the number will fail to be simply normal in the base r^t.

Before stating the first theorem, we give one more definition.

Definition 3 *A sequence of numbers $\{\alpha_j\}$ with $0 \leq \alpha_j < 1$ is* uniformly distributed *in the unit interval if for every subinterval $[c, d)$, letting $m_{[c,d)}(n)$ be the number of times α_j falls in the interval $[c, d)$ for $j \leq n$, we have*

$$\lim_{n\to\infty} \frac{m_{[c,d)}(n)}{n} = d - c.$$

We extend this definition to say a sequence of real numbers $\{\alpha_j\}$ is *uniformly distributed modulo 1* if the sequence of fractional parts of these numbers is uniformly distributed in the unit interval.

Theorem 1 *The following are equivalent:*

(1) The number α is normal to the base r.

(2) Every t-string occurs with frequency $1/r^t$ in the representation of α to the base r.

(3) The sequence $\{r^j\alpha\}$ is uniformly distributed modulo 1 for every integer $j \geq 0$.

Proof. The equivalence of (1) and (3) was proven by Wall in 1949 [39]. It is interesting to note that Wall had set out to show the equivalence of (1) and (2); but this was not proven until 1951 and 1953 in papers by Niven and Zuckerman [32], and Cassels [14]. A number of authors apparently assumed the equivalence of (1) and (2) (including Hardy and Wright [21]; see Wall [39]) before the result had been established. The fact that (1) implies (2) is fairly trivial to show and was noted by Borel [11] in his original discussion of normality; but the converse is anything but trivial.

The proof that (2) implies (1) is elementary but involved, and may be found in Niven [31].

In showing the equivalence of (2) and (3), we follow the proof given by Niven [31]. (Wall's original proof invokes the Weyl criterion, to be discussed below.)

First, let the sequence $\{r^j\alpha\}$ be uniformly distributed modulo 1, and let $a_1a_2\ldots a_t$ be any t-string. From the definition of uniform distribution, the asymptotic frequency of $\{r^j\alpha \pmod 1\}$ in the interval $(.a_1a_2\ldots a_t, .a_1a_2\ldots a_t + 1/r^t)$ is the length of the interval, r^{-t}. But $r^j\alpha$ lies inside this interval $\pmod 1$ if and only if the first t-block of the fractional part of $r^j\alpha$ is $a_1a_2\ldots a_t$, so the asymptotic frequency of this t-string is also r^{-t}. Thus, (3) implies (2).

Conversely, suppose that (2) holds, so every t-string occurs with frequency $1/r^t$ in the base r representation of α. We can divide the interval $[0,1)$ into r^m subintervals, each of length r^{-m}. Each $r^j\alpha$ lies in the subinterval determined by its first t-block, which is the same as the j-th t-block of α; so by a reversal of the argument on the last paragraph, $r^j\alpha \pmod 1$ occurs in each subinterval with asymptotic frequency r^{-t}. Now consider an arbitrary subinterval $[b,c)$. We can approximate $[b,c)$ from within by a set of the r^m subintervals lying entirely inside $[b,c)$, and from without by a set of subintervals completely containing $[b,c)$. The asymptotic frequency of $r^j\alpha \pmod 1$ in each of the two sets of subintervals is equal to the sum of the lengths of the subintervals, and the frequency of the sequence in $[b,c)$ is between its frequencies in the two sets. Since we can approximate the length of $[b,c)$ as closely as we choose by taking m large enough, the asymptotic frequency on $[b,c)$ is $c-b$. This shows that (2) implies (3). □

The equivalence of (1) and (2) is useful, since (2) gives a simpler criterion for deciding normality by examining the digits in the expansion of a number. However, Wall's proof that (1) and (3) are equivalent was the first, and perhaps to this date the only, major breakthrough in the study of normality of numbers. It allows us to decide questions of normality without examining the digits of an expansion at all. The progress made by Bailey and Crandall will be discussed below; but their progress depended on this fundamental result.

The original concept of normality of numbers refers to the expansions of real numbers to some base, and looks at the asymptotic behaviour of the digits in the fractional parts of the numbers. Besicovitch [8] asked a similar question regarding the digits of integers. Obviously, since an integer has only finitely many digits to any given base, we can no longer speak of the asymptotic behaviour of the digits. But we can certainly ask questions about the relative frequencies of digits and strings of digits in the decimal representations of integers. Besicovitch made the following definitions for a natural number m written in the base r,

$$m = a_\mu a_{\mu-1} \dots a_1 a_0,$$

so the a_j are the digits of m in the base r :

1. The number m is *ε-normal* if the frequency of each digit $0, 1, \dots, r-1$ in the expansion of m differs from $1/r$ by less than ϵ; and

2. The number m is *(k, ε)-normal* if the frequency of each k-string in the expansion of m differs from $1/r^k$ by less than ϵ.

The concept of ε-normality of integers, with respect to some base r, is precisely analogous to the concept of simple normality of real numbers, and (k, ε)-normality is loosely analogous to simple normality with respect to the base r^k. Neither Besicovitch nor Hanson [20], who also worked with these ideas, took the next step, so for the sake of speculation we will take it here:

Definition 4 *A natural number m is (k, ε)-normal* **up to** *N if it is (k, ε)- normal for every positive integer $k \leq N$.*

We do not develop any properties of this definition here, but simply note that this is presumably the closest one could come to an integer analogue of (non-simple) normality.

Besicovitch proved that almost all integers are ε-normal and (k, ε)-normal for any choice of ϵ and k, and further that almost all squares of integers are ϵ-normal. This is analogous to Borel's result that almost all numbers are normal.

Hanson made an interesting bridge between the concepts of normality and (k, ϵ)-normality. He proved the following: let $\{b_j\}$ be an increasing sequence of natural numbers, almost all of which are (k, ϵ) normal to some base r, and let ν_j be the number of digits in the base r representation of b_j. Let $S_n = \sum_{j=1}^{n} \nu_j$. Then the number

$$x = .b_1 b_2 b_3 \dots$$

formed by concatenating the numbers in their sequence is normal to the base r if the number of digits in the base r representation of $n\nu_n$ is $O(S_n)$ as $n \to \infty$.

These results allow an easy new proof of the normality of Champernowne's constant; the proof will be given in the next chapter.

2.3 The Measure of the Set of Normal Numbers

In his 1909 paper, Borel [11] proved that almost all real numbers are normal, in the sense that the set of non-normal numbers (mod 1) is of measure zero.

Borel's proof is a simple application of the Central Limit Theorem. It is worth stating and proving Borel's result as he did, both for the beauty of the proof and to illustrate the probabilistic quality of Borel's approach.

Theorem 2 *Let the number α have the base 2 representation*

$$\alpha = .a_1 a_2 a_3 \ldots,$$

where each of the digits may with equal probability $1/2$ take on the the value 0 or 1. Then the probability that the ratio between the number of zeros and the number of ones in the first n digits approaches 1 as n approaches infinity is 1. Conversely, the probability that this ratio approaches some other limit or diverges is zero.

Proof. In the first $2n$ trials, or digits, the number of zeros is between $n - \lambda\sqrt{n}$ and $n + \lambda\sqrt{n}$ with approximate probability

$$\theta(\lambda) = \frac{2}{\sqrt{\pi}} \int_0^{\lambda} e^{-t^2} dt,$$

by an application of the Central Limit Theorem to a binomial distribution of $2n$ trials. This probability tends to 1 very rapidly as λ increases.

Now consider an unboundedly increasing sequence λ_n such that

$$\lim_{n\to\infty} \frac{\lambda_n}{\sqrt{n}} = 0.$$

An example of such a sequence would be $\lambda_n = \log n$. The probability that, in the first $2n$ digits, the number of zeros is between $n - \lambda_n\sqrt{n}$ and $n + \lambda_n\sqrt{n}$ is

$$p_n = \theta(\lambda_n) = \frac{2}{\sqrt{\pi}} \int_0^{\lambda_n} e^{-t^2} dt.$$

If we set $q_n = 1 - p_n$, then q_n approaches 0 as n approaches ∞. In fact, $\sum q_n$ is a convergent series, and therefore the probability that the number of zeros in the first $2n$ digits falls outside the interval $(n - \lambda_n\sqrt{n}, n + \lambda_n\sqrt{n})$ infinitely many times is zero.

This means that, with probability 1, after some n, the number of zeros is always between $n - \lambda_n\sqrt{n}$ and $n + \lambda_n\sqrt{n}$. Then the ratio of zeros to ones is with probability 1, after this n, between

$$\frac{n - \lambda_n\sqrt{n}}{n + \lambda_n\sqrt{n}} \text{ and } \frac{n + \lambda_n\sqrt{n}}{n - \lambda_n\sqrt{n}}.$$

That is, the ratio of zeros to ones is between

$$\frac{1-\frac{\lambda_n}{\sqrt{n}}}{1+\frac{\lambda_n}{\sqrt{n}}} \text{ and } \frac{1+\frac{\lambda_n}{\sqrt{n}}}{1-\frac{\lambda_n}{\sqrt{n}}}.$$

By our choice of λ_n, these ratios tend to 1. □

Borel proceeded from this to prove that almost all real numbers are normal to every base. Such a number normal to every integer base is called *absolutely normal.*

The proofs of Hardy and Wright [21] and Niven [31] were virtually identical, but fundamentally different from Borel's proof. The theorem was equivalent to Borel's but the statement was different:

Theorem 3 *Almost every number is absolutely normal.*

Proof. Hardy and Wright proved first that almost every number is simply normal in any given base r. They made no appeal to the Central Limit Theorem; instead, they used an elementary but lengthy estimation argument.

The set of numbers not normal to the base r is therefore of measure zero. Now the theorem follows from two applications of the fact that a countable union of sets of measure zero also has measure zero. (Borel's argument also makes use of this fact.) □

An entirely different proof was given by Riesz [33]: we follow the summary by Kuipers and Niederreiter [23]. The transformation

$$\alpha \mapsto r\alpha$$

is Lebesgue measure preserving (for a proof of this, see Dajani and Kraaikamp [18]), and therefore ergodic. Then, by the ergodic theorem, for any Lebesgue integrable function on $[0,1)$, we have

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} f(r^k \alpha) = \int_0^1 f(x)dx$$

for almost every real α. If we take f to be the indicator function on the interval $[a,b)$, this gives equidistribution of the sequence $\{r^k\alpha\} \pmod 1$, and so almost every α is normal.

Wall [39] noted that the set of numbers not normal to any base is uncountably infinite, although it is of measure zero. In particular, he gave the Liouville numbers $\alpha = \sum_{j=0}^{\infty} a_j r^{-j!}$ (the a_j here can be taken from any finite set of integers, not necessarily $\{0,1,\ldots,r-1\}$) as an example of a set of numbers known to be uncountable and provably not normal. As an aside, he pointed out that this suffices to prove that the set of Liouville numbers is of measure zero.

We offer a direct proof of this fact:

Theorem 4 *In any base r, there are uncountably many non-normal numbers.*

Proof. Let S be any countably infinite set of numbers not normal in the base r. Then S can be indexed by the integers, so S is a sequence α_j with

$$\alpha_j \equiv .a_{1,j}a_{2,j}a_{3,j}\ldots \pmod 1.$$

For simplicity, write α_j with a tail of zeros where possible.

Now construct the number $\beta = .b_1b_2b_3\ldots.$ by setting

$$b_{2j-1}b_{2j} = 00$$

if $a_{2j-1,j}a_{2j,j} \neq 00$, and

$$b_{2j-1}b_{2j} = 01$$

otherwise. (Here the notation cd denotes a 2-string, not a product.)

The number β is not normal to the base r, since it contains no 2-strings other than 00 and 01. However, our Cantor diagonalization guarantees that β is different from each element of S. This shows that no countable set can contain all the numbers not normal to the base r; therefore the set of all such numbers is uncountable. □

There are a number of other results on the measure of sets of normal and non-normal numbers. We give only a few examples.

In 1966, Šalát [34] showed that the set of all simply normal numbers is of the first Baire category, and so is the set of all absolutely normal numbers.

Cassels [15] proved that there are uncountably many numbers not normal to the base 3 but normal in every base not a power of 3. Schmidt [35] generalized this result with the following theorem:

Theorem 5 *If the set of integers greater than* 1 *is divided into two disjoint classes R and S such that, for each k, every power of k is in the same class as k, then there exist uncountably many α such that α is non-normal to every base in R but normal to every base in S.*

Chapter 3

Examples of Normality and Non-normality

3.1 Numbers Provably Not Normal

As mentioned above, no rational number is normal in any base.

The Liouville numbers of the class mentioned in the last chapter, of the form $\alpha = \sum_{j=0}^{\infty} a_j r^{-j!}$, are not normal in the base r, for the simple reason that they contain too many zeros to be normal. In fact, the limiting frequency of zeros in the base r representation of one of these numbers is 1.

It is not hard to construct non-normal numbers. All one needs is a rule for writing down digits in a way that produces visibly too many or too few of some particular digit. As an example, consider the number

$$\alpha = .01001000100001\ldots.$$

This number is not normal, no matter what the base in which we choose to interpret the digits.

However, suppose we read the above number in base 2. Now if we write the same number in any base not a power of 2, the normality of the number is an open question.

As a converse to the state of affairs mentioned in the introduction, that no "naturally occurring" irrational number has been proven to be normal, it is also true that no "naturally occurring" irrational has been shown not to be normal.

An amusing and beautiful construction of a class of abnormal numbers is given by Martin [28].

3.2 Numbers Provably Normal

It was not until 1917, eight years after Borel's paper, that Sierpiński was able to produce the first example of a normal number [36]. (Lebesgue apparently constructed a normal

number in 1909, but did not publish his work until 1917; the papers by Sierpiński and Lebesgue appeared side by side in the same journal.) Sierpiński's approach was to build a well-defined set of normal numbers, and then take the lower limit of that set; the lower limit was of necessity a normal number. Lebesgue's construction [24] was similarly intangible.

However, Champernowne [16] produced a more tangible example of a normal number in 1933. The Champernowne number is

$$\alpha = .1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ldots.$$

The number is written in the base 10, and its digits are obtained by concatenating the natural numbers written in the base 10. This number is probably the best-known example of a normal number. It is the only example given by Hardy and Wright [21], but without a proof of its normality. Niven [31] also uses this example and proves its normality, giving a proof more direct than Champernowne's.

Borwein and Bailey [13] give a nice way of representing Champernowne's number: let $f(n) = \sum_{1 \le j \le n} [\log_{10} j]$, where $[\beta]$ is the integer part of β. Then

$$\sum_{n=1}^{\infty} \frac{n}{10^{n+f(n)}}$$

is Champernowne's number.

We give a simple proof of the normality of Champernowne's number, based on the results of Besicovitch and Hanson mentioned in the last chapter.

Theorem 6 *Champernowne's number is normal to the base* 10.

Proof. Champernownes's number is given in the base 10 by

$$\alpha = .b_1 b_2 b_3 \ldots;$$

where $b_j = j$, so the digits of α are the natural numbers concatenated in the order of their occurrence and written in the base 10. Then by Besicovitch's result, almost every b_j is (k, ϵ)-normal for any k and ϵ. Since the $\{b_j\}$ form an increasing sequence, one of the conditions of Hanson's theorem is met.

Now letting ν_j be the number of digits in the base 10 representation of j, we have $\nu_{10^k-1} = k$. Letting S_{10^k-1} be the sum of the first $10^k - 1$ values of ν_j, we have

$$\frac{9}{10} 10^k k < S_{10^k-1} < 10^k k.$$

But then

$$(10^k - 1)\nu_{10^k-1} < 10^k k = O(S_{10^k-1})$$

and the second condition of Hanson's theorem is met. □

There is an even easier proof of this result, mentioned below.

The Champernowne number is transcendental; this is a corollary of a more general result of Mahler [28] which is given below.

Champernowne made the conjecture that the number obtained by concatenating the primes, $\alpha = .2\ 3\ 5\ 7\ 11\ 13\ldots$, was normal in the base 10. Copeland and Erdös [17] proved this in 1946 , as a corollary of a more general result:

Theorem 7 *Let $\{a_j\}$ be an increasing sequence of integers such that for any $\theta < 1$ we have, for N sufficiently large, that the number of a_j less than N is greater than N^θ. Then if the $\{a_j\}$ are written in the base r, the number $.a_1a_2a_3\ldots$ is normal in the base r.*

The proof of this theorem is based on Besicovitch's concept of (k, ϵ) normality, as is our proof of Theorem 4.

The corollary follows since the prime number theorem implies that for any $c < 1$, if $\pi(N)$ is the number of primes not greater than N, $\pi(N) > cN/\log N$ if N is large enough. Since $cN/\log N > N^\theta$ for any $\theta < 1$, for sufficiently large N, the sequence of prime numbers satisfies the condition of the Copeland-Erdös theorem.

The number formed by concatenating the primes is commonly called the Copeland-Erdös number.

With the Copeland-Erdös theorem in hand, the normality of Champernowne's number follows as a trivial corollary.

In their paper on the concatenated primes, Copeland and Erdös conjectured that, if $p(x)$ is a polynomial in x taking positive integer values whenever x is a positive integer, then the number

$$.p(1)p(2)p(3)\ldots$$

formed by concatenating the base 10 values of the polynomial at $x = 1, 2, 3, \ldots$ is normal in the base 10. This result was proven by Davenport and Erdös in 1952 [19]. This fully generalized Besicovitch's early result that the number $\alpha = .1\ 4\ 9\ 16\ 25\ldots$, formed by concatenating the squares of the positive integers, is normal in the base 10 [8].

In 1937 Mahler [28] showed that the decimal

$$.p(1)p(2)p(3)\ldots$$

formed by concatenating the values of a non-constant polynomial p, if these values are themselves integers, is a transcendental number. The transcendence of Champernowne's number is an immediate consequence.

In contrast to these examples of normality constructed by concatenation, Stoneham constructed a number of classes of normal numbers based on the extension of the concept of (j, ε)-normality to rational fractions (see, for example, [37] or [38]). Korobov [25] constructed provably normal continued fractions.

A Bailey-Borwein-Plouffe-type formula, or *BBP-type* formula, is an expression

$$\alpha = \sum_{j=0}^{\infty} \frac{p(j)}{r^j q(j)} ,$$

where p and q are polynomials. Such formulas arose as a method of calculating isolated digits of π, $\log 2$, and other constants [4].

In 2003 Bailey and Crandall proved normality to the base r for a class of numbers with BBP-type formulas [6]. We give a simpler result of Borwein and Bailey [13]:

Theorem 8 *For $r > 1$ and c coprime to r, the generalized Stoneham number*

$$\alpha_{b,c} = \sum_{j=1}^{\infty} \frac{1}{c^j r^{c^j}}$$

is normal in the base r.

The proof of this theorem is much easier than the proof of the stronger result given by Bailey and Crandall; it relies on Roth's Theorem and the Hot Spot Lemma (see below). On the other hand, this theorem can be derived from Bailey and Crandall's result as an easy corollary.

Another corollary of Bailey and Crandall's result is that the generalized Korobov number

$$\beta_{(b,c,d)} = \sum_{j=1}^{\infty} \frac{1}{c^{d^j} r^{d^j}}$$

is normal in the base r when $r, c, d > 1$ and r, c are coprime. Several similar classes of numbers are shown to be normal as a corollary of the general result.

3.3 Numbers Believed to be Normal

The concept of normality as defined by Borel is explicitly related to randomness in the digits. In fact, Borel was thinking of numbers arising from a random sequence of digits: one builds such a number, say in the base 10, by drawing one of 10 balls numbered from 0 to 9 out of a hat, recording the digit on the ball, replacing the ball, and continuing forever. Then with probability 1, such a random number will be normal to the base 10 [11].

A number like Champernowne's number is obviously highly patterned, even though it is normal.

On the other hand, to this time nobody has been able to discern any pattern in the expansions of naturally occurring irrational constants like π, e, $\sqrt{2}$, and $\log 2$ in any base. Statistical tests performed so far on the expansions have been consistent with random behaviour.

For example, Kanada [22] computed the first 200 million digits of π in the base 10, and found the relative frequency of each digit to be close to .1, with a χ^2 value of 4.13; a χ^2 value this low indicates that the observed frequencies are close to the frequencies expected in a number with randomly chosen digits. More recently Kanada computed the first trillion decimal and hexadecimal digits of π, and found relative frequencies of the single digits in keeping with the hypothesis that π is simply normal to the bases 10 and 16. (This result is quoted by Borwein and Bailey [13].)

Bailey, Borwein, Crandall and Pomerance [3] showed, in 2003, that the asymptotic number of occurrences of the digit 1 in the first N digits of the binary expansion of any real algebraic irrational number α is at least $CN^{\frac{1}{D}}$, where D is the degree of α and C is a constant depending on α. While this result is remarkable, it is far short of the asymptotic number of occurrences $N/2$ to be expected if algebraic irrationals are indeed normal numbers.

Beyer, Metropolis and Neergard [10] applied three statistical tests to the digits of irrational square roots in various bases and found nothing inconsistent with the hypothesis of normality.

There may be subtle or rare instances of non-normality which would be difficult to detect by statistical methods. On the other hand, an apparent lack of randomness in the digits of a number is not in itself proof of a lack of normality, since even truly random numbers will occasionally fail randomness tests: a 95% level of confidence should only be achieved 95% of the time.

Chapter 4

Strongly Normal Numbers

4.1 Binomial Normality

It is ironic that most, if not all, of the numbers known to be normal have highly patterned digital representations. For example, while Champernowne's number in the base 2,

$$\gamma = .1\ 10\ 11\ 100\ 101\ldots\ ,$$

is normal to the base 2, there is an increasing excess of ones in the expansion. This does not prevent the asymptotic frequency of the digit 1 from approaching 1/2. However, the convergence to the asymptotic frequency is slower than one would expect to see in a typical binomial sequence of zeros and ones.

On the other hand, the distribution of digits in naturally-occurring irrational numbers like π and $\sqrt{2}$ is exactly what one would expect to see in a binomially random number.

Borel's original definition of normality has the advantage of great simplicity. None of the current profusion of concatenated monsters were known at the time, so there was no need for a stronger definition.

However, one would like a test or a set of tests to eliminate exactly those numbers that do not behave in the limit in every way as a binomially random number defined as follows.

Definition 5 *Let each of the numbers $a_1, a_2, a_3, \ldots$ be chosen with equal probability from the set of integers $\{0, 1, \ldots, r-1\}$, and let $\alpha = .a_1a_2a_3\ldots$ be the number represented in the base r by the concatenation of the digits a_j, $j = 1, 2, 3, \ldots$. Then α is a* **binomially random** *number in the base r.*

This leads to the following heuristic meta- definition.

Definition 6 *A number is* **binomially normal** *to the base r if it passes every asymptotic test on the frequencies of the digits that would be passed with probability 1 by a binomially random number.*

Borel's test of normality is passed with probability 1 by a binomially random number, so it would certainly be passed by a binomially normal number as well. However, there are many tests that would be failed by some normal numbers, but passed with probability 1 by a binomially random number.

It would be worthwhile to make this meta-definition concrete by finding an asymptotic test that was passed by all binomially normal numbers, and only by the binomially normal numbers.

4.2 Strong Normality

We were able to carry out part of the program suggested in the last section.

In this section, we define strong normality, and in the following sections we prove that almost all numbers are strongly normal and that Champernowne's number is not strongly normal.

The definition is motivated as follows: let a number α be represented in the base r, and let $m_k(n)$ represent the number of occurrences of the kth 1-string in the first n digits. Then α is simply normal to the base r if

$$\frac{rm_k(n)}{n} \to 1$$

as $n \to \infty$, for each $k \in \{0, 1, \ldots, r-1\}$. But if a number is binomially random, then the discrepancy $m_k(n) - n/r$ should fluctuate, with an expected value of $\sqrt{n}$.

The following definition makes this idea precise:

Definition 7 *For α and $m_k(n)$ as above, α is* simply strongly normal *to the base r if*

$$\limsup_{n\to\infty} \frac{(m_k(n) - n/r)^2}{\frac{r-1}{r^2} n^{1+\varepsilon}} = 0$$

and

$$\limsup_{n\to\infty} \frac{(m_k(n) - n/r)^2}{\frac{r-1}{r^2} n^{1-\varepsilon}} = \infty$$

for any $\varepsilon > 0$.

The constant $(r-1)/r^2$ is derived from the variance of the binomial distribution, but its value is of no importance. It can be replaced by any arbitrary constant without changing the definition.

Definition 8 *A number is* strongly normal *to the base r if it is simply strongly normal to each of the bases r^j, $j = 1, 2, 3, \ldots$.*

4.3 Almost All Numbers are Strongly Normal

The proof that almost all numbers are strongly normal is based on Borel's original proof [11] that almost all numbers are normal (see the proof of Theorem 2 above).

Theorem 9 *Almost all numbers are simply strongly normal to any integer base $r > 1$.*

Proof. Let α be a binomially random number in the base r, so that the nth digit of the representation of α in the base r is, with equal probability, randomly chosen from the numbers 0, 1, 2, ..., $r-1$. Let $m_k(n)$ be the number of occurrences of the 1-string k in the first n digits of α.

Then $m_k(n)$ is a random variable of binomial distribution with mean n/r and variance $\frac{n(r-1)}{r^2}$. As $n \to \infty$, the random variable approaches a normal distribution with the same mean and variance.

The probability that

$$\left(m_k(n) - \frac{n}{r}\right)^2 > \frac{r-1}{r^2} n^{1+\varepsilon/2}$$

is the probability that

$$\left|m_k(n) - \frac{n}{r}\right| > B\sqrt{n}n^{\varepsilon/4},$$

where $B = \sqrt{r-1}/r$, and this probability rapidly approaches zero as $n \to \infty$.

With probability 1, only finitely many $m_k(n)$ satisfy the inequality, and so with probability 1

$$\limsup_{n\to\infty} \frac{(m_k(n) - n/r)^2}{\frac{r-1}{r^2} n^{1+\varepsilon/2}} < 1.$$

We have

$$\limsup_{n\to\infty} \frac{(m_k(n) - n/r)^2}{\frac{r-1}{r^2} n^{1+\varepsilon}} = \limsup_{n\to\infty} \left(\frac{(m_k(n) - n/r)^2}{\frac{r-1}{r^2} n^{1+\varepsilon/2}}\right)\left(\frac{1}{n^{\varepsilon/2}}\right).$$

The first factor in the right hand limit is less than 1 (with probability 1), and the second factor is zero in the limit.

With probability one, this supremum limit is zero, and the first condition of strong normality is satisfied.

The same argument, word for word, but replacing $1 + \varepsilon/2$ with $1 - \varepsilon/2$ and reversing the inequalities, establishes the second condition. □

As with the corresponding result for normality, this is easily extended.

Corollary 10 *Almost all numbers are strongly normal to any base r.*

Proof. By the theorem, the set of numbers in $[0,1)$ which fail to be simply strongly normal to the base r^j is of measure zero, for each j. The countable union of these sets of measure zero is also of measure zero. Therefore the set of numbers simply strongly normal to every base r^j is of measure 1. □

Corollary 11 *Almost all numbers are strongly normal to every base.*

4.4 Champernowne's Number is Not Strongly Normal

We begin by examining the digits of Champernowne's number in the base 2,

$$\gamma = .1\ 10\ 11\ 100\ 101\ldots\ .$$

When we concatenate the integers written in base 2, we see that there are 2^{n-1} integers of n digits. As we count from 2^n to $2^{n+1}-1$, we note that every integer begins with the digit 1, but that every possible selection of zeros and ones occurs exactly once in the other digits, so that apart from the excess of initial ones there are equally many zeros and ones in the non-initial digits.

As we concatenate the integers from 1 to 2^k-1, we write the first

$$\sum_{n=1}^{k} n2^{n-1} = (k-1)2^k + 1$$

digits of γ. The excess of ones in the digits is

$$2^k - 1.$$

The locally greatest excess of ones occurs at the first digit of 2^k, since each power of 2 is written as a 1 followed by zeros. At this point the number of digits is $(k-1)2^k+2$ and the excess of ones is 2^k. That is, the actual number of ones in the first $N=(k-1)2^k+2$ digits is

$$m_1(N) = (k-2)2^{k-1} + 1 + 2^k.$$

This gives

$$m_1(N) - \frac{N}{2} = 2^{k-1}$$

and

$$\left((m_1(N) - \frac{N}{2}\right)^2 = 2^{2(k-1)}.$$

Thus, we have

$$\frac{\left((m_1(N) - \frac{N}{2}\right)^2}{\frac{1}{4}N^{1+\varepsilon}} \geq \frac{2^{2(k-1)}}{\frac{1}{4}\left((k-1)2^k\right)^{1+\varepsilon}}.$$

The limit of the right hand expression as $k \to \infty$ is infinity for any sufficiently small positive ε. Since the left hand limit is the first supremum limit in our definition of strong normality, we have proven the following theorem:

Theorem 12 *Champernowne's number in the base 2 is not strongly normal to the base 2.*

4.5 Strongly Normal Numbers are Normal

If any strongly normal number failed to be normal, then the definition of strong normality would be inappropriate. Fortunately, this does not happen.

Theorem 13 *If a number α is simply strongly normal to the base r, then α is simply normal to the base r.*

Proof. It will suffice to show that if a number is not simply normal, then it cannot be simply strongly normal.

Let $m_k(n)$ be the number of occurrences of the 1-string k in the first n digits of the expansion of α to the base r, and suppose that α is not simply normal to the base r. This implies that for some k

$$\lim_{n\to\infty} \frac{rm_k(n)}{n} \neq 1.$$

Then there is some $Q > 1$ and infinitely many n_i such that either

$$rm_k(n_i) > Qn_i$$

or

$$rm_k(n_i) < \frac{n_i}{Q}.$$

If infinitely many n_i satisfy the former condition, then for these n_i,

$$m_k(n_i) - \frac{n_i}{r} > Q\frac{n_i}{r} - \frac{n_i}{r} = n_iP$$

where P is a positive constant.

Then for any $R > 0$ and small ε,

$$\limsup_{n\to\infty} R\frac{(m_k(n) - \frac{n}{r})^2}{n^{1+\varepsilon}} \geq \limsup_{n\to\infty} R\frac{n^2P^2}{n^{1+\varepsilon}} = \infty,$$

so α is not simply strongly normal.

On the other hand, if infinitely many n_i satisfy the latter condition, then for these n_i,

$$\frac{n_i}{r} - m_k(n_i) > \frac{n_i}{r} - \frac{n_i}{Qr} = n_iP,$$

and once again the constant P is positive and the rest of the argument follows. □

The general result is an immediate corollary.

Corollary 14 *If α is strongly normal to the base r, then α is normal to the base r.*

4.6 No Rational Number is Simply Strongly Normal

A rational number cannot be normal, but it will be simply normal to the base r if each 1-string occurs the same number of times in the repeating string in the tail. However, such a number is not simply strongly normal.

If α is rational and simply normal to the base r, then if we restrict ourselves to the first n digits in the repeating tail of the expansion, the frequency of any 1-string k is exactly n/r. The excess of occurences of k can never exceed the constant number of times k occurs in the repeating string. Therefore, with $m_k(n)$ defined as before,

$$\limsup_{n\to\infty} \left(m_k(n) - \frac{n}{r}\right)^2 = Q,$$

with Q a constant.

But

$$\limsup_{n\to\infty} \frac{K}{n^{1-\varepsilon}} = 0$$

for any K if ε is small, so α does not satisfy the second criterion of strong normality.

Simple strong normality is not enough to imply normality. As an illustration of this, consider the number

$$\alpha = .01\ 0011\ 000111\ldots,$$

a concatenation of binary strings of length $2l$ in each of which l zeros are followed by l ones. After the first $l-1$ such strings, the zeros and ones are equal in number. and the number of digits is

$$\sum_{k=1}^{l-1} 2k = 2l(l-1).$$

After the next l digits there is a locally maximal excess of $l/2$ zeros and the total number of digits is $2l^2 - l$. Thus, the greatest excess of zeros grows like the square root of the number of digits, and so does the greatest shortage of ones. It is not hard to verify that α satisfies the definition of simple strong normality to the base 2. However, α is not normal to the base 2.

4.7 Further Questions

We have not produced an example of a strongly normal number. Can such a number be constructed?

It is natural to conjecture that such naturally occurring constants as the real algebraic irrational numbers, π, e, and $\log 2$ are strongly normal.

It is easy to construct normal concatenated numbers which, like Champernowne's number, are not strongly normal. Do all the numbers

$$\alpha = p(1)p(2)p(3)\ldots,$$

where p is a polynomial taking positive integer values at each integer, fail to be strongly normal? Does the Copeland-Erdös concatenation of the primes fail to be strongly normal?

Chapter 5

Integer Conditions for Normality

5.1 Modular Normality

The question of normality of real algebraic irrationals can be re-framed as a question in the integers. This approach is based on a simple observation which we state as a lemma.

Lemma 1 *Let the fractional part of α have the base r expansion*

$$(\alpha) \equiv .a_1 a_2 a_3 \ldots .$$

and $[r^m \alpha]$ be the integer part of $r^m \alpha$. Then

$$a_m \equiv [r^m \alpha] \pmod{r}.$$

Proof. Multiplying α by r^m has the effect of moving the decimal point m places to the right, so the last digit of $[r^m \alpha]$ expressed in the base r is a_m. The last digit of an integer written in the base r is its residue class modulo r. □

This has an immediate consequence of enough interest that we state it, too, as a lemma.

Lemma 2 *The number of occurrences of k in the first n digits, after the decimal point, of the number α written in the base r is equal to the number of occurrences of the kth residue class $\pmod{r}$ in the first n terms of the integer sequence $\{[r^j \alpha]\}$.*

Now we are in a position to give modular equivalents to the original definitions of normality.

Theorem 15 *(1) The real number α is simply normal to the base r if and only if the frequency of the kth residue class modulo r in the integer sequence $\{[r^n \alpha]\}$ approaches $1/r$ as $n \to \infty$, for every $k \in \{0, \ldots, r-1\}$.*

(2) The number α is normal to the base r if and only if the the frequency of the kth residue class modulo r^j in the the sequence $\{[r^{jn}\alpha]\}$ approaches $1/r^j$ as $n \to \infty$, for every $k \in \{0, \ldots, r^j - 1\}$ and every j.

(3) The number α is absolutely normal if and only if the frequency of the kth residue class modulo r in the sequence $\{[r^n\alpha]\}$ approaches $1/r$ as $n \to \infty$, for every $k \in \{0, \ldots, r-1\}$ and every r.

Proof. The theorem follows from the second lemma and the original definition of each of the three types of normality. □

5.2 Normal Sequences in an Integer Modulus

The following definition, motivated by the foregoing, will be useful.

Definition 9 *Given a sequence of integers $\{D_n\}$ and an integer $r > 1$, let $m_k(n)$ be the number of occurrences of the kth residue class modulo r in the first n elements of the sequence. Then $\{D_n\}$ is a* simply normal sequence modulo r *if the frequency $m_k(n)/n$ of the kth residue class approaches $1/r$ as n approaches ∞.*

We also define normality of a sequence modulo r, and absolute normality of a sequence, in the appropriate ways.

It should be noted that this definition of normality on a sequence of integers is fundamentally different from the definition of (j, ε)-normality on a single integer.

5.3 An Integer Criterion for Normality of Square Roots

In this section we consider the irrational square roots $\sqrt{c}$, where c is a positive non-square integer .

Theorem 16 *For each positive integer n, let A_n^2 be the greatest square integer less than $r^{2n}c$. Then $\sqrt{c}$ is simply normal to the base r if and only if the sequence of integers A_n is a simply normal sequence modulo r.*

Proof. For each n, $A_n = [r^n\sqrt{c}]$. The theorem is evident from the first part of Theorem 15 and the definition of a simply normal sequence. □

This suggests a new line of attack on the question of whether irrational square roots are normal.

For a given base r and non-square integer c, we examine the behaviour of the squares nearest to $r^{2n}c$. For each n, let A_n be the greatest integer such that $A_n^2 < r^{2n}c$, and let $B_n = A_n + 1$, so B_n^2 is the least square greater than $r^{2n}c$.

We now restrict ourselves to the case $r = 2$. If

$$(2A_n + 1)^2 < 2^{2(n+1)}c,$$

then $A_{n+1} = 2A_n + 1$; otherwise, $A_{n+1} = 2A_n$.

Let $s_n = r^{2n}c - A_n^2$, and $t_n = B_n^2 - r^{2n}c$. We have $B_n^2 - A_n^2 = s_n + t_n = 2A_n + 1$.

As we pass from n to $n + 1$, there are two cases. First, suppose $s_n > t_n$, so B_n^2 is the best square approximation to $r^{2n}c$. Then

$$\begin{aligned} A_{n+1} &= 2A_n + 1, \\ B_{n+1} &= 2B_n, \\ t_{n+1} &= 4t_n, \end{aligned}$$

and

$$s_{n+1} = 2s_n - 2t_n + 1.$$

On the other hand, if A_n^2 is the closest square to $r^{2n}c$, then $s_n < t_n$; note that $s_n < t_n + 2$, since s_n cannot equal $t_n + 1$. In this case,

$$\begin{aligned} A_{n+1} &= 2A_n, \\ B_{n+1} &= 2B_n - 1, \\ s_{n+1} &= 4s_n, \end{aligned}$$

and

$$t_{n+1} = 2t_n - 2s_n - 1.$$

A square root algorithm published on the Internet by Weisstein [41] is very similar to our algorithm and is likely to be based on the same principle.

The map

$$\varphi : (A_n, s_n, r^{2n}c, t_n, B_n) \mapsto (A_{n+1}, s_{n+1}, r^{2(n+1)}c, t_{n+1}, B_{n+1})$$

is invertible. The easiest way to generate the inverse map is to note that $A_{n-1} = A_n/2$ if A_n is even, and otherwise $A_{n-1} = (A_n - 1)/2$.

The smaller of the two errors $\{s_n, t_n\}$ grows exponentially by powers of 4, while the larger error grows exponentially by powers of 2. The closest square approximants will remain on the same side of (above or below) the sequence $r^{2n}c$ until the smaller error overtakes the larger one, at which point the nearest square switches to the other side of $r^{2n}c$. When the smaller error is very small, the larger error is close to $2A_n \approx 2r^{2n}c$ and the closest square switches sides in at most n steps.

Can questions about the behaviour of the sequence $\{A_n\}$ be framed precisely enough to give a useful approach to the question of normality?

5.4 The Binary Digits of $\sqrt{2}$

In this section we offer the simplest concrete example. Take r and c both to be 2, so A_n^2 is the greatest square less than 2^{2n+1}, and

$$\begin{aligned} B_n &= A_n + 1, \\ s_n &= 2^{2n+1} - A_n^2, \\ t_n &= B_n^2 - 2^{2n+1}. \end{aligned}$$

The equation

$$2^{2n+1} + t_n = B_n^2$$

immediately implies that t_n cannot be a square for $n > 3$.

Now let us examine the equation

$$A_n^2 + s_n \equiv 2^{2n+1} \pmod{p},$$

where p is any odd prime. If p divides s_n, then 2 must be a quadratic residue modulo p. This implies that $p \equiv \pm 1 \pmod 8$. The same argument applies to t_n; so all odd prime divisors of s_n and t_n are congruent to $\pm 1 \pmod 8$. Since $s_n + t_n$ grows exponentially, the values of these two error terms are constrained to an increasingly sparse set of integers.

Beukers has shown [9] that if x, n, and D are integers, and $x^2 + D = 2^n$, then

$$n < \frac{10 \log |D|}{\log 2} + 435.$$

This implies that any value of t_n or s_n can only occur finitely many times. However, the lower bound on their values grows like $2^{n/10}$, so the longest possible subsequences in which A_n has the same parity are still approximately of length n. However, as n increases, the rising lower bound on values of t_n and s_n also has the effect of making the possible values for these errors an increasingly sparse set.

According to Lemma 1, the residue class of A_n modulo 2 gives the nth digit of the binary expansion of $\sqrt{2}$. If the greatest square less than 2^{2n+1} is even, the nth digit is 0; otherwise, it is 1.

As an amusing aside, we present a way of calculating an isolated binary digit of $\sqrt{2}$. To find the nth digit, we simply need to find the greatest square less than 2^{2n+1}.

A crude way to find A_n in $\log n / \log 2$ steps is given here. Let Q be a starting estimate for A_n, and for certainty set $Q = 2^n$ and $P = 2^{2n+1}$. Then

$$\hat{k} = \frac{P - Q^2}{2Q}$$

is an estimate of k, the actual number of squares greater than Q and less than P.

Replace Q with the new estimate $Q + [\hat{k}]$ and repeat. When $\hat{k} < 1$, we are done.

This is a variant of Newton's method. It is not fast, since each step involves a squaring and a division of large numbers when n is large.

The same method can be used to calculate an isolated digit of any root in any base. If A_n is expressed in the base r then the claim that we have calculated an isolated digit of the root is a hoax, since all the earlier digits have simply been shifted into the integer A_n. But all we actually need to know is the residue class of A_n modulo r, and we can find this in any base. If our working base for the calculation is not r, then we really have not explicitly calculated any of the earlier digits in the process of finding the nth digit.

Once we have found A_n, it is easy and fast to calculate a string of digits before or after the nth digit, using the map φ of the last section.

5.5 Further Observations on the Map φ Generating the Binary Digits of $\sqrt{c}$

In this section we look again at the map φ as discussed in Section 5.3. It will be clear that it suffices to consider φ as a map on the pairs (s_n, t_n), since the numbers A_n, 2^{2n+1}, and B_n can be generated from these.

Given a positive non-square integer c, we set A_0 to be the greatest integer such that A_0^2 is less than c, and put $B_0 = A_0 + 1$. Then $s_0 = c - A_0$ and $t_0 = B_0 - c$. Now we can use the map φ to generate the sequence of pairs (s_n, t_n):

$$(s_n, t_n) = \varphi^n(s_0, t_0).$$

As in the last section, if we consider

$$A_n^2 + s_n \equiv 2^{2n}c \pmod{p}$$

for each odd prime p not dividing c, we see that p can only be a factor of s_n if c is a quadratic residue modulo p.

The smaller of $\{s_n, t_n\}$ grows at least twice as rapidly as the larger, until their relative sizes are reversed. It takes fewer than n steps for the smaller quantity to overtake the larger.

One would like to say something about the relative frequency of the odd and even values of s_n, since when s_n is even the nth digit of $\sqrt{c}$ is also even. The discussion of the last section makes it clear that we can have runs of digits $O(n)$ in length. In fact, if the digits have pseudorandom properties then we want to see occasional long runs of the same digit , so it is encouraging that we cannot preclude them. On the other hand, we want s_n to have equally frequent and lengthy runs in each parity, and so far we have no inkling of a way to approach this.

Each time s_n changes parity, the modular history appears to be erased. There is an easily comprehensible pattern while s_n is smaller and growing by a factor of 4 with each iteration, but the modular trajectory when s_n is larger and odd is difficult to understand.

It is the combination of modular behaviour and size comparison that makes the problem both interesting and intractable.

The parity of s_n changes when the relative magnitudes of s_n and t_n reverse. Each time this happens, there is an "overshoot," and the smaller of the two may start the next part of its trajectory much smaller or only slightly smaller than the larger. One would like to predict the average relative magnitude of the overshoot, because this is what tells us how long s_n dwells in the same parity.

It is tempting to think that one could make a precise enough investigation of the trajectories of s_n and t_n to be able to say something about the behaviour of the map φ. This avenue may be no more promising than any other, but perhaps the map has some intrinsic interest.

By way of illustration, we give the first few iterations of s_n and t_n for $c = 2$. The table also shows odd prime factors, and a_n is the nth binary digit of $\sqrt{2}$.

n	s_n	factors of s_n	t_n	factors of t_n	a_n
0	1		2		1
1	4		1		0
2	7	7	4		1
3	7	7	16		1
4	28	7	17	17	0
5	23	23	68	17	1
6	92	23	89	89	0
7	7	7	356	89	1
8	28	7	697	17, 41	0
9	112	7	1337	7, 191	0
10	448	7	2449	31, 79	0
11	1792	7	4001	4001	0
12	7168	7	4417	7, 361	0
13	5503	5503	17668	7, 361	1
14	22012	5503	24329	24329	0
15	88048	5503	4633	41, 113	0
16	166831	7, 23833	18532	41, 113	1
17	296599	17, 23, 239	74128	41, 113	1
18	444943	31^2, 463	296512	41, 113	1
19	296863	7, 42409	1186048	41, 113	1
20	1187452	7, 42409	1778369	79, 22511	0

We also tabulate the first few iterations for $c = 3$; here a_n is the nth binary digit of $\sqrt{3}$.

n	s_n	factors of s_n	t_n	factors of t_n	a_n
0	2		1		1
1	3	3	4		1
2	12	3	1		0
3	23	23	4		1
4	39	3, 13	16		1
5	47	47	64		1
6	188	47	33	3, 11	0
7	311	311	132	3, 11	1
8	359	359	528	3, 11	1
9	1436	359	337	337	0
10	2199	3, 733	1348	337	1
11	1703	13, 131	5392	337	1
12	6812	13, 131	7377	3, 2459	0
13	27248	13, 131	1129	1129	0
14	52239	3, 11, 1583	4516	1129	1
15	95477	11, 8677	18064	1129	1
16	154767	3, 23, 2243	72256	1129	1
17	165023	59, 2797	289024	1129	1
18	660092	59, 2797	248001	3, 13, 6399	0
19	824183	824183	992004	3, 13, 6399	1
20	3296732	824183	335641	335641	0

5.6 Normality Criteria for kth Roots

The nth digit of $\sqrt[k]{c}$ in the base r is given by the residue class modulo r of A_n, where A_n^k is the largest integer kth power less than $r^{kn}c$.

This gives rise to normality criteria analogous to the criteria for square roots.

5.7 A General Integer Criterion for the Normality of Real Algebraic Irrationals

The approach we used for square and kth roots can be generalized.

Let α be a real algebraic irrational number, and let α_j be the conjugates of α, so

$$p(z) = \prod_{j=1}^{d} (z - \alpha_j)$$

is the minimal polynomial of α, with $\alpha = \alpha_i$ for some i. Then for any integer $b \neq 0$,

$$\prod_{j=1}^{d}(z - b\alpha_j)$$

is the minimal polynomial of $b\alpha$.

In particular, we can fix a base r and define the sequence of polynomials

$$p_n(z) = \prod_{j=1}^{d}(z - r^n\alpha_j).$$

Then for each n, p_n is the minimal polynomial of $r^n\alpha$.

If we write

$$p(z) = \sum_{j=0}^{d} a_j z^j \ , \ a_d = 1 \ , \ a_j \in \mathbb{Q},$$

then it is clear that

$$p_n(z) = \sum_{j=0}^{d} a_j r^{n(d-j)} z^j.$$

Now we assume, without loss of generality, that $\alpha > 0$, and let g be the number of real roots of $p(z)$. We index the real roots $\alpha_1, \ldots, \alpha_g$ of $p(z)$ from least to greatest, noting that $p(z)$ has no multiple root and that $\alpha = \alpha_i$ for some i.

Let δ be the least difference between two successive roots. Then for some N, $r^N\delta > 1$, and for every $n \geq N$ there is at least one integer between every successive pair of roots of $p_n(z)$. In fact the number of integers between each such pair of roots grows like r^n.

For $n \geq N$, the real roots of $p_n(z)$ partition the integers into $g + 1$ disjoint sets. We let $S_{n,1}$ be the set of integers less than $r^n\alpha_1$, $S_{n,j}$ be the set of integers between α_{j-1} and α_j for $1 < j \leq g$, and $S_{n,g+1}$ be the set of integers greater than α_g.

Then we define A_n to be the greatest element of the set $S_{n,i}$, so A_n is the greatest integer less than $r^n\alpha$.

In light of the last statement, our definition of A_n might seem needlessly cumbersome. It is motivated by the observation that the sign of $p_n(z)$ changes at each root, so the elements of each set $S_{n,j}$ have the same sign. For sufficiently large n, we note that A_n is the last integer before the ith sign change in the values of $p_n(a)$ as $a \in \mathbb{Z}$ increases.

From the first lemma, it follows that the residue of A_n mod r is the nth digit of α in the base r.

Theorem 17 *Let $\alpha > 0$ be a real algebraic irrational number, let the base r be fixed, and let p_n and A_n be defined as above for all n greater than some N. Then α is normal to the base r if and only if the sequence $\{A_n\}$ is normal* mod r.

Proof. The theorem follows from the first part of Theorem 15, the definition of a normal sequence modulo r, and the comment preceding the statement of the theorem. □

The sequence $\{A_n\}$ is uniquely dependent on the real irrational algebraic number α and the base r. The normality of the sequence $\{A_n\}$ modulo r is equivalent to the normality of α to the base r, and there is a long-standing hypothesis that every such α is normal to every base r. But these sequences $\{A_n\}$ suggest a more general hypothesis.

Hypothesis 1 *Given a real algebraic irrational number α, and an integer base $r > 1$, let the sequence of integers $\{A(\alpha, r)_n\}$ be the sequence $\{A_n\}$ as defined above. Then for every α and r, the sequence $\{A(\alpha, r)_n\}$ is a normal sequence modulo b for every integer base $b > 1$.*

Some natural questions arise about the sequences $\{A(\alpha, r)_n\}$. The residues of such a sequence modulo b can generate a number β written in the base b: we simply let the residue of $A(\alpha, r)_j$ modulo b be the j-th digit of β. By Hypothesis 1, we surmise that β is normal in the base b. But is β always an algebraic number? If not, what conditions are necessary for β to be algebraic?

If any such β failed to be algebraic, then we would have a new class of transcendental numbers generated directly from the digits of algebraic numbers.

Chapter 6

Lines of Inquiry

The great open question is the normality, or lack of normality, of all the well-known irrational constants. Borel has conjectured, for example, that all real algebraic irrational constants are normal to every base [12]. There is no reason to believe that numbers like π, e, and $\log 2$ are not normal (see [13] or [5].

There are a number of results about normality which may prove useful in future investigations.

Since the question of normality of α in the base r turns on the equidistribution of the sequence $\{r^j\alpha\}$, we give Weyl's criterion for equidistribution:

Theorem 18 *The sequence $\{a_j\}$ is uniformly distributed modulo 1 if*

$$\sum_{j=1}^{n} e^{2\pi i m a_j} = o(n)$$

for every positive integer m as $n \to \infty$.

Weyl proved this in 1916 [40] and went on to obtain the classic result that the number α is irrational if and only if the sequence $\{j\alpha\}$ is uniformly distributed modulo 1.

Wall [39] showed that if α is normal to the base r, then so are $\alpha + q$ and $q\alpha$ for any rational q.

Kuipers and Niederreiter [23] gave the following criterion for normality:

Theorem 19 *The number α is normal to the base r if there exists a constant C such that for any nonnegative continuous function f on $[0, 1]$,*

$$\limsup_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} f(r^j\alpha) \leq C \int_0^1 f(x)dx,$$

where $r^j\alpha$ is interpreted modulo 1.

In particular, $f(x)$ can be chosen arbitrarily close to the indicator function on a subinterval $[c, d]$ of $[0, 1]$, and this yields what Borwein and Bailey [13] call the "hot spot lemma:"

Corollary 20 *The number α is normal in the base r if and only if there exists a constant C such that for every subinterval $[c, d]$ of $[0, 1]$,*

$$\limsup_{n\to\infty} \frac{1}{n(d-c)} \sum_{j=0}^{n-1} \chi(r^j\alpha) \leq C,$$

where χ is the indicator function on $[c, d]$, and $r^j\alpha$ is interpreted modulo 1.

The remarkable effect of this corollary is that, for the sequence $\{r^j\alpha\}$, bounded density modulo 1 implies uniform density modulo 1.

Bailey and Rudolph and Bailey and Misiurewicz have posted "stronger" versions of the hot spot lemma, as yet unpublished.

Bailey and Crandall [5] made the following hypothesis:

Hypothesis 2 *Let $t_j = \dfrac{p(j)}{q(j)}$, where p and q are polynomials with integer coefficients, and $\deg p < \deg q$. Let $r \in \mathbb{Z}$ and $\alpha_0 = 1$. Then the recursively-defined sequence*

$$\alpha_j = r\alpha_{j-1} + t_j \pmod 1$$

either has a finite attractor or is uniformly distributed (mod 1).

Bailey and Crandall proved that this hypothesis, if true, would imply the normality of a wide variety of irrational constants with BBP expansions, including π, $\log 2$, and $\zeta(3)$, in the base 2.

One would like to prove that all real algebraic irrationals are normal; but this problem may be solved in stages, rather than all at once, for different classes of algebraic numbers. After examining the results to date, and wrestling with the properties of the sequence $\{r^j\alpha\}$, one is led to the heuristic impression that abnormal numbers are somehow too close to rational numbers. From this point of view, it may be that an easier proof of normality can be found for badly approximable numbers, in the sense of Meyer [30]. A number is *badly approximable* if the sequence $\{a_j\}$ in the continued fraction expansion

$$\alpha = [a_0, a_1, a_2, \ldots]$$

is bounded. This is equivalent to the existence of some $c > 0$ such that for any integer $q \geq 1$, the distance from $q\alpha$ to the nearest integer is at least c/q. (See, for example, Lang [26]).

According to Meyer, the only "naturally occurring" badly approximable real numbers are the quadratic irrationals. This suggests that it may be useful to look for a proof that the quadratic irrationals in particular, or the badly approximable reals in general, are normal.

Ironically, though, the technical difficulty of the problem seems to arise because the sequence $\{r^j\alpha\}$ diverges rapidly from any sequence $\{r^j a\}$ for a rational approximation a to

irrational α. The sequence for a badly approximable number diverges most rapidly of all, so it becomes difficult to say much about the behaviour of the sequence after relatively few iterations of the map $\alpha \mapsto r\alpha$.

One also wonders whether a direct examination of the digits produced by some square root algorithm could lead to a proof of normality, However, it is hard to see how this approach could improve very much on the Bailey, Borwein, Crandall and Pomerance result on the density of zeros in the expansion [3].

Allouche and Zamboni [2] showed that if the sequence of binary digits of a positive real number α is a fixed point of a morphism (primitive or of fixed length ≥ 2) on the alphabet $\{0, 1\}$, then α is rational or transcendental. This is one approach to the heuristic hypothesis that the digits of algebraic real irrationals are unpredictable. Adamczewski, Bugeaud, and Luca showed, along the same lines, that a finite automaton cannot generate the digits of an algebraic irrational [1].

In 1909, Borel introduced the concept of normality of numbers [11]. In 1950 [12], he presented a parting challenge. He observed that a number of phenomena in the digits of $\sqrt{2}$ were inconsistent with the hypothesis that $\sqrt{2}$ should be binomially normal (as defined in this thesis). Unfortunately, he applied no statistical tests to his observations, and other results have been consistent with the hypothesis of binomial normality [10]. But Borel's challenge is fresh today: " ... the problem of knowing whether or not the digits of a number like $\sqrt{2}$ satisfy **all** the laws one could state for randomly chosen digits, still seems ... to be one of the most outstanding questions facing mathematicians."

Bibliography

[1] Boris Adamczewski, Yann Bugeaud, and Florian Luca, *Sur la complexité des nombres algébriques*, C. R. Math. Acad. Sci. Paris **339** (2004), no. 1, 11–14 (French).

[2] Jean-Paul Allouche and Luca Q. Zamboni, *Algebraic irrational binary numbers cannot be fixed points of non-trivial constant length or primitive morphisms*, J. Number Theory **69** (1998), no. 1, 119–124.

[3] D. H. Bailey, J. M. Borwein, R. E. Crandall, and C. Pomerance, *On the Binary Expansions of Algebraic Numbers* (2003). http://crd.lbl.gov/ dhbailey/dhbpapers/algebraic.pdf.

[4] David Bailey, Peter Borwein, and Simon Plouffe, *On the rapid computation of various polylogarithmic constants*, Math. Comp. **66** (1997), no. 218, 903–913.

[5] David H. Bailey and Richard E. Crandall, *On the random character of fundamental constant expansions*, Experiment. Math. **10** (2001), no. 2, 175–190.

[6] ———, *Random generators and normal numbers*, Experiment. Math. **11** (2002), no. 4, 527–546 (2003).

[7] Lennart Berggren, Jonathan Borwein, and Peter Borwein, *Pi: a source book*, 3rd ed., Springer-Verlag, New York, 2004.

[8] A. S. Besicovitch, *The Asymptotic Distribution of the Numerals in the Decimal Representation of the Squares of the Natural Numbers*, Mathematische Zeitschrift **39** (1934), 146-156.

[9] F. Beukers, *On the generalized Ramanujan-Nagell equation. I*, Acta Arith. **38** (1980/81), no. 4, 389–410.MR621008 (83a:10028a)

[10] W. A. Beyer, N. Metropolis, and J. R. Neergaard, *Statistical study of digits of some square roots of integers in various bases*, Math. Comp. **24** (1970), 455–473.MR0272129 (42 #7010)

[11] Émile Borel, *Les probabilités dénombrables et leurs applications arithmétiques*, Supplemento ai rendiconti del Circolo Matematico di Palermo **27** (1909), 247-271.

[12] Émile Borel, *Sur les chiffres décimaux de $\sqrt{2}$ et divers problèmes de probabilités en chaîne*, C. R. Acad. Sci. Paris **230** (1950), 591–593 (French).MR0034544 (11,605d)

[13] Jonathan Borwein and David Bailey, *Mathematics by experiment*, A K Peters Ltd., Natick, MA, 2004. Plausible reasoning in the 21st century.MR2033012 (2005b:00012)

[14] J. W. S. Cassels, *On a paper of Niven and Zuckerman*, Pacific J. Math. **2** (1952), 555–557.MR0051271 (14,454c)

[15] ———, *On a problem of Steinhaus about normal numbers*, Colloq. Math. **7** (1959), 95–101.MR0113863 (22 #4694)

[16] D. G. Champernowne, *The construction of decimals normal in the scale of ten*, Journal of the London Mathematical Society **3** (1933), 254–260.

[17] A. H. Copeland and P. Erdös, *Note on Normal Numbers*, Bulletin of the American Mathematical Society **52(1)** (1946), 857-860.

[18] Karma Dajani and Cor Kraaikamp, *Ergodic theory of numbers*, Carus Mathematical Monographs, vol. 29, Mathematical Association of America, Washington, DC, 2002.

[19] H. Davenport and P. Erdös, *Note on normal decimals*, Canadian J. Math. **4** (1952), 58–63.

[20] H.A. Hanson, *Some Relations Between Various Types of Normality of Numbers*, Canadian Journal of Mathematics **6** (1954), 477-485.

[21] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., The Clarendon Press Oxford University Press, New York, 1979.

[22] Y. Kanada, *Vectorization of Multiple-Precision Arithmetic Program and 201,326,395 Decimal Digits of π Calculation*, Supercomputing 88 **II, Science and Applications** (1988).

[23] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience [John Wiley & Sons], New York, 1974. Pure and Applied Mathematics.

[24] H. Lebesgue, *Sur Certaines Démonstrations d'Existence*, Bulletin de la Société Mathématique de France **45** (1917), 132–144.

[25] A. N. Korobov, *Continued fractions of some normal numbers*, Mat. Zametki **47** (1990), no. 2, 28–33, 158 (Russian).

[26] Serge Lang, *Introduction to diophantine approximations*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1966.

[27] M. Levin, *On the Discrepancy Estimates of Normal Numbers*, Acta Arithmetica **88(2)** (1999), 99–111.

[28] Kurt Mahler, *Arithmetische Eigenschaften einer Klasse von Dezimalbrüchen*, Proc. Kon. Nederlandsche Akad. v. Wetenschappen **40)** (1937), 421–428.

[29] Greg Martin, *Absolutely abnormal numbers*, Amer. Math. Monthly **108** (2001), no. 8, 746–754.

[30] Yves Meyer, *Algebraic numbers and harmonic analysis*, North-Holland Publishing Co., Amsterdam, 1972. North-Holland Mathematical Library, Vol. 2.

[31] Ivan Niven, *Irrational numbers*, The Carus Mathematical Monographs, No. 11, The Mathematical Association of America. Distributed by John Wiley and Sons, Inc., New York, N.Y., 1956.

[32] Ivan Niven and H. S. Zuckerman, *On the definition of normal numbers*, Pacific Journal of Mathematics **1** (1951), 103-109.

[33] Frédéric Riesz, *Sur la théorie ergodique*, Comment. Math. Helv. **17** (1945), 221–239 (French).

[34] Tibor Šalát, *A remark on normal numbers*, Rev. Roumaine Math. Pures Appl. **11** (1966), 53–56.

[35] Wolfgang M. Schmidt, *Über die Normalität von Zahlen zu verschiedenen Basen*, Acta Arith. **7** (1961/1962), 299–309 (German).

[36] W. Sierpiński, *Démonstration Élémentaire du Théorème de M. Borel sur les Nombres Absolument Normaux et Déteermination Effective d'un Tel Nombre*, Bulletin de la Société Mathématique de France **45** (1917), 125–132.

[37] R. G. Stoneham, *On absolute (j, ε)-normality in the rational fractions with applications to normal numbers*, Acta Arith. **22** (1972/73), 277–286.

[38] ———, *A general arithmetic construction of transcendental non-Liouville normal numbers from rational fractions*, Acta Arith. **16** (1969/1970), 239–253.

[39] D. D. Wall, *Normal Numbers*, Berkeley, 1949. Ph.D. thesis.

[40] Hermann Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Mathematische Annalen **77** (1916), 313-352.

[41] E.W. Weisstein, *Wolfram's Iteration*, Mathworld (2005). http://mathworld.wolfram.com/WolframsIteration.html.