Equidistribution Mod 1 And Normal Numbers

N. A. Carella

Abstract: Let $\alpha = 0.a_1a_2a_3 \ldots$ be an irrational number in base $b > 1$, where $0 \leq a_i < b$. The number $\alpha \in (0,1)$ is a normal number if every block $(a_{n+1}a_{n+2} \ldots a_{n+k})$ of $k$ digits occurs with probability $1/b^k$. A proof of the normality of the real number $\sqrt{2}$ in base 10 is presented in this note. Three different proofs based on different methods are given: a conditional proof, and two unconditional proofs.

Contents

1 Introduction To Normal Numbers 2
2 Notation 3
3 Lacunary and Nonlacunary Sequences 3
4 Dense Sets 4
5 Results for Pisot and Salem Numbers 5
6 Equidistribution Criteria 7
7 Equidistribution Criteria for Normal Numbers 8
8 Equidistribution Criteria for Double Sequences 8
9 Equidistribution Criteria for Multivariable Polynomials 8
10 Rational Prime Approximations 9
11 Random Rational Approximations 9
12 Multiplicative Subgroups And Exponential Sums 12
13 Large Multiplicative Orders Modulo $n$ 13
14 Estimates For Exponential Sums 14
15 Properties of the Exponential Function 14
16 Exponential Sums and Liouville Numbers 15
17 Conditional Proof For The Normality Of $\sqrt{2}$ 16

January 26, 2023

AMS MSC2020: Primary 11K16; Secondary 11J72

Keywords: Irrational number; Normal number; Uniform distribution; Borel problem.
18 Conditional Proof For The Normality Of Pi

19 Results for Multiplicative Nonlacunary Sequences

20 Unconditional Proof For The Normality Of $\sqrt{2}$

21 Problems

1 Introduction To Normal Numbers

Let $\alpha = 0.a_1a_2a_3\ldots$ be an irrational number in base $b > 1$, where $0 \leq a_i < b$. The theory of normal numbers is centered on the distribution of the blocks $(a_{n+1}a_{n+2}\ldots a_{n+k})$ of $k$ digits in the $b$-adic expansions of the real numbers. The earliest study of normal numbers is known as the Borel conjecture. This problem investigates the distribution of the blocks of digits in the decimal expansion of the number $\sqrt{2} = 1.414213562373\ldots$.

Definition 1.1. An irrational number $\alpha \in \mathbb{R}$ is a normal number in base $b > 1$ if any sequence of $k$-digits in the $b$-adic expansion occurs with probability $1/b^k$. Further, the number is called absolutely normal if it is a normal number in every base.

A normal number in any base is an irrational number, but an irrational number is not necessarily normal. The simplest, and best known construction technique of normal numbers is the integers concatenation method. In base $b = 10$, the best known examples are the followings numbers. The concatenation of the consecutive integers:

$$C_0 = \sum_{n \geq 1} \frac{n}{10^{a_0(n)}} = 0.12345678910111213151617181920\ldots,$$

where $a_0(n) = n + \sum_{1 \leq k \leq \left\lfloor \log_{10} k \right\rfloor}$. The concatenation of the consecutive primes:

$$C_1 = \sum_{n \geq 1} \frac{p_n}{10^{a_1(n)}} = 0.235711131719232931374143475359\ldots,$$

where $a_1(n) = n + \sum_{1 \leq k \leq n\left\lfloor \log_{10} p_k \right\rfloor}$, and $p_n$ is the $n$th prime in increasing order. The concatenation of the consecutive squares:

$$C_2 = \sum_{n \geq 1} \frac{n^2}{10^{a_2(n)}} = 0.149162536496481100121144169196\ldots,$$

where $a_2(n) = n + \sum_{1 \leq k \leq n\left\lfloor \log_{10} k^2 \right\rfloor}$, and many other similar numbers. The integers concatenation method generalizes to any base $b > 1$, and to certain infinite sequences of integers. The basic proofs are provided in [9], [10, Theorem 1], et alii. Another class of normal numbers is defined by series of the forms

$$C_{b,c}(s) = \sum_{n \geq 1} \frac{1}{cn^{b^s+s}},$$

where $\gcd(b,c) = 1$, and $s \in \mathbb{R}$, see [26], [4], et alii. More complex constructions and algorithms for generating normal numbers are developed in [2], [8], et alii. However, there are no known normal numbers in closed forms such as $\sqrt{2}$, $e$, $\pi$, $\log 2$, $\gamma$, ..., et cetera in any base $b \geq 2$. This note contributes the followings conditional results using two different methods.
Theorem 1.1. The irrational number $\sqrt{2} \in \mathbb{R}$ is a normal number in base $p \geq 2$. In particular, $\sqrt{2}$ is simply normal number in base $10$. Hence, the decimal expansion

$$\sqrt{2} = 1.4142135623730950488016887242096980785696718753769480731766797379\ldots$$

contains infinitely many digit 0, infinitely many digit 1, infinitely many digit 2, et cetera.

Theorem 1.2. Assume the GRH. Then, the irrational number $\pi \in \mathbb{R}$ is a normal number in base 10.

The preliminary foundational results required to prove these results are covered in Section 11 to Section 12. The proofs are presented in chronological order as discovered. The conditional proof of the normality of $\sqrt{2}$ in base 10, Theorem 1.1, is exhibited in Section 17, and the conditional proof of the normality of $\pi$ in base 10, Theorem 1.2, is exhibited in Section 18. The first unconditional proof of the normality of $\sqrt{2}$ in base $p \geq 2$ is a corollary of Theorem 19.1 in Section 19 and the second unconditional proof of the normality of $\sqrt{2}$ in base $p \geq 2$ is a corollary Theorem 19.1 in Section 19.

Surveys of some of the literature on normal numbers appear in [17], et alii. A survey of some of the literature on the number $\pi$ appears in [7], and its irrationality is proved in [23, Corollary 2.6].

2 Notation

The sets $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ and $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ are the set of nonnegative integers and the set of integers. The symbols $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the sets of rational numbers, the set of real numbers, and the set of complex numbers respectively.

Let $f, g : [x_0, \infty) \to \mathbb{R}$ be a pair of functions, and assume $g(x) > 0$. The little $o$ notation is defined by

$$f(x) = o(g(x)) \iff |f(x)| \leq cg(x) \quad (2.1)$$

for any constant $c > 0$ as $x \to \infty$. The negation of the little $o$ notation is defined by

$$f(x) \neq o(g(x)) \iff f(x) = \Omega_{\pm}(g(x)). \quad (2.2)$$

This has the explicit form

$$f(x) = \Omega_{\pm}(g(x)) \iff |f(x)| \geq cg(x). \quad (2.3)$$

for some constant $c > 0$ as $x \to \infty$. The big $O$ notation is defined by

$$f(x) = O(g(x)) \iff |f(x)| \leq cg(x) \quad (2.4)$$

for some constant $c > 0$ as $x \to \infty$.

3 Lacunary and Nonlacunary Sequences

A lacunary sequence is a sparse or thin sequence of integers. A few of the properties of lacunary sequences are recorded in this section.

Definition 3.1. A pair of integers $p > 1$ and $q > 1$ are multiplicative independent over the integers if $p^a \neq q^b$ for all nonzero integers $a, b \in \mathbb{Z}^\times$. 

**Definition 3.2.** Let \( \mathcal{U} \subset \mathbb{N} \) be a subset of integers. The subset is **lacunary** if and only if it is generated by a sequence of powers \( \mathcal{U} = \{u^n : n \geq 0\} \), where \( u > 1 \) is an integer. In particular,
\[
\lim_{n \to \infty} \frac{u_{n+1}}{u_n} > 1.
\]
Otherwise, it is **nonlacunary** and it is generated by two or more powers.

The basic nonlacunary sequences can be classified into two different forms: additive and multiplicative.

**Definition 3.3.** An **additive nonlacunary sequence** is of the form
\[
\mathcal{U} = \{u_{m,n} = p^{n_1}q_1 + p^{n_2}q_2 + \cdots + p^{n_d}q_d : m, n \geq 1\},
\]
and a **multiplicative nonlacunary sequence** is of the form
\[
\mathcal{V} = \{v_{m,n} = p_1^{n_1}q_1 p_2^{n_2}q_2 \cdots p_d^{n_d}q_d : m, n \geq 1\},
\]
where the generators \( p_i \) and \( q_i \) are multiplicative independent integers, and \( d \geq 1 \) is fixed dimension.

The analytic method for determining the whether or not a semigroup is lacunary has a simple form.

**Lemma 3.1.** A semigroup \( \mathcal{L} = \{u_n : n \geq 1\} \subset \mathbb{N} \) is lacunary if and only if
\[
\lim_{n \to \infty} \frac{u_{n+1}}{u_n} > 1.
\]

**Example 3.1.** Consider the generators \( u = 2 \) and \( v = 3 \). Then
1. \( \mathcal{L} = \{2^n : n \geq 0\} \subset \mathbb{N} \), is a lacunary semigroup.
2. \( \mathcal{M} = \{2^m3^n : m, n \geq 0\} \subset \mathbb{N} \), is a nonlacunary semigroup.

**Example 3.2.** The simple limit test classifies of the followings subsets of integers.
1. \( \mathcal{M} = \{u_n = n^7 : n \geq 0\} \subset \mathbb{N} \), is a nonlacunary semigroup.
2. \( \mathcal{P} = \{u_n = p^9 : p \geq 2\} \subset \mathbb{N} \), with \( p \) prime, is a nonlacunary semigroup.

**4 Dense Sets**

Several techniques for generating dense sets of real numbers are described in this section.

**Theorem 4.1.** ([13, Theorem IV.1]) If \( \mathcal{M} \subset \mathbb{N} \) is a nonlacunary semigroup of integers, and \( \alpha \) irrational number, then, the subset of real numbers \( \{\alpha n : n \in \mathcal{M}\} \) is dense in the torus. In particular, the closure
\[
\overline{\{\alpha n : n \in \mathcal{M}\}} = \mathbb{R}/\mathbb{Z}.
\]

**Example 4.1.** For a pair of multiplicative independent integers \( p \) and \( q \), and an irrational number \( \alpha \), the double sequence of real numbers \( \{\beta_{m,n} = p^m q^n \alpha : m, n \geq 1\} \) is dense in the torus \( T = \mathbb{R}/\mathbb{Z} \).
A few generalizations of this result have been established in the literature. One of these results is stated here.

**Theorem 4.2.** ([16, Theorem 1.2]) Let \( p_i, q_i \in \mathbb{N} \) with \( 1 < p_i < q_i \) for \( i = 1, \ldots, d \) and assume that \( p_1 \leq p_2 \leq \cdots \leq p_k \). Assume that the pairs \( p_i, q_i \) are multiplicative independent for \( i = 1, \ldots, d \). Then for distinct \( \alpha_1, \ldots, \alpha_d \in \mathbb{T} \) with at least one \( \alpha_i \notin \mathbb{Q} \), the subset of real numbers
\[
A = \{ \beta_{m,n} = p_1^n q_1^m \alpha_1 + p_2^n q_2^m \alpha_2 + \cdots + p_d^n q_d^m \alpha_d : m, n \geq 1 \}
\]
is dense in the torus \( \mathbb{T} = \mathbb{R}/\mathbb{Z} \). In particular, the closure
\[
\{ \alpha \in A \} = \mathbb{T}.
\]

A result linking the space of countable dense sets to the space of equidistributed sequences will be required to complete the proof of the main result.

**Lemma 4.1.** Let \( \mathcal{D} \subset [0,1] \) be a countable subset of real numbers. Then, the following statements are equivalent.

(i) The countable set \( \mathcal{D} = \{ x_1, x_2, \ldots \} \) is dense in \( [0,1] \).

(ii) There exists a permutation \( \sigma : \mathcal{D} \to \{ y_1, y_2, \ldots \} \) of the countable set \( \mathcal{D} \) such that the sequence \( \{ y_n = \sigma(x_n) : n \geq 1 \} \) is equidistributed in \( [0,1] \).

## 5 Results for Pisot and Salem Numbers

A distinguished collection of algebraic numbers is defined below. The recent papers, [25], [5] et alii, introduce some of the properties of these numbers.

**Definition 5.1.** Let \( \theta \neq 0 \) be a root of an irreducible polynomial \( f(z) \in \mathbb{Z}[z] \) of degree \( \deg f = d \geq 2 \). Then,

1. The real number \( \theta > 1 \) is called a **Pisot number** if the conjugates roots have absolute value \( |\theta_i| < 1 \) for \( i = 1, 2, 3, \ldots, d - 1 \).

2. The real number \( \theta > 1 \) is called a **Salem number** if the conjugates roots have absolute value \( |\theta_i| \leq 1 \), and at least one has \( |\theta_j| = 1 \) for \( i = 1, 2, 3, \ldots, d - 1 \).

**Lemma 5.1.** The sequence powers \( \{ \theta^n : n \geq 1 \} \) of a Pisot number is approximates a subsequence of integers exponentially fast.

**Proof.** By the Newton identity, a sum of conjugate algebraic integers
\[
\theta^n + \theta_1^n + \theta_2^n + \cdots + \theta_{d-1}^n
\]
is an integer for any integer \( n \geq 1 \). By the definition of a Pisot number \( |\theta_i| < 1 \), and \( |\theta| > 1 \). Therefore, the rearrange sum
\[
\theta^n = -\theta_1^n - \theta_2^n - \cdots - \theta_{d-1}^n
\]
converges to an integer at exponential rate as \( n \to \infty \). ■
Example 5.1. The first Pisot number seems to be the real root
\[ \theta = \sqrt[3]{\left(\frac{9 + \sqrt{69}}{18}\right)} + \sqrt[3]{\left(\frac{9 - \sqrt{69}}{18}\right)} = 1.324717957244746 \ldots \]
of the polynomial \( x^3 - x - 1 \). The sum of the remaining conjugate roots is
\[ \theta_1 + \theta_2 = 2r \cos 2\pi \omega, \]
where \( r < 1 \) and \( \omega \in (0, 1) \), see Figure 5.1 below.

The corresponding sequence
\[ x_n = \theta^n + \theta_1^n + \theta_2^n \]
is exponentially close to a subsequence of integers as \( n \to \infty \).

Example 5.2. The first Salem number seems to be the real root
\[ \theta = 1.266361236713076 \ldots \]
of the Lehmer polynomial \( x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1 \). The sum of the conjugate roots is
\[ \theta + \theta_1 + \theta_2 + \cdots + \theta_8 + \theta_9 = \theta + \theta_1 + 2r_1 \cos 2\pi \omega_1 + \cdots + 2r_4 \cos 2\pi \omega_4, \]
where \( \theta_1 = \theta^{-1} < 1 \), \( |\theta_i| = r_i \leq 1 \) and \( \omega_i \in (0, 1) \) for \( i \in \{2, 3, \ldots, 9\} \). The first pair of conjugate roots \( \theta_2 + \theta_3 = 2r_1 \cos \omega_1 \), and so on.

The corresponding sequence
\[ x_n = \theta^n + \theta_1^n + \theta_2^n + \cdots + \theta_8^n + \theta_9^n \]
\[ = \theta^n + \theta_1^n + r_1^n \cos \omega_1 n + \cdots + r_4^n \cos \omega_4 n, \]
where at least one \( r_i = 1 \), is exponentially close to a subsequence of integers as \( n \to \infty \).

Theorem 5.1. If \( \theta > 1 \) is a Salem number of degree \( d = 2m \geq 2 \), then sequence powers
\[ \theta^n + \theta^{-n} = -\theta_2^n - \cdots - \theta_{d-2}^n - \theta_{d-1}^n \]
\[ = -2 \cos 2\pi \omega_1 n - \cdots - 2 \cos 2\pi \omega_{m-1} n, \]
where \( \omega_i \in (0, 1) \), is dense, but not equidistributed on the unit interval \( (0, 1) \).
**Proof.** Under this condition all the complex roots \( \theta_2, \theta_3, \ldots, \theta_{2d-1} \) are on the unit circle, and the two real roots are \( \theta > 1 \) and \( \theta_1 = \theta^{-1} < 1 \). A proof that the sequence is not equidistributed is derived from the relation

\[
e^{i2\pi k(\theta^n + \theta^{-n})} = e^{-i2\pi k(\theta_2^2 + \cdots + \theta_{2d-1}^2)} = e^{-i2\pi k(2 \cos 2\pi \omega_1 n + \cdots + 2 \cos 2\pi \omega_{m-1} n)},
\]

and the Bessel function identity

\[
J_0(-4\pi k) = \int_0^1 e^{-i4\pi k \cos 2\pi \omega(t)} dt. \tag{5.3}
\]

A complete and short proof is given in [24].

Recent refinements of this results are available in the literature, see [3], [12].

### 6 Equidistribution Criteria

The standard Weyl criterion claims that (6.1) is true for all integer parameter \( k \neq 0 \), see [19, Theorem 2.1]. This result is extended to all rational parameter \( k = r \neq 0 \).

**Theorem 6.1.** (Extended Weyl Criterion) The sequence of real number \( \{u_n : n \geq 1\} \) is uniformly distributed modulo 1 if and only if

\[
\lim_{x \to \infty} \frac{1}{x} \sum_{n \leq x} e^{i2\pi ku_n} = 0 \tag{6.1}
\]

for any fixed rational number \( k \neq 0 \).

**Proof.** Without loss in generality assume \( \{u_n = \alpha n : n \geq 1\} \), where \( \alpha \neq 0 \) is an irrational number. Summing the exponential sum yields

\[
\left| \sum_{n \leq x} e^{i2\pi \alpha n} \right| = \left| \frac{e^{i2\pi \alpha (x+1)} - 1}{e^{i2\pi \alpha} - 1} \right| \leq \frac{1}{|\sin(\pi \alpha)|}. \tag{6.2}
\]

Since \( \alpha \neq 0 \) is an irrational number, the product representation of the sine function shows that

\[
\sin(\pi \alpha) = \pi \alpha \prod_{n \geq 1} \left( 1 - \frac{k^2 \alpha^2}{n^2} \right) \neq 0
\]

for any fixed rational number \( k \neq 0 \), the last inequality (6.2) is bounded by a constant.

**Theorem 6.2.** ([18]) For any real number \( \alpha \neq 0 \), and almost all irrational \( \theta \in \mathbb{R}^\times \), the sequence \( \{\alpha \theta^n : n \geq 1\} \) is equidistributed modulo 1.

The best known exceptions to this theorem are documented in Theorem 5.1.
7 Equidistribution Criteria for Normal Numbers

**Theorem 7.1.** (Wall) An irrational number \( \alpha \in \mathbb{R} \) is a normal number in base \( p \geq 2 \) if and only if the sequence \( \{\alpha p^n : n \geq 1\} \) is uniformly distributed modulo 1.

The proof of this criterion appears in [23, Theorem 8.15].

**Theorem 7.2.** Given real number \( \alpha \in \mathbb{R}^\times \), the following statements are valid.

(i) If \( \alpha \) is irrational, then \( r\alpha + s \) is irrational for all rational scale \( r, s \in \mathbb{Q}^\times \).

(ii) If \( \alpha \) is normal in base \( b \), then \( r\alpha + s \) is normal in base \( b \) for all rational scale \( r, s \in \mathbb{Q}^\times \).

**Proof.** (ii) This follows from the Wall criterion, Theorem 7.1. \( \square \)

8 Equidistribution Criteria for Double Sequences

There are several criteria for the equidistribution of double sequences. The criterion stated in Theorem 8.1, and the well known Furstenberg criterion, see Theorem 8.10, are used in proof of the main result. Basically, these are extensions of the Weyl criterion in Theorem 6.1 and or Wall criterion in Theorem 7.1.

**Theorem 8.1.** ([19, Theorem 2.9]) The double sequence of real numbers \( \{\beta_{m,n} : m, n \geq 1\} \) is uniformly distributed modulo 1 if and only if

\[
\lim_{x,y \to \infty} \frac{1}{xy} \sum_{m \leq x, n \leq x} e^{i2\pi k\beta_{m,n}} = 0
\]

for all integers \( k \neq 0 \).

9 Equidistribution Criteria for Multivariable Polynomials

The equidistribution criteria for the sequences of real numbers \( \{x_{n_1,...,n_d} = f(n_1,\ldots,n_d)\alpha : n_i \geq 1\} \) generated by multivariable polynomials \( f(t_1,\ldots,t_d) \in \mathbb{Z}[t_1,\ldots,t_d] \) are similar to the criteria for polynomial of a single variable.

**Theorem 9.1.** Let \( \alpha \) be an irrational number, and let \( f(t_1,\ldots,t_d) \) be a monotonically increasing polynomial over the integers. Then, the sequence of real numbers \( \{f(t_1,\ldots,t_d)\alpha : n_i \geq 1\} \) is uniformly distributed modulo 1.

**Proof.** The proof for the simplest case of additive multivariable polynomial \( f(t_1,t_2) = t_1^a + t_2^b \), where \( a \geq 1 \) and \( b \geq 1 \), is provided here. Consider the sequence of real numbers

\[
\{\beta_{m,n} = (m^a + n^b)\alpha : m, n \geq 1\}.
\]

An application of Theorem 8.1 yields

\[
\frac{1}{x^2} \sum_{m \leq x, n \leq x} e^{i2\pi k\beta_{m,n}} = \frac{1}{x^2} \sum_{m \leq x, n \leq x} e^{i2\pi k(m^a+n^b)\alpha} = o(1)
\]

for any parameter \( k \neq 0 \).
Rearranging the exponential sum as a product yields the decomposition

\[
\frac{1}{x^2} \sum_{m \leq x, n \leq x} e^{i 2\pi k (m^a + n^b) \alpha} = \left( \frac{1}{x} \sum_{m \leq x} e^{i 2\pi km^a \alpha} \right) \times \left( \frac{1}{x} \sum_{n \leq x} e^{i 2\pi kn^b \alpha} \right) = o(1). \tag{9.3}
\]

Clearly, these exponential sums satisfy the conditions

\[
\frac{1}{x} \sum_{m \leq x} e^{i 2\pi km^a \alpha} = o(1) \quad \text{and} \quad \frac{1}{x} \sum_{n \leq x} e^{i 2\pi kn^b \alpha} = o(1). \tag{9.4}
\]

Therefore, the sequence of real numbers \((9.1)\) is equidistributed modulo 1. The general case for any multivariable polynomial is similar.

**Example 9.1.** The following sequences of real numbers are equidistributed modulo 1.

1. For any irrational \(\alpha\), the subset of real numbers \(M = \{v_{m,n} = (m^2 + n^3)\alpha : m, n \geq 0\}\).

2. For any irrational \(\alpha\), the subset of real numbers \(M = \{v_{m,n} = (m^4 + n^5 + m^9 + n^3)\alpha : m, n \geq 0\}\).

### 10 Rational Prime Approximations

The quantity \(\|x\| = \min_{n \in \mathbb{Z}} \{|x - n|\} \geq 0\) defines the least distance to an integer. Using this notation, the rational number approximation \(|q\alpha - m| < q^{-1}\) can be written in the form \(\|q\alpha\| < q^{-1}\), where \(q \geq 1\) is an integer. The rational prime approximations is a refinement to primes denominators \(q = p\).

**Theorem 10.1.** ([22, Theorem 1]) Let \(\varepsilon > 0\) and \(\tau = 1/3 - \varepsilon\). Then, there exist infinitely many primes \(p\) such that

\[
\|p\alpha\| < p^{-1/3 + \varepsilon}. \tag{10.1}
\]

For applications to normal numbers, an additional property is essential.

**Conjecture 10.1.** Let \(\varepsilon > 0\) and \(\tau = 1/3 - \varepsilon\). Then, there exist infinitely many primes \(p\) such that

\[
\|p\alpha\| < p^{-1/3 + \varepsilon}, \tag{10.2}
\]

and the integer 10 has a large multiplicative order \(\text{ord}_p 10 \gg p^\delta\), where \(\delta > 0\) is a small number.

### 11 Random Rational Approximations

The one-to-one correspondence between the fractional parts of the sequence \(x_n = n \log 10 + \log \pi\) and \(y_n = \pi 10^n\), where \(n \geq 1\), via the map \(x_n \mapsto y_n = e^{\pi n}\) clues to the uniform
distribution of both sequences. To explicate the relationship between all the sequences and fractional parts consider the sets

\[
X = \{ x_n = n \log 10 + \log \pi : n \geq 1 \}, \\
Y = \{ y_n = \pi 10^n : n \geq 1 \}, \\
U = \{ \{ x_n \} : n \geq 1 \}, \\
V = \{ \{ y_n \} : n \geq 1 \},
\]

and the correspondence diagram.

\[
\begin{array}{ccc}
X & \xrightarrow{e^{x_n}} & Y \\
\rho & \downarrow & \rho \\
U & \xrightarrow{e^{x_n}} & V
\end{array}
\]

The class function \( \rho : \mathbb{R} \rightarrow [0, 1] \), refer to the above diagram, assigns the fractional parts \( \rho(x_n) = \{ x_n \} \) and \( \rho(y_n) = \{ y_n \} \) of the corresponding sequences \( x_n = n \log 10 + \log \pi \) and \( y_n = e^{x_n} = \pi 10^n \), respectively, where \( n \geq 1 \).

The equidistribution of the sequence \( x_n \) is established in the Lemma below.

**Lemma 11.1.** The sequence of real number \( x_n = n \log 10 + \log \pi \), where \( n \geq 1 \), is uniformly distributed modulo 1.

**Proof.** A routine application of Theorem 6.1, see also [19, Theorem 2.1].

The conditional proof of the equidistribution of the sequence \( y_n = e^{x_n} = \pi 10^n \) is significantly longer. Some of the required foundational results are established here.

The result below shows that for each integer \( n \geq 1 \), the fractional part \( \{ \pi 10^n \} \) is contained in some random subinterval of the form

\[
\left[ \frac{r_n}{q_k} + \frac{1}{q_k^{\mu-1}}, \frac{s_n}{q_k} + \frac{c_n}{q_k^2} \right] \subseteq [0, 1],
\]

where \( 0 \leq r_n, s_n, c_n \leq q_k \). In this application, the lower bound \( \mu(\pi) \geq 2 \) of the irrationality measure of the real number \( \pi \) is sufficient, see [29, p. 556] for the definition of this quantity.

**Lemma 11.2.** If \( p_k/q_k \) is the \( k \)th convergent of the real number \( \pi \), then, for each \( n \leq q_k \), the fractional part \( \{ \pi 10^n \} \) of the real number \( \pi 10^n \) satisfies one or both of the following inequalities.

(i) \( \frac{r_n}{q_k} + \frac{10^n}{2q_k^\mu} \leq \{ \pi 10^n \} \leq \frac{r_n + 1}{q_k}, \) if \( 10^n \leq q_k \),

(ii) \( \frac{r_n}{q_k} + \frac{1}{q_k^{\mu-1}} \leq \{ \pi 10^n \} \leq \frac{s_n}{q_k} + \frac{c_n}{q_k^2}, \) if \( 10^n > q_k \),

where \( \mu = \mu(\pi) \geq 2 \) is the irrationality measure of \( \pi \), and \( 0 \leq c_n, r_n, s_n < q_k \).
Proof. The verification is split into two cases, depending on the magnitude of the integer $10^n$.

**Case I.** Observe that for all sufficiently large $q_k$, and any integer $10^n \leq q_k$, there is the rational approximation inequality
\[
\frac{1}{2q_k^2} \leq 1 - \frac{p_k}{q_k} \leq \frac{1}{2q_k^2},
\] (11.3)
for any even index $k \geq 1$, see [15, Theorem 163]. This leads to the new inequality
\[
\frac{10^n}{2q_k^2} \leq \pi 10^n - \frac{10^n p_k}{q_k} \leq \frac{1}{2q_k^2}.
\] (11.4)
Now, replace $10^n p_k = a_n q_k + r_n$ to get the equivalent expression
\[
\frac{10^n}{2q_k^2} \leq \pi 10^n - a_n - \frac{r_n}{q_k} \leq \frac{1}{2q_k^2}.
\] (11.5)
Clearly, this implies that the fraction part satisfies
\[
\frac{r_n}{q_k} + \frac{10^n}{2q_k^2} \leq \{\pi 10^n\} \leq \frac{r_n}{q_k} + \frac{1}{q_k},
\] (11.6)

**Case II.** For all sufficiently large $q_k$, and any integer $10^n > q_k$, there is the rational approximation inequality
\[
\frac{1}{q_k^2} \leq 1 - \frac{p_k}{q_k} \leq \frac{1}{q_k^2},
\] (11.7)
for any even index $k \geq 1$, see [15, Theorem 163]. Here, the quantity $\mu = \mu(\pi) \geq 2$ is the irrationality measure of $\pi$, see [29, p. 556]. This leads to the new inequality
\[
\frac{1}{10^n q_k^{\mu-1}} \leq 1 - \frac{p_k}{q_k} \leq \frac{1}{q_k^2}.
\] (11.8)
Equivalently, this is
\[
\frac{1}{q_k^{\mu-1}} \leq 1 - \frac{p_k}{q_k} \leq \frac{10^n}{q_k^2}.
\] (11.9)
Now, rearrange it as
\[
\frac{p_k 10^n}{q_k} + \frac{1}{q_k^{\mu-1}} \leq \pi 10^n \leq \left(\frac{p_k q_k + 1}{q_k^2}\right) 10^n,
\] (11.10)
and replace $p_k 10^n = a_n q_k + r_n$ and $(p_k q_k + 1) 10^n = b_n q_k^2 + s_n q_k + c_n$ to get the equivalent expression
\[
\frac{a_n + r_n}{q_k} + \frac{1}{q_k^{\mu-1}} \leq \pi 10^n \leq \frac{s_n}{q_k} + \frac{c_n}{q_k^2},
\] (11.11)
where $0 \leq a_n, b_n, c_n, r_n, s_n < q_k$. This implies that the fraction part satisfies
\[
\frac{r_n}{q_k} + \frac{1}{q_k^{\mu-1}} \leq \{\pi 10^n\} \leq \frac{s_n}{q_k} + \frac{c_n}{q_k^2},
\] (11.12)
as claimed. ■
Lemma 11.3. Let \( p_k/q_k \) be the \( k \)th convergent of the real number \( \pi \), and let \( q = q_k + o(q_k) \) be a large prime. Then, for each \( n \leq q \), the fractional part \( \{\pi 10^n\} \) of the real number \( \pi 10^n \) satisfies one or both of the following inequalities for infinitely many primes \( q \).

\[
(i) \quad \frac{r_n}{2q} + O\left(\frac{1}{q^2}\right) \leq \{\pi 10^n\} \leq \frac{r_n+1}{q} + O\left(\frac{1}{q^2}\right), \quad \text{if } 10^n \leq q_k,
\]

\[
(ii) \quad \frac{r_n}{2q} + \frac{1}{(2q)^{\mu-1}} + O\left(\frac{1}{q^2}\right) \leq \{\pi 10^n\} \leq \frac{s_n}{q} + O\left(\frac{1}{q^2}\right), \quad \text{if } 10^n > q_k,
\]

where \( \mu = \mu(\pi) \geq 2 \) is the irrationality measure of \( \pi \), and \( 0 \leq c_n, r_n, s_n < q \).

Proof. For a large integer \( q_k \geq 2 \), and a large prime \( q = q_k + o(q_k) \), the inequalities

\[
\frac{1}{2q} + O\left(\frac{1}{q^2}\right) \leq \{\pi\} \leq \frac{1}{q} + O\left(\frac{1}{q^2}\right)
\]

are valid.

Case I. Replacing (11.13) into (11.6) yields

\[
\frac{r_n}{2q} + O\left(\frac{1}{q^2}\right) \leq \{\pi 10^n\} \leq \frac{r_n+1}{q} + O\left(\frac{1}{q^2}\right)
\]

for any even index \( k \geq 1 \), and all sufficiently large \( q = q_k + o(q_k) \).

Case II. Replacing (11.13) into (11.12) yields

\[
\frac{r_n}{2q} + \frac{1}{(2q)^{\mu-1}} + O\left(\frac{1}{q^2}\right) \leq \{\pi 10^n\} \leq \frac{s_n}{q} + O\left(\frac{1}{q^2}\right),
\]

for any even index \( k \geq 1 \), see [15, Theorem 163], and the irrationality measure \( \mu = \mu(\pi) \geq 2 \) of \( \pi \), see [29, p. 556] for additional information.

12 Multiplicative Subgroups And Exponential Sums

The cardinality of a subset of integers \( H \subset \mathbb{Z} \) is denoted by \( \#H \geq 0 \). The multiplicative order of an element \( r \neq 0 \) in a finite ring \( (\mathbb{Z}/m\mathbb{Z})^\times \) is defined by \( \nu_r = \min\{n \geq 1 : r^n \equiv 1 \mod m\} \), where \( m \geq 1 \) is an integer. The multiplicative order is a divisor \( n \mid \nu_r \) of the totient function \( \nu_r \) of the finite ring \( (\mathbb{Z}/m\mathbb{Z})^\times \), see [1, Theorem 2.4].

Lemma 12.1. Let \( \{p_k/q_k : k \geq 1\} \) be the sequence of convergents of the real number \( \pi \). Assume that \( \gcd(10, q_k) = 1 \). Then,

(i) \( G = \{p_k10^n \equiv r_n \mod q_k : n \geq 1\} \) is a large multiplicative subgroup of the finite ring \( (\mathbb{Z}/q_k\mathbb{Z})^\times \).

(ii) \( H = \{(p_kq_k + 1)10^n \equiv s_n \mod q_k : n \geq 1\} \) is a large multiplicative subgroup of the finite ring \( (\mathbb{Z}/q_k\mathbb{Z})^\times \).

Proof. (ii) The hypothesis \( \gcd(10, q_k) = 1 \) implies that the integer 10 generates a multiplicative subgroup

\[
H = \{10^0, 10^1, 10^2, \ldots, 10^n, \ldots\} \subseteq (\mathbb{Z}/q_k\mathbb{Z})^\times
\]

(12.1)
of cardinality \( N = \#\mathcal{H} \). Moreover, since \( \gcd(p_k q_k + 1, q_k) = 1 \), the map
\[
n \mapsto (p_k q_k + 1) 10^n \equiv s_n \mod q_k
\]
is 1-to-1 on the finite ring \((\mathbb{Z}/q_k \mathbb{Z})^\times\), it permutes the finite ring \(\mathbb{Z}/q_k \mathbb{Z}\). Therefore, the two subsets are equal, that is, \( \mathcal{H} = \mathcal{H} \).

Trivially, \( N = \#\mathcal{H} > \log q_k \), but it requires considerable more works to show that \( N > q_k^\varepsilon \), where \( \varepsilon > 0 \) is a small number. The ideal case has a large prime \( q = q_k \geq 2 \), and the integer 10 generates the maximal multiplicative group \( \mathbb{F}_q^\times \) of cardinality \( N = \varphi(q) \).

**Lemma 12.2.** Assume the Artin primitive root conjecture is valid. Let \( \{p_k/q_k : k \geq 1\} \) be the sequence of convergents of the real number \( \pi \), and let \( q \sim q_k \) be a large prime. Then,

(i) \( \mathcal{G} = \{p_k 10^n \equiv r_n \mod q : n \geq 0\} \) is the multiplicative group of the finite field \( \mathbb{F}_q^\times \),

(ii) \( \mathcal{H} = \{(p_k q_k + 1) 10^n \equiv s_n \mod q : n \geq 0\} \) is the multiplicative group of the finite field \( \mathbb{F}_q^\times \),

for infinitely many large primes \( q = q_k + o(q_k) \) such that \( \gcd(p_k q_k + 1, q) = 1 \), as \( q_k \to \infty \).

**Proof.** (ii) The conditional proof of the Artin primitive root conjecture, states that 10 generates the multiplicative group of the finite field \( \mathbb{F}_q^\times \) of a subset of primes \( \mathcal{Q} = \{\text{prime } q \geq 2 : \text{ord}_q 10 = q - 1\} \) of density \( \delta(\mathcal{Q}) = 0.3739558 \ldots \), see [14, p. 220]. In particular, the interval \([q_k, q_k + O(q_k/\log q_k)]\) contains approximately
\[
\pi(q_k + O(q_k/\log q_k)) - \pi(q_k) \gg q_k/(\log q_k)^2,
\]
large primes \( q = q_k + o(q_k) \) such that \( < 10 > = \mathbb{F}_q^\times \), as \( q \to \infty \), confer [11, p. 113] or similar reference. Now, proceed to use the same analysis as in the previous Lemma to complete the proof.

---

### 13 Large Multiplicative Orders Modulo \( n \)

The **multiplicative order** of an element \( u \) in a finite group \( G \) of cardinality \( n = \#G \) is defined by \( \text{ord}_u n u = \min\{m : u^m \equiv 1 \mod n\} \). The definition of the average multiplicative order in a fixed finite group has a very useful analytic formulation.

**Definition 13.1.** Let \( G \) be a cyclic group of order \( n = \#G \). The average multiplicative order of the elements \( u \in G \) is defined by
\[
A(n) = \frac{1}{n} \sum_{u \in G} \text{ord}_u n u = \frac{1}{n} \sum_{d | n} d \varphi(d),
\]
where \( \varphi(n) = n \prod_{d | n} (1 - 1/p) \).

On average, a random element in a random finite cyclic group \( G \) of cardinality \( n = \#G \leq x \) has a large order \( \text{ord}_n n u \approx n \).

**Theorem 13.1.** The mean average order \( \overline{A(n)} \) of the elements in the finite cyclic groups of cardinality \( n \#G \) such that \( n \leq x \) is
\[
\overline{A(n)} = a_0 x + O(\log^2 x),
\]
where the constant is
\[
a_0 = \zeta(3)/2\zeta(2) = 0.365381484700719249363018365653857 \ldots.
\]
Proof. Taking the mean value of the average multiplicative order gives

\[
\frac{1}{x} \sum_{n \leq x} A(n) = \frac{1}{x} \sum_{n \leq x} \frac{1}{n} \sum_{d|n} d\varphi(d)
\]

(13.2)

\[
= \frac{1}{x} \sum_{m \leq x} \frac{1}{m} \sum_{d \leq x/m} \varphi(d).
\]

The condition \(d \mid n\) was used to cancel the \(d\) term in the inner sum. Substituting the asymptotic average order of the totient function \(\varphi(n)\), [1, Theorem 3.7], and similar references, leads to

\[
\frac{1}{x} \sum_{n \leq x} A(n) = \frac{1}{x} \sum_{m \leq x} \frac{1}{m} \left( \frac{1}{2\zeta(2)} \left( \frac{x}{m} \right)^2 + O \left( \frac{x}{m} \log(x/m) \right) \right) + O \left( \frac{1}{m} \right)
\]

(13.3)

\[
= \frac{1}{2\zeta(2)} \sum_{m \leq x} \frac{1}{m^3} + O \left( \log x \sum_{m \leq x} \frac{1}{m} \right)
\]

\[
= \frac{\zeta(3)}{2\zeta(2)} x + O \left( \log^2 x \right).
\]

This completes the proof. \(\blacksquare\)

The double averaging accounts for the small error term. Moreover, since the mean average order \(A(n)\) is almost the same magnitude as the largest groups \(#G = n \approx x\), this result shows that the generators of the cyclic group, elements of maximal multiplicative orders, contribute the sheer bulk of the of the mean average order. A slightly more difficult proof appears in [28, Theorem 3.1].

Almost every element in a random finite cyclic group \(G\) of cardinality \(n = #G \leq x\) has a large order bounded below by \(\text{ord}_n u \gg n/\log n\).

**Theorem 13.2.** ([20, Theorem 6]) Assume GRH. Let \(x\) be a large number, and let \(G\) be finite cyclic group of cardinality \(n = #G \leq x\). Then, almost every element \(u \in G\) has large multiplicative order \(\text{ord}_n u \gg n/\log x\).

### 14 Estimates For Exponential Sums

**Theorem 14.1.** ([6, Theorem 1]) Let \(\mathcal{H} \subseteq \mathbb{F}_p\) be a multiplicative subgroup of order \(#\mathcal{H} > p^{c_0/\log \log p}\) for some sufficiently large constant \(c_0 > 1\). Then

\[
\max_{\gcd(a,p) = 1} \sum_{x \in \mathcal{H}} e^{2\pi ax/p} < e^{-\left(\log p\right)^c} #\mathcal{H},
\]

(14.1)

where \(c > 0\) is an absolute constant.

### 15 Properties of the Exponential Function

**Lemma 15.1.** Let \(\{p_k/q_k : k \geq 1\}\) be the sequence of convergents of the irrational real number \(\alpha \neq 0\), and let \(q = q_k + o(q_k)\) be a large integer. If the fractional part has an effective rational approximation
where \(0 \leq s_n < q_k\), then

\[
\left| e^{i2\pi \{\alpha 10^n\}} - e^{i2\pi \frac{s_n}{q}} \right| \ll \frac{1}{q^2}.
\] (15.2)

**Proof.** Basically, this follows from the Lipschitz property

\[
|f(x) - f(y)| \ll |x - y|
\] (15.3)

of the continuous function \(f(x) = e^{ix}\) of the real variable \(0 \leq |x| < 1\). Specifically,

\[
D = \left| e^{i2\pi \{\alpha 10^n\}} - e^{i2\pi \frac{s_n}{q}} \right|
\]

\[
= e^{i2\pi \frac{s_n}{q}} \left( e^{i2\pi \{\alpha 10^n\} - \frac{s_n}{q}} - 1 \right)
\]

\[
= \cos 2\pi \left( \{\alpha 10^n\} - \frac{s_n}{q} \right) - 1 + i \sin 2\pi \left( \{\alpha 10^n\} - \frac{s_n}{q} \right)
\]

\[
\leq \cos 2\pi \left( \{\alpha 10^n\} - \frac{s_n}{q} \right) - 1 + \sin 2\pi \left( \{\alpha 10^n\} - \frac{s_n}{q} \right)
\]

\[
\leq \left| \{\alpha 10^n\} - \frac{s_n}{q} \right|
\]

\[
\ll \frac{1}{q^2},
\]

since \(\cos z = 1 + O(z^2)\) and \(\sin z = z + O(z^3)\) for \(0 \leq |z| < 1\).

\[\square\]

16 Exponential Sums and Liouville Numbers

The next lemma demonstrates how the properties of irrational numbers can change the estimates of exponential sums.

**Theorem 16.1.** (Weyl) Let \(f(t) = a_d t^d + a_{d-1} t^{d-1} + \cdots + a_1 t + a_0\) be a polynomial of degree \(\deg f = d\), and let \(H, a, q \geq 1\) be integers with \(\gcd(a, q) = 1\). If \(\alpha\) is an irrational number such that

\[
\left| \alpha - \frac{a}{q} \right| < \frac{c}{q^\mu}
\] (16.1)

for some constants \(c \geq 1\) and \(\mu \geq 2\), then for any small number \(\varepsilon > 0\),

\[
\sum_{H \leq n \leq H+x} e^{i2\pi kf(n)\alpha} \ll x^{1+\varepsilon} \left( \frac{c}{q} + \frac{1}{x} + \frac{q}{x^\mu} \right)^{2^{1-d}}
\] (16.2)

The combination of the arbitrary large blocks of consecutive zeros in the \(b\)-adic expansion of a Liouville number, and Weyl inequality proves that certain exponential sums have trivial upper bounds.
Lemma 16.1. Let \( f(t) \) be a polynomial of degree \( \deg f = d \geq 1 \), and let \( \alpha \) be a Liouville number. Then,
\[
\sum_{n \leq x} e^{2\pi kf(n)\alpha} = \Omega_{\pm}(x),
\]
where the implied constant depends on the irrational number \( \alpha \), and the parameter \( k \neq 0 \) as \( x \to \infty \).

Proof. Let \( \{p_v/q_v : v \geq 1\} \) be the sequence of convergents of the Liouville \( \alpha \), and consider
\[
|\alpha - p_v/q_v| > \frac{1}{q_v^{\mu+\epsilon}}. \tag{16.3}
\]
Next, let \( x^{d-1} \in [q_v, q_v^\mu] \). Replacing these in the Weyl inequality, Theorem 16.1, yields
\[
\sum_{H \leq n \leq H+x} e^{i2\pi kf(n)\alpha} \ll x^{1+\epsilon} \left( \frac{c}{q} + \frac{1}{x} + \frac{q}{xd} \right)^{21-d} \tag{16.4}
\]
\[
\ll x^{1+\epsilon} \left( \frac{c}{xp^{3/4+\epsilon}} + \frac{1}{x} + \frac{x^{d-1}}{xd} \right)^{21-d},
\]
c \( \geq 1 \) and \( k \neq 0 \) are constants. Therefore, the hypothesis \( \mu \to \infty \) implies the trivial inequality
\[
\sum_{H \leq n \leq H+x} e^{i2\pi kf(n)\alpha} \ll x^{1+\epsilon}. \tag{16.5}
\]
This proves the claim. \( \square \)

17 Conditional Proof For The Normality Of \( \sqrt{2} \)

The proof of the normality of \( \sqrt{2} \) in base 10 is based on the rational prime approximations in stated in Section 10, the average large subgroups modulo \( p \) generated by the base 10, see Theorem 13.1, (which is similar to the conditional result for rational primes approximations in Section 10), the Weyl criterion in Section 6, and the Wall criterion stated in Theorem 7.1.

Proof. (Theorem 1.1) Let \( x \) be a large number. Now, consider the sequence of real numbers
\[
\mathcal{B}(\sqrt{2}) = \{\sqrt{2} \cdot 10^n : n \geq 1\}, \tag{17.1}
\]
and the corresponding exponential sum
\[
\sum_{n \leq x} e^{i2\pi r \sqrt{2} \cdot 10^n}, \tag{17.2}
\]
where \( r \neq 0 \) is a rational parameter. By Theorem 10.1, there exists an infinite sequence of primes \( \mathcal{P} = \{p \geq x : p \text{ prime}\} \) such that
\[
\left| \sqrt{2} - \frac{a}{p} \right| < \frac{1}{p^{4/3-\epsilon}} \tag{17.3}
\]
for each \( p \in \mathcal{P} \), where \( 1 \leq a < p \). Moreover, on average, the subset of integers
\[
\mathcal{A} = \{10^n \equiv m \mod p : n \leq x \leq p\} \tag{17.4}
\]
is sufficiently large for each $p \in \mathcal{P}$, and has cardinality $\#A \gg p^\delta$, where $\delta > 0$ is a small number, see Theorem 13.1 and Conjecture 10.1. Therefore,

$$\sum_{n \leq x} e^{i2\pi \sqrt{2} \cdot 10^n} = \sum_{m \leq x} e^{i2\pi r m + O\left( \frac{1}{m^{1/3 - \varepsilon}} \right)} \ll p^{1-\varepsilon}. \tag{17.6}$$

By Theorem 14.1, the exponential sums have nontrivial upper bounds

$$\sum_{n \leq x} e^{i2\pi \sqrt{2} \cdot 10^n} = \sum_{m \in A} e^{i2\pi r m + O\left( \frac{1}{m^{1/3 - \varepsilon}} \right)} \ll p^{1-\varepsilon}. \tag{17.6}$$

By the Weyl criterion, see Theorem 6.1, it follows that the sequence of real numbers (17.1) is uniform distributed modulo 1. Lastly, by Theorem 7.1, it follows that the real number $\sqrt{2}$ is normal in base $b = 10$. ■

18 Conditional Proof For The Normality Of Pi

The proof is based on the foundational results in Section 11, Section 12, the Weyl criterion in Section 6, and the Wall criterion stated in Theorem 7.1.

Proof. (Theorem 1.2) By Lemma 11.3, almost every fractional part has the random rational approximation

$$\frac{r_n}{2q} + \frac{1}{(2q)^{\mu-1}} + O\left( \frac{1}{q^2} \right) \leq \{\pi 10^n\} \leq \frac{s_n}{q} + O\left( \frac{1}{q^2} \right), \tag{18.1}$$

where $0 \leq c_n, r_n, s_n \leq q_k$, and $\mu \geq 2$. There are at most $O(\log q)$ exceptions, see Lemma 11.2. The nonsymmetric inequalities (18.1) are rewritten as

$$\left| \{\pi 10^n\} - \frac{r_n}{2q} - \frac{1}{(2q)^{\mu-1}} \right| \ll \frac{1}{q^2}, \tag{18.2}$$

and

$$\left| \{\pi 10^n\} - \frac{s_n}{q} \right| \ll \frac{1}{q^2}, \tag{18.3}$$

Therefore, by Lemma 15.1, the corresponding exponentials pairing

$$e^{i2\pi m \left( \frac{r_n}{2q} + \frac{1}{(2q)^{\mu-1}} \right)} \asymp e^{i2\pi m \{\pi 10^n\}}, \tag{18.4}$$

and

$$e^{i2\pi m \{\pi 10^n\}} \asymp e^{i2\pi m \frac{s_n}{q}}, \tag{18.5}$$

where $m \neq 0$, are proportionals. Similarly, the corresponding exponential sums

$$\sum_{n \leq q} e^{i2\pi m \left( \frac{r_n}{2q} + \frac{1}{(2q)^{\mu-1}} \right)} \asymp \sum_{n \leq q} e^{i2\pi m \{\pi 10^n\}}, \tag{18.6}$$
and
\[ \sum_{n \leq q} e^{i2\pi m \{ \pi 10^n \}} \asymp \sum_{n \leq q} e^{i2\pi m \frac{2n}{q}}, \quad (18.7) \]
where \( q = q_k + o(q_k) \) is a large prime such that \( \gcd(p_k q_k + 1, q) = 1 \), are proportionals.

By Lemma 12.2 the subsets
\[ G = \{ p_k 10^n \equiv r_n \mod q \} \quad \text{and} \quad H = \{ (p_k q_k + 1)10^n \equiv s_n \mod q \} \quad (18.8) \]
are sufficiently large multiplicative subgroups of the finite field \( \mathbb{F}_q^\times \). In particular, conditional on the Artin primitive root conjecture, the cardinalities are
\[ \#G = q - 1 \gg q^\varepsilon, \quad \#H = q - 1 \gg q^\varepsilon, \quad \varepsilon > 0. \]

By Theorem 14.1, the exponential sums have nontrivial upper bounds
\[ \sum_{n \leq q} e^{i2\pi m \left( \frac{1}{2q} + \frac{1}{2(q)^{\mu - 1}} \right)} \asymp \sum_{n \leq q} e^{i2\pi m \{ \pi 10^n \}} \ll q^{1-\varepsilon}, \quad (18.9) \]
and
\[ \sum_{n \leq q} e^{i2\pi m \{ \pi 10^n \}} \ll \sum_{n \leq q} e^{i2\pi m \frac{2n}{q}} \ll q^{1-\varepsilon}. \quad (18.10) \]

By the Weyl criterion, see [19, Theorem 2.1], any of the expressions (18.9) or (18.10) is sufficient to prove the uniform distribution of the sequence \( \{ \pi 10^n : n \geq 1 \} \).

Establishing the main result as an unconditional does not seem to be difficult, because proving the existence of infinitely many large multiplicative subgroups
\[ \mathcal{H} = \{10^0, 10^1, 10^2, \ldots, 10^n, \ldots \} \subseteq (\mathbb{Z}/q_k \mathbb{Z})^\times \quad (18.11) \]
of cardinalities \( \# \mathcal{H} \gg q^{\varepsilon} \) as \( q_k \to \infty \), is not a difficult task, see Section 13. The techniques employed appear to be extendable to other irrational numbers \( \alpha \) of finite irrationality measure \( \mu(\alpha) \geq 2 \) and base \( b = 10 \). The generalization to other bases \( b \neq 10 \) seems to require significant additional works.

19 Results for Multiplicative Nonlacunary Sequences

The proof provided here is based on the results for "multiplicative orbits" of nonlacunary sequences (19.2). This proof seems to be depend on the arithmetic properties of the irrational numbers. Accordingly, this analysis seems to be well suited for structured irrational numbers such as algebraic irrational numbers, and nonLiouville numbers. This restriction circumvents the exceptional cases such as the Liouville type numbers
\[ \alpha = \sum_{n \geq 1} \frac{1}{b^{f(n)}}, \quad (19.1) \]
where \( b > 1 \) is a base, and \( f(n) \) is a rapidly increasing function. In [13, p. 49] there is a short discussion on an exceptional case, and confer [21] for some other exceptional cases. Other closely related problems are studied in [3], [12], et alii.
Theorem 19.1. Let $p \geq 2$ and $q \geq 2$ be multiplicative independent integers, and let $\alpha$ be a nonLiouville number. Suppose that the sequence of real numbers
\[ \{p^m q^n \alpha : m, n \geq 1\}. \] is dense in $\mathbb{R}/\mathbb{Z}$, then, the irrational number $\alpha$ is a normal number in both base $p$ and base $q$.

Proof. (i) Let $k = q^m$ be an integer parameter, and consider the sequence $\beta_n = p^n \alpha$, with $m, n \geq 1$.

It is sufficient to consider nonLiouville irrational number numbers $\alpha$. Otherwise, for Liouville numbers $\alpha$, equation (19.3) is false since the $p$-adic expansion of the number $\alpha$ can have blocks of consecutive zeros of arbitrary lengths infinitely often as $x \to \infty$. So Liouville numbers are not normal in any base $p$, see Remark 19.1.

Suppose that the nonLiouville irrational number $\alpha$ is not a normal number in base $p$. Equivalently, the Wall criterion
\[ \frac{1}{x} \sum_{n \leq x} e^{i2\pi k \beta_n} = \frac{1}{x} \sum_{n \leq x} e^{i2\pi (p^n q^m \alpha)} = o(1) \] any parameter $k = q^m > 0$, as $x \to \infty$, is false, see Theorem 7.1.

This implies that
\[ \frac{1}{x} \sum_{n \leq x} e^{i2\pi k \beta_n} = \frac{1}{x} \sum_{n \leq x} e^{i2\pi (p^n q^m \alpha)} = \Omega_{\pm}(1) \] as $x \to \infty$, see the definition of the symbol $o(1)$ in (2.1) and its negation in (2.3).

Moreover, summing over the parameter $k = q^m \leq x$ yields
\[ \frac{1}{x} \sum_{m \leq x} \frac{1}{x} \sum_{n \leq x} e^{i2\pi k \beta_n} = \frac{1}{x} \sum_{m \leq x} \frac{1}{x} \sum_{n \leq x} e^{i2\pi (p^n q^m \alpha)} \]
\[ = \frac{1}{x} \sum_{m \leq x} \Omega_{\pm}(1) \]
\[ = \Omega_{\pm}(1) \] as $x \to \infty$. But, this contradicts the hypothesis that the sequence of real numbers
\[ \{p^n q^m \alpha : m, n \geq 1\}. \] is dense in $\mathbb{R}/\mathbb{Z}$. Specifically, by Lemma 4.1, there is a rearrangement of this sequence
\[ \{\beta_{m,n} = p^{\sigma(n)} q^{\sigma(m)} \alpha : m, n \geq 1\} \] such that
\[ \frac{1}{x^2} \sum_{m \leq x, n \leq x} e^{i2\pi h \beta_{m,n}} = \frac{1}{x^2} \sum_{m \leq x, n \leq x} e^{i2\pi h (p^{\sigma(n)} q^{\sigma(m)} \alpha)} \]
\[ = o(1), \]
where \( h \neq 0 \), as \( x \to \infty \). Therefore, the hypothesis (19.4) is false. It implies that the irrational number \( \alpha \) is a normal number in base \( p \geq 2 \).

(ii) Since the sequence (19.6) is symmetric in the bases \( p \) and \( q \), reversing the labels in (i) yields the same result for base \( q \geq 2 \).

**Remark 19.1.** Note that for Liouville type numbers \( \alpha \), the \( p \)-adic expansions have arbitrary large number of zeros, so the relation

\[
\frac{1}{x} \sum_{n \leq x} e^{2\pi k \beta_n} = \frac{1}{x} \sum_{n \leq x} e^{2\pi (p^m q^m \alpha)} = \Omega_{\pm}(1)
\]

any parameter \( k = q^m > 0 \), as \( x \to \infty \), is actually true, see Lemma 16.1. Thus, Theorem 19.1 is restricted to a collection of nonLiouville numbers \( \alpha \). For example, quadratic irrationals cannot have arbitrary large number of zeros in the decimal expansions since the irrationality measures of these irrational numbers is 2.

**Remark 19.2.** The dense sets \( \{ \theta^n : n \geq 1 \} \) generated by Pisot and Salem numbers \( \theta > 1 \) have a single generators. These dense sets, which are ”exponential orbits”, have different properties than the dense sets generated by two or more generators, as in (19.6). These dense sets, which are ”multiplicative orbits”, and other closely related problems are studied in [3], [12], et alii.

## 20 Unconditional Proof For The Normality Of \( \sqrt{2} \)

Theorem 1.1 is a corollary of the previous theorem. The details are shown below, and the statement is repeated here for convenience.

**Theorem 1.1** The irrational number \( \sqrt{2} \in \mathbb{R} \) is a normal number in base \( p \geq 2 \). In particular, \( \sqrt{2} \) is simply normal number in base 10. Hence, the decimal expansion

\[
\sqrt{2} = 1.414213562373095048801688724209698075696718753769480731766797379 \ldots
\]

contains infinitely many digit 0, infinitely many digit 1, infinitely many digit 2, et cetera.

**Proof.** Fix the pair of multiplicative independent integers \( p = 10, q = 3 \), and let \( \alpha = \sqrt{2} \). By the Furstenberg criterion, see Theorem 4.1, the set of real numbers

\[
\{3^m 10^n \alpha : m, n \geq 1\}
\]

is dense in \( \mathbb{R}/\mathbb{Z} \). Therefore, by Theorem 19.1, the irrational number \( \sqrt{2} \) is normal in base \( p = 10 \). ■
21 Problems

21.1 Lacunary and Nonlacunary Sequences

Exercise 21.1. Show that the sequence \( \{u_n = 2^n + 3^n : n \geq 1\} \) is lacunary.

Exercise 21.2. Show that the sequence \( \{u_{m,n} = 2^m3^n : m, n \geq 1\} \) is nonlacunary.

21.2 Powers of Polynomials Roots

Exercise 21.3. Which of these polynomials \( x^3 - x + 1, x^3 - x - 2, \) and \( x^3 + x + 1 \) has root which is a Pisot number?

Exercise 21.4. Let \( \theta > 1, \theta_1 = \theta^{-1}, \theta_2, \ldots, \theta_9 \) be the roots of the Lehmer polynomial \( x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1 \). Show the the sequence of real numbers

\[
x_n \equiv \theta^n + \theta_1^n + r_1^n \cos \omega_1 n + \cdots + r_4^n \cos \omega_4 n \mod 1,
\]

where \( \theta_i + \theta_{i+1} = r_1 \cos \omega_1, |\theta_i| = r_i \leq 1 \) and \( \omega_i \in (-\pi, \pi) \) for \( i \in \{1, 2, 3, 4\} \), is dense in the unit interval \((0, 1)\).

References

[1] Apostol, T. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976. 12, 14

[2] Aistleitner, Christoph; Becher, Veronica; Scheerer, Adrian-Mari; Slaman, Theodore A. *On the construction of absolutely normal numbers*. Acta Arith. 180 (2017), no. 4, 333–346. 2

[3] Akiyama, S.; Tanigawa, Y. *Salem numbers and uniform distribution modulo 1*. Publ. Math. Debrecen 64(3-4) (2004), 329-34. 7, 18, 20

[4] Bailey, David H.; Crandall, Richard E. *Random generators and normal numbers*. Experiment. Math. 11 (2002), no. 4, 527-546, 2003. 2

[5] Boyd, D. W. *Pisot and Salem numbers in intervals of the real line*. Math. Comp. 32 (1978), 1244-1260. 5

[6] Bourgain, J.; Glibichuk, A. Ft *Exponential sum estimates over a subgroup in an arbitrary finite field*. J. Anal. Math. 115 (2011), 51-70. 14

[7] Borwein, Jonathan M. *The life of \( \pi \): from Archimedes to ENIAC and beyond. From Alexandria, through Baghdad*, 531-561, Springer, Heidelberg, 2014. 3

[8] Becher, Veronica; Yuhjtman, Sergio A. *On absolutely normal and continued fraction normal numbers*. Int. Math. Res. Not. IMRN 2019, no. 19, 6136-6161. http://arxiv.org/abs/1704.03622. 2

[9] Champernowne, D. G. *The Construction of Decimals Normal in the Scale of Ten*. J. London Math. Soc. 8 (1933), no. 4, 254-260. 2

[10] Copeland, A. H.; Erdos, P. *Note on Normal Numbers*. Bulletin of the American Mathematical Society, 52 (10): 857-860, 1946. 2
[11] Davenport, H. *Multiplicative Number Theory*. Graduate Texts in Mathematics, Springer-Verlag New York 1980. 13

[12] Doche, Christophe; Mendes France, Michel; Ruch, Jean-Jacques. *Equidistribution modulo 1 and Salem numbers*. Funct. Approx. Comment. Math. 39(2): 261-271 (December 2008). 7, 18, 20

[13] Furstenberg, H. *Disjointness in ergodic theory, minimal sets, and a problem in diophantine approximation*. Math. Systems Theory, 1:1-49, 1967. 4, 18

[14] Hooley, Christopher. *On Artin’s conjecture*. J. Reine Angew. Math. 225 (1967), 209-22. 13

[15] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. 5th ed., Oxford University Press, Oxford, 1975. 11, 12

[16] Kra, Bryna. *A generalization of Furstenberg’s diophantine theorem*. Proceedings of the American Mathematical Society, 127(7):1951-1956, 1999. 5

[17] Khoshnevisan, Davar. *Normal numbers are normal*. Clay Mathematics Institute Annual Report 2006: 15, continued pp. 27-31. 3

[18] Koksma, J. F. *Jin mengentheoretiecher Satz fiber die Gleichverteilung modulo Eins*. Compositio Mathematica, vol. 2(1935), pp. 250-258. 7

[19] Kuipers, L.; Niederreiter, H. *Uniform distribution of sequences*. Pure and Applied Mathematics. Wiley-Interscience, New York-London-Sydney, 1974. 7, 8, 10, 18

[20] Kurlberg, P. Pomerance, C. *On a problem of Arnold: the average multiplicative order of a given integer*. Algebra and Number Theory, 7 (2013), 981-999. 14

[21] Martin, Greg. *Absolutely Abnormal Numbers*. http://arxiv.org/abs/0006089. 18

[22] Matomaki, Kaisa. *The distribution of αp modulo one*. Math. Proc. Camb. Phil. Soc. (2009), 147, 267. 9

[23] Niven, I. *Irrational Numbers*. Am. Math. Assotiation, Weley and Sons Inc., 1956. 3, 8

[24] Pisot, C. Salem, R. *Distribution modulo 1 of the powers of real numbers larger than 1*. Compositio Math. 16 (1964), 164-168. 7

[25] Salem, R. *A remarkable class of algebraic integers. Proof of a conjecture of Vijayaraghavan*. Duke Math. J. 11(1): 103-108 (March 1944). 5

[26] Stoneham, R. G. *On absolute (j,ε)-normality in the rational fractions with applications to normal numbers*. Acta Arith. 22 (1972/73), 277?286. 2

[27] Schmiedt, Anja; Weiss, Christian. *The Pair Correlation Function of Low-Discrepancy Sequences with Small Stochastic Error Terms*. https://arxiv.org/abs/2211.09891.

[28] von zur Gathen, Joachim; Knopfmacher, Arnold; Luca, Florian; Lucht, Lutz G.; Shparlinski, Igor E. *Average order in cyclic groups*. J. Theor. Nombres Bordeaux 16 (2004), no. 1, 107-123. 14
[29] Waldschmidt, M. *Diophantine approximation on linear algebraic groups. Transcendence properties of the exponential function in several variables.* Grundlehren der Mathematischen Wissenschaften, 326. Springer-Verlag, Berlin, 2000. 10, 11, 12